SÉRIE PENSAMENTO MATEMÁTICO @ CIÊNCIA COMPUTAÇÃO

Volume I: Dos Primórdios da Matemática aos Sistemas Formais da Computação

João Bosco M. Sobral

EDIÇÃO DO AUTOR

João Bosco M. Sobral

Dos Primórdios da Matemática aos Sistemas Formais da Computação

Série Pensamento Matemático @
Ciência da Computação
Edição do Autor

Laboratório e Grupo de Pesquisa
UFSC-CNPq

Revisão Técnica
Lucas Guardalben
Ph.D. MAP-I Doctoral Programme Computer Science
NAP - Network Architectures and Protocols, Universidade de Aveiro, Portugal

Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística
Laboratório DMC & NS
Projeto de Pesquisa PRPE 2013.1533

João Bosco M. Sobral

Dos Primórdios da Matemática aos Sistemas Formais da Computação

Série Pensamento Matemático @
Ciência da Computação

1ª Edição

Florianópolis
Edição do Autor
2015

Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística
Laboratório DMC & NS
Projeto de Pesquisa PRPE 2013.1533

Nota - Muito trabalho foi empregado nesta edição. No entanto, podem ocorrer erros de digitação, impressão ou dúvida sobre os conceitos usados. Em qualquer das hipóteses, o autor e editor, solicita a comunicação no email *bosco.sobral@ufsc.br*, para que o mesmo possa encaminhar a correção da questão mencionada.

Catalogação na fonte pela Biblioteca Universitária
da
Universidade Federal de Santa Catarina

S677d Sobral, João Bosco M.
Dos Primórdios da Matemática aos Sistemas Formais da Computação [recurso eletrônico] / João Bosco M. Sobral. - 1. ed. - Florianópolis : Edição do Autor, 2015.
315 p. : il., tabs.-(Série Pensamento Matemático. Ciência da Computação.)

Esta publicação foi organizada pelo Departamento de Informática e Estatística da Universidade Federal de Santa Catarina.

Inclui bibliografia e índice.
ISBN: 978-85-902995-2-3(v.1)

1. Matemática - história. 2. Lógica matemática. 3. Ciência da Computação. I. Título. II. Série.

CDU: 51(091)

Agradecimentos

O autor gostaria, primeiramente, de agradecer ao Departamento de Informática e Estatística pela oportunidade de trazer neste projeto de pesquisa, o fruto da minha formação matemática e da experiência de ensino de graduação e pós-graduação em Ciência da Computação, nos meus 38 anos na UFSC.

Embora, eu não tenha sido um professor do ensino em disciplinas de Matemática do INE, mas obtive todo o sentimento do elo entre a matemática e a lógica nas várias disciplinas onde atuei: ensino de programação, linguagens formais, redes de computadores, computação paralela e distribuida, sistemas distribuidos, métodos formais de especificação de sistemas, mobilidade em computação e segurança computacional.

Agradecimentos pessoais para os colegas do INE, Jerusa Marchi, Vânia Bogorny, Rafael Cancian, José Fletes, João Dovicchi, Fernando Cruz, Roberto Willrich, Juliana Eyng, Jean Martina, Sergio Peters, Patricia Plentz, Marcelo Menezes Reis, Carla Westphall e Carlos Westphall, com os quais em breves momentos, eu pudi falar do meu trabalho, mas que contribuiram direta ou indiretamente, motivando-me para a realização do mesmo. Também, a Lucas Guardalbem pela revisão e criação das capas, e a dedicação incondicional de Renato Bobsin Machado, incentivador e revisor deste projeto, a quem agradeço incondicionalmente.

A série de livros intitulada **Pensamento Matemático @ Ciência da Computação** é aqui iniciada, no INE-UFSC, aberta aos que lidam com matemática, lógica e ciência da computação, a qual não seria possivel ser publicada, facilmente, sem o template ABNTeX2, a liberdade de edição do autor na Agência Brasileira do ISBN, o serviço de catalogação da BU-UFSC e a projeção do sistema Repositório Institucional da UFSC.

Lista de ilustrações

Lista de tabelas

Sumário

Prefácio

É comum ouvir-se dizer que "a Matemática é a linguagem da Ciência", mas o simplismo da frase esconde diversos aspectos inerentes às palavras "Matemática" e "Ciência". Em alguns ramos do conhecimento, como na Física, por exemplo, têm-se plena consciência de que um conhecimento mais profundo da Matemática é essencial para entender e descrever os fenômenos naturais que nos cercam. Um corolário imediato dessa consciência é o evidente interesse pela Matemática demonstrado pelos alunos que se iniciam nos cursos de Física. Embora, e talvez, não se possa dizer o mesmo da maioria dos alunos que se iniciam em outros ramos de estudos, o mundo moderno está repleto de exemplos onde a Matemática se mostra essencial, como no caso da Ciência da Computação.

Neste volume I, o Prof. João Bosco faz um passeio pela Matemática e pela Lógica, citando grandes personagens dessa epopeia humana e descrevendo os resultados mais relevantes sob o foco dos fundamentos da Ciência da Computação. É gratificante, por exemplo, verem-se mencionados no Capítulo 14, resultados de Kurt Gödel, monumentos à inteligência humana.

O autor não tem a pretensão de ser este um livro texto; como ele próprio escreve. O mesmo foi pensado como livro de apoio ao estudo dos fundamentos da Ciência da Computação. Além de muito bem ilustrado com reproduções fotográficas das imagens dos vários matemáticos, lógicos e filósofos que deram contribuições fundamentais à ciência da computação, o livro fornece ao final de cada capítulo uma boa quantidade de referências recomendadas aos leitores interessados.

Rio de Janeiro, Novembro de 2015

Rolci de Almeida Cipolatti
Departamento de Matemática
Instituto de Matemática da UFRJ

Prefácio

Podemos dizer que dentre as atividades intelectuais humanas, as principais são a ciência e a filosofia. Dentre estas, as consideradas mais elevadas e mais antigas são a matemática, a música, e a filosofia. A música e a matemática, aliás, se separaram em épocas relativamente recentes. A aritmética, a geometria, a trigonometria, a álgebra e outros ramos da matemática estão intrinsecamente ligados à noção de quantidade mas a natureza da matemática como ciência e o foco de seu estudo estão, também, vinculados à filosofia e à história da matemática.

A música, por exemplo, seja ela de Bach, Beethoven, Jazz, Rock ou Bossa Nova não tem muito significado fora de seu contexto histórico. Em alguns casos, temos que levar em consideração o contexto temporal e espacial. Por exemplo, podemos até gostar da música de Tchaikovisky mas, certamente não a percebemos como um russo do século XIX a perceberia. São questões vinculadas ao ethos cultural de tempo e origem. Assim é a matemática. Postulados, conceitos e teoremas estão em um contexto histórico em que o homem, em seu desejo de aprender foi estabelecendo as bases da matemática durante a construção de sua trajetória rumo à civilização.

As civilizações egípcias, babilônicas e, posteriormente, a grega clássica criaram os fundamentos da matemática que se estabeleceram para evoluírem até os dias de hoje. Durante sua evolução histórica a matemática passou de um nível de simplicidade aritmética para um nível de maior complexidade nas suas áreas de domínio. Ou seja, do simples ato de contar às integrais de contorno, aos diferenciais de Laplace, às equações de Riemann, à constante de Plank, aos princípios como o de Heisenberg, aos teoremas de Gödel ou mesmo aos operadores como os hamiltonianos da mecânica quântica. Cada problema, solução ou teorema estão ligados à história que deve ser conceitualmente compreendida em relação ao tempo e espaço.

Não temos como entender a computabilidade sem a sua perspectiva histórica. As provas de Alonso Church e Alan Turing vieram de conceitos anteriores como os conceitos de recursividade de Cantor, da lógica combinatória de Schönfinkel e do cálculo lambda de Haskell Curry. Hilbert, no início do século XX, propôs 23 problemas a serem resolvidos no século. Em 1910 apresentou 10 deles na conferência de Paris, dos quais apenas 4 foram resolvidos. Assim, liga-se a história ao tempo espaço dos problemas e a história liga Hilbert com von Neumann, Heisenberg, Dirac, Schrödinger, Niels Bohr e Einstein, mostrando como as principais teorias da física moderna foram criadas.

A perspectiva histórica também é importante para compreender como Einstein chegou à relatividade e a sua busca pela teoria geral do universo, ou como Turing usou a computabilidade para resolver o problema da máquina Enigma, ou, ainda, como Heisenberg chegou ao princípio da incerteza buscando pela posição do elétron. Como todos se relacionam? Se relacionam por meio da transformação histórica de conceitos matemáticos que vão se juntando como um enorme quebra-cabeça. Só a história pode mostrar que a matemática que estudamos hoje foi gerada por um processo construído no tempo da jornada da humanidade. Uma jornada de milhares de anos de teorias obtidas pela ciência e experimento. A história, na verdade, é quem molda teorias. A relatividade de Einstein nunca foi sua principal teoria. Um dos matemáticos da teoria quântica era von Neumann que propos o modelo da computação determinística. Vejam que paradoxo! Um dos cientistas da teoria quântica, nada determinística, propõe um modelo de arquitetura de processador para o computador como uma máquina de estado determinística.

Podemos dizer que a ciência é investigativa mas grande parte nasce da criatividade, da intuição e da interatividade humana, ou seja, do processo histórico. Portanto, há que se diferenciar entre o modelo investigativo da matemática e o modelo cognitivo. Sendo a matemática uma ciência com base em postulados toda validação de resultados da matemática como modelo investigativo, é corroborado por ela mesma como ciência cognitiva. Desta forma podemos dizer que o contexto histórico é fundamental para a compreensão do seu conteúdo. Certamente, a matemática atingiu, hoje, uma importância crucial em todas as atividades humanas. Seja na economia, na engenharia ou na saúde, todos dependem de métodos matemáticos. Cada um dos ramos da matemática agora se subdividem em áreas com especificidades como as especialidades da engenharia ou da medicina.

A matemática tem uma teia de relações com várias áreas do conhecimento. As relações da matemática com a astronomia, a física e outras ciências podem ser observadas desde há muito tempo, em livros como os de Newton, Kepler, Pascal, Descartes e outros mais modernos como Gauss, Hamilton, Boole, Cantor, Riemann, entre outros. Assim forma-se a base para a um livro de suma importância. Um livro que é fundamental para a compreensão, pelo leitor, de como surgiram as ideias matemáticas. Antes de deduzir e demonstrar os teoremas principais ou mais elaborados da matemática, é importante mostrar ao leitor as bases a partir das quais foram enunciados os problemas e como foi conduzida sua solução com o alicerce matemático existente. Mas o livro não para por aí. Trata-se de uma leitura muito agradável que nos transporta à visão de problemas e soluções matemáticas em seu tempo; na sua origem; ou na sua fonte. Organizado, preferencialmente numa linha temporal, o livro aborda as diversas teorias matemáticas de uma maneira interdependente, mostrando que os conceitos fundamentais se mantém e se aplicam às descobertas matemáticas cada vez mais complexas.

Evitando a grande dificuldade de expor e demonstrar as modernas teorias rela-

tivísticas, quânticas ou das cordas o livro compensa pela facilidade de expor as ideias sobre elas e como foram elaboradas, questionadas e resolvidas. Torna-se mais fácil entender e mais evidente de se constatar as relações conceituais do homem e sua obra no contexto temporal da evolução da matemática. É como compreender de que maneira a matemática vai se revelando a si mesma e por si mesma. É a história permitindo a formação do homem acostumado à discussão matemática e ao pensamento matemático, mais do que um usuário habituado a formulários e receitas como ferramentas de soluções de problemas. Resta-me apenas desejar uma boa leitura.

Florianópolis, Novembro de 2015

João Cândido Dovicchi
Departamento de Informática e Estatística da UFSC

Do Autor

Bem vindo à serie "Pensamento Matemático @ Ciência da Computação". Este é o primeiro volume intitulado "*Dos Primórdios da Matemática aos Sistemas Formais da Computação*". Este livro foi organizado através das atividades do projeto de pesquisa INE-UFSC 2013.1333, realizado no Departamento de Informática e Estatística da UFSC, durante os anos de 2014 e 2015. O seu conteúdo diz respeito ao elo existente entre a matemática, a lógica, e a ciência da computação. Destina-se a servir como material de apoio para o ensino em disciplinas de matemática ou lógica, para alunos em ciência da computação. O conteúdo aqui exposto, tenta mostrar como a matemática e a lógica contribuiram para o surgimento da ciência da computação, colocando do ponto de vista histórico os diversos acontecimentos que surgiram de mentes geniais que, no passado, foram bem aproveitados ou redundaram diretamente na aparição da ciência da computação. As páginas deste livro mostrarão que a matemática e a lógica sempre foram realizações humanas que proporcionaram as ideias para as soluções dos problemas teóricos e práticos, que fizeram surgir a ciência da computação. O tema do livro tem uma história longa e bastante abrangente e interessante. Afinal, onde quer que olhemos a ciência da computação, permeia a lógica e a matemática nos fundamentos desta ciência. Sem a matemática e lógica como base, não haveria ciência da computação.

São 16 capítulos. Assim, os assuntos dos foram escolhidos e distribuidos nos capítulos para enfatizar como os conceitos da matemática foram utilizados na ciência da computação. O livro deve ser utilizado como complemento de estudo relativo a outros livros de matemática, lógica ou ciência da computação teórica. O principal objetivo é mostrar as origens dos fundamentos da ciência da computação, e de alguns conceitos que temos hoje na computação. O seu conteúdo mostra para que serve a matemática e a lógica, quando se pensa em ciência da computação. Ao final, os sistemas axiomáticos da ciência da computação, são definidos no sentido de se deixar mais claro, a base matemática e lógica para a ciência da computação. O livro focaliza a matemática discreta e a lógica, desde seus primórdios até final dos anos 40 do século XX.

É comum no meio universitário, encontrarmos alunos detestando matemática, porque não sabem do que se trata ou porque não sabem bem para que ela serve. Na realidade, os professores de matemática pura, em virtude de só viverem essa matemática, não tem como dizer como a matemática serve para a ciência da computação. A matemática, da forma como é ensinada, acaba não depertando interesse para a grande maioria dos alunos, pela simples razão que o que se ensina não são ideias

e a razão dos conceitos existirem. Em geral, desde tenra idade, para os estudantes a matemática é ensinada no sentido de resolver problemas práticos, e não uma educação em matemática. O conhecimento bruto, a memorização e a rapidez são quesitos considerados ao invés das ideias. Muitas vezes, manipulações de fórmulas e cálculos acabam produzindo, o desejo de se livrar da matemática. Muitas vezes, ocasionando a evasão de alunos da computação.

Este livro tem a missão de ajudar e destina-se a alunos de graduação de ciência da computação, ou mesmo os de níveis mais avançados que não despertaram para a matemática e a lógica, a se conectarem com a matemática. Neste sentido, para ensinar matemática e lógica na computação é melhor que essas disciplinas sejam ensinadas por professores que conheçam, também, pelo menos algumas das áreas da ciência da computação. A experiencia de ensino do autor, mostra também que a distância em que são colocadas certas disciplinas num curriculo de ciência da computação, acaba dificultando o entendimento de outras disciplinas desta área, porquê se estuda certas disciplinas de matemática e lógica, nos primeiros períodos, e determinadas disciplinas da computação, onde se precisa de matemática e lógica, nas últimas fases. Se eu conseguir avançar neste caminho, terei alcançado o objetivo de evitar de muitos jovens desistam, logo no início de um curso de graduação em computação, simplesmente, por não saberem de que se trata a matemática e a lógica, que é colocada nos seus primeiros cursos de graduação.

A sua essência é mostrar como os conceitos da matemática e da lógica influiram e serviram no surgimento e construção da ciência da computação. Embora muito do conteúdo aqui colocado, seja abstrato para um aluno iniciante, possivelmente ainda imaturo, a intenção do material do livro é servir de apoio em disciplinas de matemática, lógica ou computação teórica. É uma tentativa de acrescentar o conhecimento sobre as raízes da ciência da computação, proporcionando uma visão que outros livros, que tratam de temas específicos, não contemplam do ponto de vista histórico e conceitual. Quem deseja conhecer uma ciência, precisa também conhecer suas raízes. A ideia neste trabalho é motivar o aluno a ficar conectado com o mundo da matemática e da lógica, voltado à ciência da computação, tentando motivá-lo, evitando o que é muitas vezes não entendido e acabam por originar o problema da evasão de alunos nas fases iniciais de um curso de graduação. É neste contexto que este livro apresenta seu conteúdo.

Toda a evolução histórica aqui descrita é mostrada nos capítulos apropriados, mostrando a participação de matemáticos e lógicos famosos e importantes, como **Euler**, **Fermat**, **Leibniz**, **De Morgan**, **George Boole**, **Frege**, **Gauss**, **Cantor**, **Hilbert**,**Gödel**, **Alonzo Church**, **Bertrand Russell** e tantos outros. O assunto é bastante abrangente, mas o autor tenta enfatizar as ideias e os conceitos, sem entrar no mérito das demonstrações matemáticas, que estão em toda parte, nos livros de matemática, lógica e nos de teoria matemática da computação. O livro apresenta o lado humano da matemática e da lógica, e enaltece as realizações dos grandes matemáticos e lógicos, no seu contexto histórico, cujas ideias influiram na aparição da

ciência da computação. Com isso, o autor imagina o sentido de mostrar a importância da matemática e da lógica para a construção desta nossa ciência.

Entre os princípios que nortearam o autor na apresentação do seu material destacam-se os seguintes: (1) Salientar a afinidade das civilizações orientais nos primórdios da matemática, onde tudo começou. (2) Relacionar as tendências da matemática aritmético-algébrica e da lógica, ambas *formalistas*, em direção à construção da ciência da computação. (3) Se a matemática e a lógica são uma grande aventura nas ideias, as suas histórias refletem alguns dos mais nobres pensamentos de inúmeras gerações. Como consequência, a ciência da computação também comporta ideias geniais de gerações mais recentes, mas sobretudo, numa evolução muito mais rápida, talvez pela grande contribuição dada pela matemática, pela lógica e pela aparição da microeletrônica que revolucionou o computador digital. Assim, o autor vislumbrou, a princípio, a organização de dois volumes, baseando a exposição da matematica e da lógica, em termos das personalidades, as verdadeiras donas das ideias, as vezes narrando fatos e suas ideias geniais, além de algumas escolas, em vez de assuntos. Os vários assuntos aqui abordados estão em outros livros mais específicos de matemática, de lógica e nos livros da ciência da computação teórica. O autor pretende, em outros volumes, explicitar alguns temas aqui tratados muito superficialmente

Por vezes, uma referência bibliográfica substitui uma análise histórica. A história aqui contada começou nos primórdios da matemática, indo até **kurt Gödel** e **Alonzo Church**, já no século XX, no limiar do surgimento da ciência da computação. A seleção do material foi baseada exclusivamente levando-se em conta os personagens da lógica e da matemática, que mais influiram para a ciência da computação. Nem sempre foi possivel consultar todas as fontes em primeira mão. Algumas vezes, foram ulilizadas fontes de segunda. O autor reconhece que é um bom princípio, conferir as afirmações tanto quanto possivel pelas fontes originais. Entretanto, no tempo disponível ao autor, as citações decorreram, de vários livros de sua própria biblioteca sobre matemática, lógica e computação. Além dos recursos próprios de bibliografia do autor, foram feitos o uso extensivo de diversos sites de Internet, pelo conteúdo interessante que apresentaram. Também, pelos recursos financeiros disponíveis, nestes dois volumes, o editor é o próprio autor, conforme as regras da Agência Brasileira do ISBN.

Florianópolis, Novembro de 2015

João Bosco M. Sobral

CAPÍTULO 1

As Bases da Ciência da Computação

Iniciamos este livro focalizando as bases da Ciência da Computação: a Matemática e a Lógica. Os grandes cientistas da Matemática e da Lógica, mesmo sem ter a visão de todo o conjunto da obra, avançaram no tempo, construindo a ciência que levou à construção do computador digital e o desenvolvimento desta ciência. A evolução da Ciência da Computação ocorreu promovida pelas mentes geniais, cada uma delas se baseando no trabalho dos que os antecederam. Se prestarmos atenção, perceberemos que o laço entre certos gênios, mesmo separados entre séculos, é algo admirável. A natureza da Matemática (números, fundamentos e lógica, estruturas algébricas, geometrias) conduziram à *computabilidade*, aos modelos de computação, suas origens e limitações que temos hoje. Enfim, a evolução das ideias da Matemática e da Lógica conduziram ao surgimento da Ciência da Computação. Os conceitos originais da Computação sempre estiveram ligados à Matemática e à Lógica, o que mostra que quem criou a Ciência da Computação foram os matemáticos e o lógicos. As ideias da Matemática e da Lógica, algumas que estão aí a séculos, foram muito bem aproveitadas impulsionando o desenvolvimento da Computação. Neste capítulo são colocadas as constribuições, numa visáo geral de como a Matemática e a Lógica influiram diretamente no surgimento da Ciência da Computação.

O conhecimento histórico proporciona um enriquecimento da cultura humana, a qual, permite enfrentar novos desafios e estes serem concluídos com êxitos. A história destaca os papéis dos personagens principais que a criou, pois a criatividade é a extrapolação das ideias já incorporadas em novas versões.

1.1 O que é a Matemática

A palavra *matemática* vem do grego, significando "estudo", "ciência", "conhecimento", "aprendizagem". Matemática é entender o mundo de uma forma mais estruturada e objetiva.

Matemática consiste em uma simplificação do nosso mundo que é limitado em muitos dos seus aspectos. Genericamente, pode-se definir a Matemática como "**matemática é aprender com a natureza**". Em Struik (1987) e Janos (2009), em seu livro "Matemática e Natureza", é bem destacado que a matemática é, genericamente, sobre ideias.

Há muito tempo buscava-se um consenso quanto à definição do que é a Matemática. No entanto, nas últimas décadas do século XX tomou forma uma definição que tem ampla aceitação entre os matemáticos:

"A Matemática é a ciência das regularidades" (os padrões).

Segundo esta definição, o trabalho do matemático consiste em examinar **padrões abstratos**, tanto reais (visuais) como imaginários (mentais). Ou seja, os matemáticos procuram regularidades na natureza, nos números, no espaço, na ciência e na imaginação. E formulam teorias com as quais tentam explicar as relações observadas.

Matemática é a ciência do raciocínio abstrato e lógico. A matemática estuda quantidades, medidas, estruturas, espaços e variações. Um trabalho matemático consiste em procurar por **padrões**, formular **conjecturas** e a partir de **axiomas** e **definições**, por meio de **deduções** rigorosas estabelecer novos resultados. Deduções que levam a resultados, constituem os **teoremas**. Teoremas, base para outros teoremas, são chamados de **lemas**. Resultados consequentes de teoremas, são os chamados **corolários**.

Como veremos no próximo capítulo, desde as nossas primeiras concepções de **número** e **forma**, que datam de tempos tão remotos como os do começo do *período neolítico*, que a Matemática sempre foi parte da atividade humana. Ela evoluiu a partir de contagens, medições, cálculos e do estudo sistemático de formas geométricas e movimentos de objetos físicos. Depois, a Matemática se desenvolveu, primitivamente, no Egito, no Oriente Médio, mais precisamente na Mesopotâmia, na Grécia, na Índia (Hindus), e na civilização árabe. Os raciocínios mais abstratos que envolviam *argumentação lógica* surgiram com os matemáticos gregos aproximadamente em 300 a.C., notadamente com a obra *Os Elementos* de **Euclides** (aproximadamente, 365 a.C-300 a.C). A partir do período histórico da *Renascença* (fins do século XIV e início do século XVII), o desenvolvimento da Matemática intensificou-se na Europa, quando novas descobertas científicas levaram a um crescimento acelerado de resultados, que influencia até os dias de hoje.

1.2 Características da Matemática

Como em Omnes (1996), deparamo-nos com as características da Matemática, as quais são elencadas a seguir:

- (a) Seu íntimo parentesco com a Lógica, a tal ponto que não se pode dizer

onde as duas se separam.

- (b) A capacidade das matemáticas se reduzirem a um puro uso de símbolos, com o que elas mostram a distância que as separa de qualquer espécie de realidade concreta. As matemáticas são o extremo da abstração (ausência de detalhes), que desde o nascimento da geometria grega, essa característica de abstração é separada da realidade concreta.

- (c) Uma terceira característica é o estreito laço que elas conservam com a realidade, na medida em que as ciências da natureza, particularmente a Física, não podem dispensar-se da linguagem ou dos conceitos da matemática.

- (d) Além dessas, as matemáticas são um produto do cérebro humano, são realizações humanas e, são feitas por homens que vivem em sociedade.

1.3 A estrada de Leibniz a Gödel

Por volta do século III a.C., o matemático indiano **Pingala** já havia originado a primeira ideia do que viria a ser o sistema de numeração binário. No século XVIII, **Gottfried Leibniz** (1646-1716) acreditava que se poderia resolver todos os problemas de cooperação humana através de uma linguagem universal ("*characteristica universallis*") e de uma álgebra de raciocínio ("*calculus ratiocinator*"). **Leibniz** tentou desenvolver algo pelo qual todo raciocínio poderia ser reduzido a uma cálculo matemático. Provavelmente, a partir da ideia de **Pingala**, **Leibniz** em 1703, desenvolveu a Lógica em um sentido formal e matemático, utilizando o sistema binário. Em seu sistema, uns e zeros também representam conceitos como verdadeiro e falso, ligado e desligado, válido e inválido. Ainda usado atualmente no processamento de todos computadores modernos, o sistema estabelece que sequências específicas de uns e zeros podem representar qualquer informação.

Na linha divisória entre a matemática dos séculos XVIII e XIX, dos que contribuiram indiretamente para assuntos na Ciência da Computação, domina a figura de **Carl Friedrich Gauss** (1777-1855), que tem participação na "teoria dos números" com o surgimento da *aritmética modular*, muito utilizada em computação.

Em Stewart (2012), **Ian Stewart** (o autor de *Mania de Matemática* e *Será que Deus joga dados?*) faz um maravilhoso trabalho de equilibrar história e teoria matemática num livro fácil de se entender. Em *Uma História da Simetria na Matemática*, **Ian Stewart** conta sobre o conceito de simetria e em seu prefácio ressalta:

A data é 13 de maio de 1832. Na névoa da alvorada, dois jovens franceses se encaram, pistolas em punho, em duelo por causa de uma mulher. O tiro é disparado, e um dos homens tomba no chão, mortalmente ferido. Ele morre duas semanas depois, de peritonite, aos 21 anos, sendo enterrado numa vala comum - uma sepultura não identificada. Uma das mais importantes ideias da história da Matemática e da ciência

quase morre como ele.

O duelista que sobreviveu continou desconhecido. O que morreu era **Évariste Galois**, revolucionário político e matemático obsessivo cujos trabalhos reunidos ocupavam apenas seis páginas. Mas o legado que transmitiu revolucionou a Matemática. **Galois** inventou uma linguagem que descreve a simetria nas estruturas matemáticas e deduz as suas propriedades. Conhecida como "teoria de grupo", hoje essa linguagem é usada tanto na Matemática pura quanto na aplicada, na qual regula a formação dos padrões naturais do mundo em que vivemos. A simetria também tem papel central nas fronteiras da física, no mundo quântico do muito pequeno e no mundo relativístico do mundo grande. Então, a teoria dos grupos é uma unificação matemática dos principais campos da física moderna. E tudo começou como uma simples questão de álgebra, sobre a resolução de equações matemáticas - encontrar uma incógnita a partir de algumas indicações matemáticas, que correspondeu a tentativa de solução algébrica para as quínticas.

É importante compreender que já se sabia da existência de soluções particulares para as equações quínticas. A questã era: será que essas soluções podaim ser sempre representadas por uma fórmula algébrica? Em 1821, o jovem norueguês **Niels Henrik Abel** demonstrou que uma quíntica não poderia ser resolvida de forma algébrica. Suas demonstração, porém foi indireta e bem misteriosa. Ele provou que nenhuma solução geral era possível, mas não mostrou o porquê. **Évariste Galois** descobriu que a impossibilidade de resolver a quíntica derivava das simetrias da equação. Se essas simetrias passassem pelo teste de **Galois**, elas se encaixariam de uma forma muito específica, e as equações poderiam ser resolvidas por uma fórmula algébrica. Se as simetrias não passassem, essa fórmula não existiria. **Galois** descobriu que ma quíntica não poderia ser resolvida por uma fórmula porque ela tinha um tipo errado de simetria.

Simetria não é um número nem um formato, é um tipo de *transformação* - uma maneira de mover um objeto. Se o objeto parecer o mesmo depois de movido, a transformação presente é uma simetria. Por exemplo, um quadrado continua um quadrado se for rotacionado em um ângulo reto.

Essa ideia, muito desenvolvida, é básica na atual compreesão atual do Universo. No cerne da "teoria da relatividade"teoria da relatividade, de **Albert Einstein** (1879-1955), encontra-se o princípio de que as leis da Física devem ser as mesmas em todos os lugares e em todos os tempos. Ou seja, as leis devem ser simétricas em relação ao movimento no espaço e à passagem do tempo. A nos diz que tudo no Universo é constituído a partir de uma coleção de partículas "fundamentais". O comportamento dessas partículas é regido por equações matemáticas - as "leis da natureza" - e essas leis também tem uma simetria. Partículas podem se transformar matematicamente em outras bem diferentes (este não é o caso de simetria), e essas transformações também não alteram as leis da Física.

Esses conceitos, e outros mais recentes, nas fronteiras da física atual, não poderiam ser descobertos sem uma profunda compreensão matemática da simetria. Essa compreensão veio da matemática pura; seu papel na Física só surgiu depois. Ideias extraordinariamente úteis podem sair de considerações apenas abstratas.

Simetria tem um história que começou na antiga **Babilônia** e termina nos tempos de hoje do século XXI. A história da simetria mostra como a busca aparentemente inútil do que parecia uma fórmula impossível abriu um novo horizonte para o Universo, revolucionando a Ciência e a Matemática. De uma maneira mais abrangente, a história da simetria ilustra como as influência culturais e a continuidade histórica das grandes ideias podem ganhar destaque por conta de sublevações ocasionais, tanto políticas quanto científicas.

A simetria não se tornou uma ideia dominante pelo caminho esperado: a geometria. O indispensável conceito de simetria que os matemáticos e físicos usam hoje chegou pela álgebra.

Neste mesmo período de **Gauss** (1877-1855), **Évariste Galois** (1811-1832), antes de sua morte, deixou nada menos do que a chave da álgebra moderna, que veio a ser a **teoria dos grupos**.

No século XIX, durante muitas décadas, a matemática pura, nos países de língua inglesa, manteve a sua forte ênfase na álgebra formal. **Augustus De Morgan** (1806-1871), de 1826-1866 foi professor na University College, em Londres, e também apresentou uma forma de uma lógica das proposições. **De Morgan** influenciou muito as matemáticas britânicas da época. A influência de **De Morgan** pode ser atestada em sua obra *Budget of Paradoxes* (1872) publicada postumamente. Esta "álgebra oriunda de uma lógica"iniciou uma escola de pensamento que aspirava estabelecer a unificação da lógica e da matemática.

George Boole (1815-1864) foi influenciado pelos trabalhos de lógica simbólica realizados por **De Morgan**. A tendência formalista nos matemáticos ingleses teve importância para a aparição de *An Investigation of the Laws of Thought* em 1854, de **George Boole** (1815-1864) do Queens's College em Dublin. Um século e meio depois de **Leibniz**, **George Boole** publicou, baseado neste trabalho, *álgebra booleana* (em 1854), com um sistema completo que permitia a construção de modelos matemáticos para o processamento computacional. Então, mostrava-se como as leis da lógica formal, que tinham sido codificadas por **Aristóteles** (384 a.C-322 a.C), que eram ensinadas durante séculos nas Universidades, e depois sistematizada por **Leibniz** (1703) podiam, elas próprias, tornar-se um objeto de uma álgebra, como surgiu a álgebra de Boole.

Em 1884, as ideias ficaram mais fortalecidas com o livro de **Gottlob Frege** "*Die Grundlagen der Aritmetik*", no qual propôs uma dedução dos conceitos da aritmética a partir da lógica. Estas investigações atingiram o clímace no início do século XX e,

influenciaram o trabalho posterior de **David Hilbert** (1862-1943) sobre os fundamentos da aritmética.

Por outro lado, o estudo moderno da teoria dos conjuntos foi iniciado por **Georg Cantor** (1845-1818) e **Richard Dedekind** (1831-1916) em 1870. **Georg Cantor** ficava conhecido como o criador da *teoria dos conjuntos*. Seus principais artigos sobre esta teoria aconteceram entre 1895-1897. Neste mesmo tempo, **Cantor** descobriu o primeiro dos paradoxos suscitados pela teoria dos conjuntos. Ele descobriu os paradoxos, enquanto trabalhava sobre seus artigos de 1895 e 1897, e ele escreveu a **Hilbert** (1862-1943) em 1896, explicando o paradoxo para este. **Hilbert** contribuiu indiretamente para a Ciência da Computação. **Hilbert** pensava na Matemática, mas dois dos sues problemas que ele colocou na comunidade científica da época, bem no início do século XIX, influenciaram, posteriormente, as primeiras ideias de **Turing** (1912-1954) para a Ciência da Computação.

Mais ainda, **Bertrand Russel** (1872-1970) descobriu um paradoxo que leva seu nome **Russell** em 1903, enquanto trabalhava sobre sua obra *Principles of Mathematics* (1910-1913). O paradoxo surgiu em conexão com o conjunto de todos os conjuntos, os quais não são membros deles próprios, isto é, sobre a teoria dos conjuntos de **Cantor**. Tornava-se claro que se tinha de usar a teoria dos conjuntos com cuidado, especialmente na utilização do termo "todos", e evitar o descuido semântico.

A resposta ao paradoxo veio do próprio **Russell**, com a introdução de sua **teoria dos tipos**. Embora primeiro introduzido por Russell em 1903 nos *Princípios*, sua *teoria dos tipos* encontra sua expressão madura em seu artigo *Mathematical Logic como base na Teoria dos Tipos* de 1908, e na obra monumental que ele com co-autoria de **Alfred North Whitehead** (1861-1947), *Principia Mathematica* (1910 , 1912, 1913). Sua idéia básica era que a referência a coleções problemáticas (*como o conjunto de todos os conjuntos que não são membros de si mesmos*) poderiam ser evitados, organizando todas as sentenças em uma hierarquia, começando com frases sobre os *membros* no nível mais baixo, sentenças sobre *conjuntos de membros* no próximo nível mais baixo, sentenças sobre *conjuntos de conjuntos de membros* no próximo nível mais baixo, e assim por diante. Deste ponto de vista, segue-se que é possível, se referir a uma *coleção de objetos* para os quais uma determinada condição vale, se esses estão todos ao mesmo nível ou do mesmo "*tipo*". Surge então, a ideia de *tipos* e a *teoria dos tipos*, que veio ser utilizada na Ciência da Computação, no sentido de se organizar os espaços de dados em programas de computador. No último capítulo do segundo volume, sobre *Tipos Abstratos de Dados*, o leitor verá que a *teoria dos tipos* deu origem às *classes* de objetos, e que este conceito norteou em como se pode programar um computador segundo o paradigma da orientação a objetos. Em teoria dos conjuntos, uma *classe* (também chamada *coleção*) é "quase"um conjunto, ou seja, classes tem várias propriedades em comum com conjuntos, mas não são, necessariamente, conjuntos.

Após a descoberta de paradoxos na *teoria ingênua dos conjuntos*, sistemas de

axiomas foram propostos no início do século XX. Foram feitas muitas tentativas para revelar o valor verdadeiro das matemáticas. E um dos caminhos foi estabelecer um *sistema de axiomas* para a teoria dos conjuntos de **Cantor**, dos quais os axiomas de **Zermelo-Fraenkel** são os mais conhecidos. **Ernst Zermelo** e **Adolf Fraenkel**, participantes do círculo de **Hilbert**, realizou-os em 1908, para evitar o paradoxo de **Russel**. E hoje, a teoria dos conjuntos é uma forma matemática de se modelar o mundo em conjuntos, enquanto o *paradigma orientado a objetos* é a forma computacional de se modelar o mundo através das classes de objetos, advinda da *teoria dos tipos*.

Este volume termina lembrando **Kurt Gödel**. Grande parte da Ciência da Computação teórica mais geral, tem suas raízes, historicamente, bem como conceitualmente, no campo da lógica, e por isso, muitos dos resultados de **Gödel** também são importantes no campo do valor teórico para Ciência da Computação. Entre 1933-1935, **Gödel** introduziu as funções recursivas primitivas. Em 1934,**Gödel** definiu as funções recursivas gerais, a partir das ideias de **Jacques Herbrand**. **Gödel** não se preocupou com a noção de efetivamente computável, mas somente com a definição de função recursiva, como as *funções recursivas primitivas*.

O final do século XIX e início do século XX foi marcado pelas controvérsias na matemática, sobretudo na forma de método, de como a matemática deveria conduzir a sua teoria da prova. Como explicado em Costa (2008) sobre as correntes filosóficas época, divididas em *Logicismo*, *Intuicionismo*, *Formalismo* e a *Matemática e Linguagem*. O intuicionismo deu origem a algumas formas de construtivismo.

A corrente clássica logicista de **Bertrand Rusell** conduziu à primeira iniciativa sobre a *teoria dos tipos*. E a corrente filosófica construtivista dos anos 30, não se limitou apenas à matemática. A década dos anos 30, na mesma época de **Gödel**, foi marcada por avanços na **teoria da computação** através dos trabalhos de **Alonzo Church**, **Kleene**, **Rosser** e **Alan Turing**. A época foi de grande importância para o surgimento e desenvolvimento da *teoria da recursão*. Com isso, surgiu uma nova área da matemática chamada *matemática recursiva*. Essa área, assim como as demais áreas da matemática clássica, utilizava a lógica clássica.

Na década de 1940, o matemático **Andrei Andreyevich Markov** desenvolveu uma versão construtiva da matemática recursiva. Basicamente, **Markov** desenvolveu a *matemática recursiva* substituindo a lógica clássica pela lógica intuicionista. E o mesmo fez, **Martin Löf**, na década de 60, quando estudou a teoria dos tipos, substituindo a lógica clássica pela lógica intuicionista. O fato é que a teoria dos tipos veio contribuir para a Ciência da Computação, quando se trata de dados de programas, e redundar no que temos hoje, relativo a visão dos tipos abstratos de dados, que nos proporcionou as classes de objetos do paradigma de programação orientado a objetos.

1.4 A Matemática Discreta

Uma das maneiras de se dividir a Matemática em dois grandes grupos de sistemas matemáticos, é fazê-la pela classe dos **sistemas discretos** e a classe dos **sistemas contínuos** Janos (2009). Mas estamos, neste livro, interessados nos sistemas discretos. Deixemos a matemática dos sistemas contínuas para um outro volume da série *Pensamento Matemático @ Ciência da Computação*. A Matemática Discreta é utilizada, diretamente, como uma ferramenta essencial para a Ciência da Computação, e é abordada nas primeiras disciplinas de um curso de graduação em ciência da computação. A classe dos **sistemas discretos** está associada aos **números naturais** $\mathbb{N}$, um conjunto **enumerável**, tal como $\{0, 1, 2, \ldots\}$, e que modelam os fenômenos com *variações discretas*. Para sistemas discretos da computação, temos a **Matemática Discreta**, a mais apropriada para estudar e modelar esses sistemas. No computador digital todas as grandezas são de estados elementares e de tempo discreto.

Na **Matemática Discreta** teórica, existem estruturas muito utilizadas, com aplicação na Ciência da Computação. Referências bibliográficas que podem ser citadas, por exemplo, são os livros Deo (1974) (teoria dos grafos) , Stanat (1977) (modelos matemáticos, raciocínio matemático, conjuntos, relações binárias, funções, contagem e teoria da Complexidade, conjuntos infinitos e álgebras), Tremblay (1987) (Lógica, teoria dos conjuntos, álgebra, teoria dos grafos e teoria da computabilidade), Sudkamp (1988) (Matemática preliminar e linguagens, gramáticas de linguagens, teoria dos autômatos e linguagens, decidibilidade, computabilidade e complexidade computacional) Carnielli e Epstein (2005) (Computabilidade, funções computáveis, Lógica e o fundamentos da matemática) e Sipser (2011) (Autômatos e linguagens, teoria da computabilidade e teoria da complexidade). Existem muitas outras obras tratando sobre a Matemática Discreta e entre estas existem as obras que tratam da álgebra como em Monteiro (1969).

No contexto da matemática discreta, destaca-se a "teoria dos grafos", surgida no século XVIII, com **Euler** (1707-1783) em 1736, com o problema das *pontes de Königsberg*, e que se desenvolveu como base para várias teorias subsequentes. A teoria está intimamente ligada a muitos ramos da Matemática, e é poderosa na construção de modelos matemáticos e resolução de problemas relacionados a qualquer sistema envolvendo uma relação binária. Ainda no século XIX, **Gustav Kirchhoff**(1824-1887), que investigava redes elétricas, e **Arthur Cayley** (1821-1895), que estudava química orgânica, desenvolveram a *teoria das árvores*, hoje proporcionando as estruturas de dados usadas em Computação. **Cayley** foi um dos primeiros a usar a teoria dos conjuntos de **Cantor** e a definir o conceito de *conjunto* de forma moderna e, juntamente com **William Hamilton** (1788-1856) contribuiram para a álgebra linear. **Arthur Cayley** foi um matemático britânico. Foi professor Matemática Pura, na Universidade de Cambridge, de 1863 a 1895. As suas contribuições incluem a multiplicação de matrizes e o teorema de Cayley.

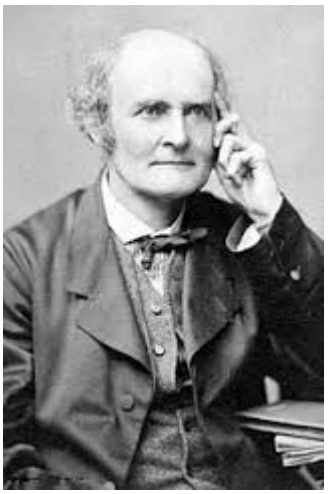


Figura 1 – Arthur Cayley - Árvores em grafos, estruturas de dados e multiplicação de matrizes.

Fonte: Google Images - pt.wikipedia.org.

Em matemática, e mais especificamente na teoria dos grafos, uma árvore é um grafo não direcionado em que quaisquer dois vértices são conectados por exatamente um caminho. Em outras palavras, qualquer gráfico ligado sem ciclos simples é uma árvore. Uma floresta é uma união disjunta de árvores. Os vários tipos de estruturas de dados referidos como árvores em Ciência da Computação tem gráfos subjacentes que são árvores na teoria dos grafos, embora as estruturas tais dados são árvores geralmente com nodo-raiz, assim, de fato, a ser grafos orientados, e também pode ter ordenação adicional de ramos. O termo "árvore" foi cunhado em 1857 pelo matemático britânico **Arthur Cayley**.

Gustav Robert Kirchhoff foi um físico alemão. Suas contribuições científicas foram principalmente no campo dos circuitos elétricos, e com isso criu a Tree Theory (Teoria das Árvores), estruturas de grafos muito utilizadas para estruturar dados em Ciência da Computação.

Também na primeira metade do século XX, a álgebra modificou o seu caráter ancestral. Em vez de tratar meramente da teoria das equações algébricas, tornou-se a doutrina abstrata dos dias de hoje, com suas estruturas algébricas, com suas estruturas de grupos, anéis, corpos e conceitos. Uma das origens da nova álgebra foi o desenvolvimento da "teoria dos grupos", partindo da teoria de **Galois** das equações algébricas e levando a uma teoria abstrata autônoma, especialmente à **teoria dos grupos finitos** Struik (1987), estabelecendo deste modo a transformação da álgebra como um todo. *Grupos finitos* acabaram por encontrar seu espaço na área da criptografia aplicada a sistemas computacionais de segurança. Portanto, a partir da teoria dos números (que nos proporcionou a aritmética modular, aplicada na área de Segurança da Informação) e da teoria dos conjuntos, surgiram as estruturas algébricas como os grupos, anéis (polinômios), corpos, espaços vetoriais (que tem

Figura 2 – Gustav Kirchhoff - Árvores em ciência da computação.

Fonte: Google Images - www.nndb.com.

uma álgebra vetorial), espaços métricos (**Hilbert**) servindo para a computação quântica, e espaços topológicos (computação gráfica). Todas estas teorias alicerçam e contribuem para determinadas áreas da Ciência da Computação, beneficiadas pela Lógica ou Matemática Discreta.

1.5 Lógica e Ciência da Computação

A "teoria da computação" se baseiou em conceitos definidos pelos lógicos e matemáticos. Na ordem de suas existências, vieram **Leibniz**, **De Morgan**, **Boole**, **Frege**, **Gödel**, **Church**, **John von Neumann**, **Turing** e **Shannon**.

A partir da Lógica de **Aristóteles**, sistematizada por **Leibniz** no século XVII, criando o cerne de uma lógica proposicional, no século XIX, em 1854, o matemático e lógico britânico **George Boole**, através da obra intitulada "*An Investigation of the Laws of Thought*", apresentou um sistema matemático de análise lógica conhecido como *Álgebra de Boole*. Depois da álgebra de **Boole**, o lógico **Gottlob Frege** definiu o primeiro cálculo baseado em . **Gottlob Frege** (1879) evoluiu da *Lógica Proposicional* (Leibniz) para a *Lógica dos Predicados*, passando das verdades absolutas para as verdades relativas, que é a lógica que viria a ser usada nos programas mais comuns do computador de hoje - $x < 3$ é um predicado, uma função que retorna *verdade* ou *falso*.

Giuseppe Peano (1858-1932) foi um matemático e lógico italiano. Autor de mais de 200 livros e artigos, ele foi um dos fundadores da lógica simbólica e desenvolvedor da teoria dos conjuntos, para as quais ele também contribuiu bastante na notação. De 1890 até sua morte em 1932, ele trabalhou a lógica simbólica e usava o método axiomático, realçando a necessidade do rigor matemático. Isto conduziu-o ao seu *Formulário Matemático* (5 volumes, 1895-1908), uma apresentação compreensiva dos

teoremas da matemática (cerca de 4200), logicamente fundamentada com a ajuda dos seus silogismos. **Peano** não convenceu suficientemente o mundo matemático, mas a sua influência em questão de Lógica é inequívoca Struik (1987).

Alonzo Church, nos anos 30, depois de ter passado um ano na Universidade de Harvard, em seguida, um ano em Göttingen e Amsterdam, voltou para os Estados Unidos tornando-se professor na Universidade de Princeton em 1929, instituição excitante para a Lógica em 1930. Haviam **Church**, juntamente com seus alunos **Rosser** e **Kleene**. **Kurt Gödel**, matemático e lógico, visitou o *Institute for Advanced Study* de 1933-1935, antes de se mudar para lá permanentemente. Havia também,**John von Neumann** que foi orientado por **Hilbert**. Importante também citar **Alan Turing**, que já pensava sobre a noção de calculabilidade efetiva (depois, chamada de computabilidade), que veio como um estudante-visitante em 1936 e ficou para completar seu doutorado sob a orientação de **Church**.

O trabalho de **Church** é de grande importância na lógica matemática, na "teoria da computabilidade" (também chamada de "teoria da recursão") e em Ciência da Computação teórica. **Church** contribuiu com alguns trabalhos importantes, dentre os quais *Alternatives to Zermelo's Assumption* (1927). Ele criou o λ-Cálculo nos anos 30, que hoje é uma ferramenta inestimável para cientistas da computação. **Church** foi fundador do *Journal of Symbolic Logic* in 1936. O λ-cálculo deu origem, posteriormente, a primeira linguagem de programação funcional, *LISP*, concebida por **John McCarthy** em 1958. Num célebre artigo, **McCarthy** mostra que é possível usar exclusivamente funções matemáticas e estruturas de dados elementares. O que é possível a partir do momento em que há um mecanismo formal para manipular funções, como o λ-Cálculo de **Alonzo Church**. A linguagem *LISP* (List Processing) foi projetada, primariamente, para o processamento de dados simbólicos. Ela é uma linguagem formal oriunda da Matemática, classificada como uma linguagem funcional. Durante os anos de 1970 e 1980, *LISP* tornou-se a principal linguagem da comunidade da área de Inteligência Artificial.

A Lógica é utilizada na especificação de sistemas computacionais. Como em Zach (2006), computações são estruturas matemáticas contendo nodos (estados) e transições de estados e a Lógica faz afirmações sobre tais estruturas. Portanto, computações são modelos para expressões lógicas. Esta abordagem é conhecida como *computação-como-modelo*. Como um exemplo de como a Lógica é utilizada nesta abordagem, considere as triplas de **Hoare**, que tipicamente são representados como $\{\Gamma\}\, P\, \{\Delta\}$, significando que se um programa P começa a ser rodado em um estado que satizfaz as proposições lógicas em Γ, então P termina (se é que termina) em um estado que satisfaz as proposições em Δ. As fórmulas em Γ são chamadas de *pré-condições* de P, enquanto que as em Δ são chamadas de *pós-condições*, depois que P foi executado. Esta abordagem é a essência dos métodos formais baseados na linguagem Z, como em Spivey (1989), constituída da "teoria dos conjuntos", Lógica dos Predicados e do λ-Cálculo, na qual os estados são descritos por fórmulas da lógica dos predicados, enquanto as transições são descritas nos esquemas da linguagem Z. Nesses esquemas,

existem as variáveis envolvidas nas transições e mais as pré-condições e pós-condições descritas em fórmulas da lógica dos predicados.

1.6 Lógica e Computadores

Julius Edgar Lilienfeld (1882-1963) foi um físico Austro-Húngaro Judeu. Nasceu em Lemberg na Áustria-Hungria (hoje chamado Lviv na Ucrânia). Entre 1900 e 1904, **Lilienfeld** estudou na *Friedrich-Wilhelms-Universität* (rebatizada Universidade Humboldt, em 1949), em Berlim, onde recebeu seu Ph.D. em 18 de fevereiro de 1905. Em 1905 ele começou a trabalhar no Instituto de Física da Universidade de Leipzig.

Figura 3 – Julius Lilienfeld - O criador do Field Effect Transistor e do Electrolytic Capacitor em meados dos anos 20.

Fonte: www.computerhistory.org.

O início da carreira de **Lilienfeld** foi na Universidade de Leipzig, onde realizou importante trabalho inicial sobre as descargas elétricas no "vácuo", entre eletrodos metálicos, de cerca de 1910 em diante. Mais do que qualquer outro cientista, ele era responsável pela identificação de emissão de elétrons como um efeito físico separado. Ele o chamou de "emissão auto-eletrônico, e estava interessado como uma possível fonte de *elétrons* para tubos de raios-X miniaturizados, em aplicações médicas. **Lilienfeld** foi o responsável pelo primeiro relato confiável da fenomenologia experimental de elétron campo emissão, em 1922. O efeito foi explicado por **Fowler** e **Nordheim** em 1928.

Lilienfeld emigrou para os Estados Unidos no início de 1920, originalmente para defender patentes que possuía, e em seguida, fez uma carreira científica e industrial nos Estados Unidos, tornando-se cidadão americano posteriormente.

Entre outras coisas, ele inventou um transistor "FET-like" e o "capacitor eletrolítico" na década de 1920. Ele apresentou várias patentes que descrevem a construção e

operação de transistores, assim como muitas características de transistores modernos. Um transistor "FET-like" foi concedido 28 de janeiro de 1930. Quando **Brattain**, **Bardeen** e **Robert Gibney** tentaram obter patentes em seus primeiros dispositivos, a maioria de suas reivindicações foram rejeitada devido às patentes **Lilienfeld**.

A radiação óptica emitida quando elétrons atacam uma superfície de metal é denominado "Lilienfeld radiação", depois que ele descobriu que perto de ânodos de tubos de raios-X. A Sociedade Americana de Física nomeou um dos seus principais prêmios após **Lilienfeld**.

Na estrada de **Leibniz** à **Shannon**, em 1931, apenas seis anos depois de **Julius Lilienfeld** (1882-1963) ter inventado o *transistor* no Canadá, **Kurt Gödel** (1906-1978) definiu os fundamentos da Ciência da Computação teórica com seu trabalho em linguagens formais universais e os limites de prova e computação. Ele construiu sistemas formais que permitam declarações auto-referenciais que falavam sobre si mesmas, em particular, sobre se essas podiam ser derivadas de um conjunto enumerável de axiomas dados através de um procedimento de prova de teoremas computacional.

Gödel passou a construir expressões que afirmavam a sua própria indemonstrabilidade, para provar que a Matemática tradicional ou era falha, ou continha declarações improváveis. O resultado da incompletude de **Gödel** é amplamente considerada como a realização mais notável da Matemática do século XX, embora alguns matemáticos dizem que era uma questão da Lógica, não da Matemática, e outros chamam o resultado fundamental da Ciência da Computação teórica. Reformulado posteriormente por **Church**, **Post** e **Turing**), o assunto transformou-se numa disciplina que ainda não existia oficialmente naquela época, mas foi efetivamente criada através do trabalho iniciado por **Gödel**. O resultado de **Gödel** teve um enorme impacto não só sobre a Matemática, na Filosofia, mas também veio a ter na Ciência da Computação. Seguindo **Herbrand**, **Gödel** também contribuiu para o desenvolvimento das funções recursivas, depois muito estudadas por **Church** e seus alunos **Kleene** e **Rosser**.

No século XX, em 1936, a *Lógica* foi incorporada à ideia da construção das máquina abstratas de **Alan Turing**. Partindo-se do princípio que muitas das nossas tarefas diárias são uma sequência de passos que obedecem a uma determinada ordem, de um estado inicial, através de um período de tempo finito, e que nesse período produzimos resultados esperados e bem definidos num estado final, podemos classificar essas tarefas dentro de um procedimento lógico, que utilizam os conceitos da lógica para fazer com que uma máquina pudesse produzir as sequências de passos apropriados para essas tarefas. **Turing** descobriu que qualquer procedimento lógico bem definido, passo a passo, podia ser executado numa *máquina abstrata*. **Turing** provou também que, teoricamente, podia-se construir uma máquina de **Turing** universal, que podia seguir os passos de um procedimento *lógico* bem definido, passo a passo, lendo instruções e processando as mesmas, seguindo regras de transição entre passos, assim fazendo surgir a ideia de uma *máquina programável*.

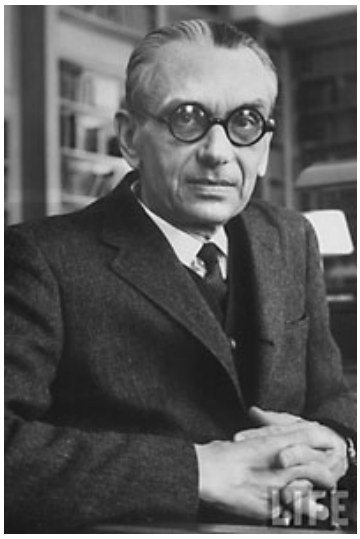


Figura 4 – Kurt Gödel em 1962 - Os limites de prova dos sistemas formais.

Fonte: www.qotd.org.

Em 1937, o engenheiro americano **Claude Shannon** utilizou as teorias da Álgebra de Boole para a solução de problemas de circuitos de telefonia com relés, tendo publicado um trabalho denominado "*Symbolic Analysis of Relay and Switching*", praticamente introduzindo na área tecnológica o campo da eletrônica digital. Esse ramo da eletrônica emprega em seus sistemas um pequeno grupo de circuitos básicos padronizados conhecidos como *portas lógicas*. Portas lógicas ou circuitos lógicos, são dispositivos que operam um ou mais sinais lógicos de entrada para produzir uma e somente uma saída, dependente da função implementada no circuito. São geralmente usadas em circuitos eletrônicos, por causa das situações que os sinais deste tipo de circuito podem apresentar: presença de sinal ("1"); e ausência de sinal ("0"). As situações "Verdade"e "Falso"são estudadas na lógica em que Boole transformou em Álgebra. O comportamento das portas lógicas é conhecido pela *tabelas-verdade*, criadas por **Emil Post** (aquelas que estudamos no primeiro curso de lógica proposicional) que apresentam os estados lógicos das entradas e das saídas dos circuitos lógicos.

Konrad Zuse (1910-1995), um engenheiro alemão (Figura 5), no período de 1935-1940, levara a ideia de máquina programável de **Turing** à frente. A sua terceira versão de máquina, o Z3, foi finalizado em 1941. Ela era baseada em relés telefônicos e funcionou satisfatoriamente. A troca do sistema decimal, mais difícil de implementar (utilizado no projeto de **Charles Babbage**) pelo simples sistema binário tornou a máquina de **Zuse** mais fácil de construir e potencialmente mais confiável, com a tecnologia disponível naquele tempo. O Z3 passou a ser o primeiro computador programável funcionando. Em vários aspectos ele era muito semelhante às máquinas modernas, sendo pioneiro em vários avanços, como o uso de aritmética binária e números de ponto flutuante. Os programas eram armazenados no Z3 em filmes perfurados. Desvios condicionais não existiam, mas o Z3 ainda era um computador universal (ignorando sua limitação no seu espaço de armazenamento físico). Em

duas patentes de 1937, **Konrad Zuse** antecipou que as instruções da máquina poderiam ser armazenadas no mesmo espaço de armazenamento utilizado para os dados, a primeira idéia do que viria a ser conhecida como a *arquitetura de* ***John Von Neumann*** e que seria implementada no projeto do EDSAC britânico (1949). **Zuse** ainda projetou a primeira linguagem de alto nível, em 1945, chamada de *Plankalkül*.

Figura 5 – Konrad Zuse - O primeiro computador programável com sistema binário e arquitetura de von Neumann.

Fonte: www.dsc.ufcg.edu.br.

Desde a exposição dos limites fundamentais de prova e computação de **Gödel**, e posterior construção de **Konrad Zuse** do primeiro computador programável (1935-1941), tem havido uma série de trabalhos sobre algoritmos especializados resolvendo classes de problemas. A Lógica é extensivamente utilizada em todas as áreas vinculadas aos computadores. No século XX, entre as décadas de 30 a 60, a partir da ideia de **Turing** sobre a inteligência em máquinas, pesquisadores previram que quando o conhecimento humano pudesse ser expresso usando Lógica, seria possível criar uma máquina com a capacidade de pensar, ou seja, com *Inteligência Artificial*. Isto se mostrou mais difícil que o esperado em função da complexidade do raciocínio humano. Entretanto, com a lógica simbólica, demonstrações feitas por humanos podem ser auxiliadas por computador. Usando prova automática de teoremas, os computadores podem conduzir demonstrações. No capítulo 7 o leitor poderá conhecer mais detalhes, desde o advento da lógica, até a apresentação das lógicas mais utilizadas em sistemas de computação.

1.7 Para os nossos Propósitos ...

Das matemáticas e lógicas aqui mencionadas, além desta introdução (1) As Bases da Ciência da Computação, focalizaremos (2) As Origens: A Aritmética, (3) Os Números, (4) Os Números Primos, (5) Congruência e Aritmética Modular, (6) Álgebra na Europa (7) A Lógica: de Leibniz à Boole, (8) Século XIX: Frege e a Lógica dos Predicados, (9) A Teoria dos Conjuntos, (10) Relações e Funções, (11) Grupos e

Corpos (12) Conjuntos e Enumeração, (13) A Aritmética nos Séculos XIX e XX, (14) Hilbert - Formalismo e os Sistemas Axiomáticos, (15) Gödel e os Limites dos Sistemas Formais, (16) Dos Fundamentos da Matemática aos Sistemas Formais, e finalizando, (17) Os Sistemas Formais da Computação.

1.8 Bibliografia e Fonte de Consulta

Dirk J. Struik - História Concisa das Matemáticas, Ed. Gradiva, 1987.

Roland Omnès - Filosofia da Ciência Contemporânea, Editora UNESP, ISBN 85-7139-120-3, 1996.

Biografia de Georg Cantor - http://www-groups.dcs.st-and.ac.uk/ history/Biographies/-Cantor.html

Bigrafia de Bertrand Russel - ⟨http://www-history.mcs.st-and.ac.uk/Biographies/Russell.html⟩

Aristóteles - ⟨https://pt.wikipedia.org/wiki/Aristoteles⟩

Silogismo - ⟨https://pt.wikipedia.org/wiki/Silogismo⟩

Lógica - ⟨https://pt.wikipedia.org/wiki/Logica⟩

Biografia de Church - http://www-groups.dcs.st-and.ac.uk/ history/Biographies/Church.html

Portas Lógicas - ⟨https://pt.wikipedia.org/wiki/Porta_logica⟩

História do Hardware - https://pt.wikipedia.org/wiki/História_do_hardware

Konrad Zuse - ⟨http://people.idsia.ch/~juergen/zuse.html⟩

Kurt Gödel - ⟨http://people.idsia.ch/~juergen/goedel.html⟩

Julius Edgar Lilienfeld - http://www.circuitstoday.com/the-story-history-of-transistor-invention

Julius Edgar Lilienfeld - https://en.wikipedia.org/wiki/Julius$_E dgar_L ilienfeld$

1.9 Referências e Leitura Recomendada

Epstein, R. L, Carnielli W. A. - Computability: Computable Functions, Logic and the Foudations of Mathematics, Wadsworth & Brooks/Cole. Mathematics Series.

1989.

W. K. C. Guthrie (1990). "A history of Greek philosophy: Aristotle : an encounter". Cambridge University Press. p.156. ISBN 0-521-38760-4.

Popkin, Richard Henry; Stroll, Avrum. Philosophy Made Simple. [S.l.]: Random House Digital, Inc, 1993. ISBN 978-0-385-42533-9.

Cox, J. Robert; Willard, Charles Arthur. Advances in Argumentation Theory and Research. Southern Illinois University Press, 1983.

Martyn Oliver. História ilustrada da filosofia. [S.l.]: Manole, 1998. p. 20. ISBN 978-85-204-0820-9.

Bryan Magee. Historia de la filosofía. [S.l.]: lume, 1999. p. 32. ISBN 978-85-15-01929-8.

Cezar A. Mortari. Introdução à lógica. [S.l.]: Comped, 2001. p. 28. ISBN 978-85-7139-337-0.

Fisher, Alec. A Lógica dos Verdadeiros Argumentos. Novo Conceito, 1a edição 2008, 336p. ISBN 85-99560-29-8.

Souza, João Nunes de. Lógica para Ciência da Computação. Campus, 2a edição 2008, 240p. ISBN 85-352-2961-2.

Pinto, Paulo Roberto Margutti. Introdução à Lógica Simbólica. UFMG 2a edição 2006 339p. ISBN 85-7041-215-0.

Gorsky, Samir. A semântica algébrica para a lógica modal e seu interesse filosófico. Dissertação de mestrado. IFCH-UNICAMP. 2008.

Finger, Marcelo; Silva, Flávio Soares Corrêa da; Melo, Ana Cristina Vieira de. Lógica para Computação. Thomson Pioneira, 1a edição 2006, 244p. ISBN 85-221-0517-0.

Copi, I., Cohen, C. - Introduction to logic. 8 ed. New York: Macmillan Publishing Company, 1990. 569 p. p. 45-46. ISBN 0-02-946192-8.

McCarthy, John; Abrahams, Paul W.; Edwards, Daniel J.; Hart, Timothy P.; Levin, Michael I. Lisp 1.5 Programmer´s Manual. Cambridge, Massachusetts: The MIT Press, 1962. 106 p. p. 1. ISBN 0-262-13011-4

Whitehead, Alfred North Russell, Bertrand: Principia Mathematica. 3 vols, Merchant Books, 2001, ISBN 978-1603861823 (vol. 1), ISBN 978-1603861830 (vol. 2), ISBN

978-1603861847 (vol. 3)

Russell, Bertrand (1919), Introduction to Mathematical Philosophy, George Allen and Unwin, London, UK. Reimpressão, John G. Slater (intro.), Routledge, London, UK, 1993

CAPÍTULO 2

As Origens - A Aritmética

Este capítulo diz respeito a aritmética, a área mais antiga e mais elementar da Matemática. Os primeiros registros escritos indicam que os egípcios e babilônios usavam todas as operações aritméticas elementares. O termo aritmética também é usado em referência à teoria dos números. É neste contexto que se pode encontrar o teorema fundamental da aritmética e funções aritméticas. Na Idade Média, a aritmética era uma das artes liberais ensinadas nas universidades.

2.1 As Origens

O *período paleolítico* diz respeito aos fatos históricos da humanidade há aproximadamente 15 milênios atrás, 15000 a.C. O *período neolítico* - na pré-história europeia, portanto, não se aplicando à pré-história americana (incluindo o Brasil), Neolítico (pedra nova) ou Período da Pedra Polida é o nome do período que vai aproximadamente do décimo milênio a.C., com o início da sedentarização e surgimento da agricultura, ao terceiro milênio a.C.(3000 a.C.), dando lugar à Idade dos Metais. Na antropologia evolucionária, sedentarização é um termo aplicado à transição cultural da colonização nômade para a permanente. Na transição para o sedentarismo, as populações semi-nômades possuíam um acampamento fixo para a parte sedentária do ano. O sedentarismo se tornou possível com novas técnicas agrícolas e pecuárias. O desenvolvimento do sedentarismo aumentou a agregação populacional e levou à formação de vilas, cidades e outras formas de comunidades.

As nossas primeiras concepções de **número** e **forma** datam de tempos tão remotos como os do começo da idade da pedra, o período **neolítico**. Durante este período, os homens viviam em cavernas, em condições pouco diferentes das dos animais, e as suas principais atividades eram orientadas para o recolhimento de alimentos onde fosse possível encontrá-los. Eles faziam instrumentos para caçar e pescar, desenvolviam a linguagem para comunicar uns com os outros. Com o desenvolvimento da *linguagem* e com o uso da palavra, tal *percepção quantitativa* aumentou tanto, e chegou a tal nível de sofisticação que permitiu a determinadas

culturas dar o nome a imensidades das coisas, e nos últimos tempos do **paleolítico** enriqueceram suas habitações com certas formas de arte, como estatuetas e pinturas. As pinturas em cavernas já revelavam a compreensão da forma; matematicamente falando, revelavam uma compreensão da descrição bidimensional dos objetos no espaço Struik (1987).

Poucos progressos ocorreram no conhecimento de valores numéricos e de relações espaciais até se dar a transição da era da atividade do recolhimento de alimentos para a sua produção, da caça e da pesca para a agricultura. Com esta transformação, uma revolução na qual a atitude do homen perante a natureza deixou de ser passiva para ser ativa - inicia-se um novo período da idade da pedra, o período **neolítico** Struik (1987).

2.2 Período Neolítico

Neolítico (pedra nova) é o nome do período que vai aproximadamente do décimo milênio a.C.(9000 a.C), com o surgimento da agricultura, a aproximadamente o quarto milênio (4000 a.C.): o grande acontecimento na história da humanidade. Os nômades que vagavam a procura de alimentos foram desaparecendo, os caçadores e pescadores foram sendo substituídos por agricultores (entre 6000-5000 a.C. invenção do arado). Esses se fixavam num local enquanto o solo se mantivesse fértil, construíram habitações mais permanentes, surgindo assim as povoações. Neste período já faziam o pão, fermentavam a cerveja, e nos últimos tempos do neolítico, preparavam e fundiam o cobre e o bronze. Inventaram a roda e aperfeiçoaram os barcos e os abrigos. Esta invenções deram-se somente em certas regiões. Quando comparado o neolítico com o período paleolítico, o ritmo de aperfeiçoamento técnico foi muito mais acelerado Struik (1987).

Durante o **neolítico**, surgiu a atividade considerável de troca de objetos, quando, provavelmente, deu-se início ao comércio primitivo entre as diversas povoações, quando foram estabelecidas as ligações entre localidades afastadas algumas centenas de quilômetros. A descoberta de técnicas de fundição e de manufatura, primeiro de cobre e depois de utensílios de bronze, estimulou fortemente as primeiras atividades de comércio primitivo. Falar, no período **neolítico**, também era uma atividade presente em todos os povos em todas as épocas. Isto também promoveu a formação de linguagens . As palavras dessas linguagens exprimiam coisas bem concretas e pouco abstratas, mas já havia lugar para termos numéricos simples e algumas relações de forma.

Os termos numéricos , lentamente começaram a ser usados. A percepção de quantidade pelo homem primitivo era praticamente intuitiva. As primeiras ocorrências de contagem faziam a distinção entre um, dois e muitos. A partir de um grupo de três ou quatro objetos, o homem dizia simplesmente que havia muitos objetos nesse grupo. Quando o conceito de número foi-se ampliando, os números maiores foram,

primeiro, formados por adição: adicionando um e dois dava três; adicionando dois e dois dava quatro; adicionando dois e três dava cinco Struik (1987).

O desenvolvimento das atividades do **comércio primitivo** estimulou o conceito de número . Os números foram ordenados e agrupados em unidades cada vez maiores. Os registros numéricos eram conservados por meio de agrupamentos em entalhes de madeira, nodos de corda ou conchas, em grupos de cinco. Deste método à utilização de símbolos especiais para cinco, dez, vinte, ..., foi apenas um passo e vamos encontrar exatamente tais símbolos no início da história da escrita Struik (1987).

A percepção de noções primitivas como a diferença entre um círculo e uma reta, entre um animal e um rebanho, uma árvore e uma floresta, fazem parte das primeiras noções de números, formas e quantidades diferentes percebidas. Mesmo sem conhecer um **sistema numérico**, o homem primitivo tinha uma ideia nítida e clara, para indicar uma quantidade de dois, três, quatro ou cinco elementos, porque dispunha de cinco dedos em uma mão, dez dedos nas duas mãos ou vinte dedos nas mãos e nos pés. Isto conduziu à numeração de base cinco e mais tarde a de base dez, completada com a adição e, por vezes, a subtração. Assim, doze era considerado dez mais dois, e nove como dez subtraído de um Contador (2008).

Contar pelos dedos, ou seja, contar de cinco em cinco, e dez em dez, surgiu apenas, numa fase do desenvolvimento social. Quando se alcançou essa fase, os números passaram a exprimir-se em uma base, com a ajuda da qual podem ser formados números maiores. Para contar, quando os dedos das mãos e dos pés não eram suficientes, amontoavam-se pedras em grupos de cinco, ou marcações em ossos, bastões, para registrar um determinado número. Foi desta maneira que surgiu uma aritmética de tipo primitivo. O número quatorze, por exemplo, exprimia-se por adicionar “dez mais quatro”, ou algumas vezes subtraindo “quinze menos um”. A multiplicação começou quando vinte se exprimiu não como ”dez mais dez”, mas como ”duas vezes dez”. Tais operações de dois operandos (**diádicas**) foram usadas durante milhares de anos como uma espécie de meio caminho entre adição e multiplicação, especialmente no Egito e na civilização Indu (Índia). A divisão começou quando se exprimiu dez como metade de vinte, embora a formação consciente de frações permanecesse bastante rara. Um fenômeno curioso era a o gosto pelos números grandes, que podia ser explicado pela tendência que o homem primitivo tinha para exagerar em determinadas contagens Struik (1987).

A quantidade **dez** foi adotada com o passar do tempo e a partir da percepção de sua própria anatomia, o homem deu o passo fundamental e muitas civilizações desenvolveram um sistema numérico próprio, apesar da distância e do tempo entre elas. Assim, **não é possível datar exatamente, o surgimento da aritmética**, a primeira área da matemática a ser desenvolvida, pois **contar** era uma atividade presente em todos os povos e em todas as épocas. A palavra *Aritmética* vem da palavra grega *arithmetike*, que se compõe de *arithmos* (número) e de *techne* (ciência), resultando assim, na ciência dos números (números e suas operações).

Tornou-se também necessário medir o comprimento ou volume de certos objetos. Os padrões eram grosseiros e muitas vezes provinham de partes do corpo humano, o que deu origem a unidades de medida, como dedo, a mão e o pé. Os nomes "vara", "braça" e "cúbito" recordam este costume. Quando se contruiam casas, as dos agricultores indianos e dos habitantes da Europa central, estabeleciam-se regras para a construção ser feita segundo linhas retas e ângulos retos. A palavra "reta" se relaciona com "esticar" uma corda; a palavra "linha" relaciona-se com "linho", o que mostra alguma ligação entre a tecelagem e as origens da geometria. Este foi um dos modos pelos quais o interesse pela medição se desenvolveu no período **neolítico**.

O homem do **neolítico** também revelou um sentido para os **padrões geométricos**. A cozedura e a pintura de cerâmica, o entrelaçamento de juncos, a tecelagem de cestos e têxteis, a fabricação de metais conduziram à noção de plano e relações espaciais. A ornamentação neolítica mostra a **manisfestação da congruência**, da **simetria**, e da **semelhança** (similaridade). Nestas formas ocorreram as **relações numéricas** com **padrões pré-históricos**. Tais padrões constituem exemplos de padrões geométricos utilizados na cerâmica, na tecelagem e na cestaria.

Esses padrões ficaram populares através da história: nos primeiros períodos da Grécia, nos mozaicos bizantinos e árabes, e na tapeçaria persa e chinesa. Alguns autores consideram que este aspecto da matemática foi um fator determinante do seu desenvolvimento Struik (1987). Embora, as raízes sociais da matemática fossem mais evidentes nos tempos primitivos da história da humanidade, e mais obscuros nos tempos modernos.

Nos povos com uma estrutura social bem distante da nossa civilização técnica, encontramos registros do tempo e, relacionados com ele, conhecimentos dos movimentos do sol, da Lua e das estrelas. Com o desenvolvimento da agricultura e do comércio, tal conhecimento atingiu pela primeira vez um caráter científico. O uso do calendário lunar teve origem muita antiga na história da humanidade e está ligado às variações da vegetação com as fases da Lua. Os povos primitivos mais antigos registros já atribuiam conhecimentos astronômicos nos períodos pré-históricos mais remotos. Dessa astronomia resultaram alguns conhecimentos sobre as propriedades da esfera, das direções angulares, dos círculos e mesmo de figuras mais complicadas. Termina o período **neolítico**, inicia-se a era dos metais (bronze). A Idade do Bronze é um período da civilização no qual ocorreu o desenvolvimento desta liga metálica, resultante da mistura de cobre com estanho. Iniciou-se no Oriente Médio em torno de 3300 a.C, substituindo diretamente o período **neolítico** (popularmente conhecida como Idade da Pedra), até 1500 a.C.

2.3 O Desenvolvimento da Aritmética

A *aritmética* (da palavra grega *arithmós*, que significa "número" é o ramo da matemática que lida com números e com as operações possíveis entre eles Davenport (1999). É o ramo mais antigo e mais elementar da matemática, usado por quase todos nós, seja em tarefas do cotidiano, em cálculos de negócios ou cálculos científicos. Resumidamente são as quatro mais simples operações matemáticas, ou seja, **adição**, **subtração**, **multiplicação** e **divisão**, que formam a **aritmética elementar**. Originariamente, as operações de **adição** e **subtração** eram feitas através do **ábaco**.

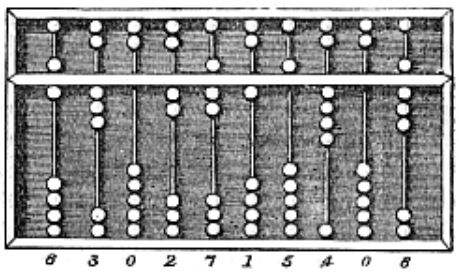


Figura 6 – O ábaco primitivo - Primeira calculadora utilizada pelo homem: representando o número 6302715408.

Fonte: http://pt.wikipedia.org/wiki/Ábaco.

Como uma extensão do ato natural de se contar nos dedos, o **ábaco** é um antigo instrumento de cálculo, que segundo muitos historiadores foi inventado em sua forma primitiva, na região da Mesopotâmia, onde vários povos antigos habitaram essa região entre os séculos V e I a.C. Entre esses povos antigos estavam: babilônios, assírios, sumérios, caldeus, amoritas e acádios. Os babilônios foram os primeiros a usar o ábaco mais primitivo. Desde então, uma variedade de ábacos foram desenvolvidos pelos egípcios, gregos, romanos, indianos, chinêses e japonêses, nativos americanos e russos, até se chegar a um ábaco escolar do século XIX.

Desde sua forma original, o **ábaco** é, basicamente, formado por uma moldura com bastões ou arames paralelos, dispostos no sentido vertical, correspondentes cada um a uma posição digital (unidades, dezenas, centenas, ...) e nos quais estão os elementos de contagem (bolas, contas,...) que podem fazer-se deslizar livremente, e um processo de cálculo com sistema decimal, atribuindo a cada haste um múltiplo de dez, pode ser utilizado ainda hoje para ensinar às crianças as operações de somar e subtrair.

2.4 Oriente Antigo - A Matemática Egípcia

O Oriente Antigo é o termo utilizado para denominar a região de onde apareceram as civilizações anteriores às clássicas, na região que atualmente se denomina Oriente Médio (Iraque, parte do Irã, parte da Turquia, Síria, Líbano, Israel, Egito) no período

que vai desde a Idade do Bronze (início em 3300 a.C.) chegando até à expansão dos Persas (2000 a.C-1500 a.C.). A área geográfica do Oriente Antigo: (a) **Mesopotâmia**: inclui os modernos estados de Iraque e Irã; **Levante**: inclui os modernos estados de Israel, Jordânia, Líbano, Síria e os Territórios ocupados Palestinos; (c) **Anatólia**: inclui a parte asiática do moderno estado de Turquia; **Egito**: área atual , mas com as intensas relações políticas, econômicas e culturais mantidas com toda a área chamado Oriente Antigo, a partir de 2000 a.C.

No oriente antigo, a civilização egípcia, um povo que emergiu lentamente das condições **neolíticas**, se aglutinou em torno de 3150 a.C. com a unificação política do Alto e do Baixo Egito, e se desenvolveu ao longo dos três milênios seguintes, às matgens do Rio Nilo. A descoberta do papiro (do grego Pápyros, vegetal característico das margens alagadiças do Rio Nilo, que de suas longas folhas obtinha-se o papiro, material sobre o qual se escrevia), fez surgir, assim, a palavra papel, pelos egípcios. A maior parte do conhecimento da matemática egípcia deriva de dois papiros: o chamado *Papiro de Moscovo*, dois séculos mais antigo, com 25 problemas, do que o *Papiro de Rhind*, com 85 problemas. Esta matemática baseava-se no **sistema de numeração decimal**, com sinais especiais para cada unidade mais elevada. Na base deste sistema, os egípcios desenvolveram uma aritmética de carater predominantemente aditivo, o que significa que o seu principal objetivo era reduzir multiplicações a adições sucessivas. Surge o primeiro sistema de numeração (os hieróglifos egípcios), tal como no Egito (3000 a.C).

O sistema de numeração egípcio - O primeiro sistema de escrita numérica mais antigo que se conhece é o dos egípcios. Os egípcios usavam um sistema de agrupamento simples, com base 10, com símbolos especiais para 1, 10, 100, 1000, ... e de uma forma aditiva. Os egípcios usavam hieróglifos, como mostrados na Figura 7. Os símbolos numéricos egípcios eram baseados no **sistema de numeração decimal**, com sinais especiais para cada unidade mais elevada. Na base deste sistema, os egípcios desenvolveram uma aritmética de caráter predominantemente aditivo, o que significa que o seu principal objetivo era reduzir multiplicações a adições sucessivas.

O aspecto mais notável da aritmética egípcia é o seu cálculo de frações. Todas as frações eram reduzidas a frações unitárias (de numerador 1). Eram indicadas pelo denominador com um símbolo do numerador. As únicas exceções eram 1/2 e 2/3, para as quais existiam símbolos especiais. A redução a somas de frações unitárias, era possível através de tabelas, que davam a decomposição de frações da forma $2/n$ - a única decomposição necessária por causa da multiplicação diádica. O *Papiro de Rhind* tem uma tabela que dá as equivalências em frações unitárias para todos os números ímpares entre 5 e 101. O princípio subjacente a esta redução a frações unitárias não é claro: por exemplo, porque é que, quando $n = 19$, a redução é $(1/12 + 1/76 + 1/114)$ e não $(1/12 + 1/57 + 1/228)$? Este cálculo com frações deu à matemática egípcia um carater complicado. Mas, a maneira de operar com frações unitárias foi praticada durante milhares de anos, no período grego e na Idade Média.

Classe	Número decimal	Hieróglifo egípcio	Significado
Unidade	1		Haste/Bastão
Dezena	10		Arco de cesto/Calcanhar
Centena	100		Pergaminho/Rolo de corda
Milhar	1.000		Flor de lótus
Dez milhares	10.000		Dedo dobrado
Cem milhares	100.000		Girino/Sapo/Peixe
Milhão	1.000.000		Deus acocorado/Homem espantado

Figura 7 – Os egípcios usavam hieróglifos para representar números em base 10.

Fonte: obaricentrodamente.blogspot.com/2015/02/a-multiplicacao-egipcia.html.

A decomposição pressupunha alguma perícia matemática. No *Papiro de Rhindi*, encontrou-se 2/7 representado pela soma $1/4 + 1/28$, 2/7 por $1/56 + 1/776$, 2/99 por $1/66 + 1/198$. Há teorias interessantes para explicar os métodos egípcios nas decomposições de uma fração em uma soma de frações unitárias. Muitos problemas eram simples e não iam além de equações lineares com uma incógnita. Por exemplo: a soma de $(2/3 + 1/2 + 1/7)$ de uma quantidade x com ela própria dá 33. Qual é a quantidade x ? Resposta: 141/41/971/561/6791/7761/1941/388. Hoje escrevemos: 1428/97. Para a incógnita de uma equação egípcia existia um *hieróglifo*.

Os problemas, relacionados com a qualidade do pão e de diferentes tipos de cerveja, com a alimentação dos animais, e o armazenamento do trigo, mostram a origem prática desta aritmética pouco cômoda e desta álgebra primitiva. Alguns problemas revelam o conhecimento de uma progressão aritmética e de progressão geométrica. Alguns problemas tinham natureza geométrica, relacionada com a medição. A área do triângulo era dada pela metade do produto da base pela altura; a área do cículo de diâmetro d era dada por $(d - d/9) * *2$ o que conduzia a um a valor de π de $256/81 = 3,1605$. Existiam também fórmulas para volumes sólidos, como o cubo, o paralelepípedo e o cilindro circular, todos concebidos como recipientes, principalmente sementes. O mais notável da medição egípcia foi a fórmula do valor do volume de uma pirâmide quadrangular truncada paralelamente à base: $V = (h/3)(a**2 + ab + b**2)$, onde a e b são os lados dos quadrados e h é a altura. Este resultado, de que ainda, não foi encontrado um equivalente em outras formas de matemática antiga, é tanto mais notável quanto é certo de que os egícios não tinham qualquer conhecimento do teorema de Pitágoras. Todas as formas de desenvolvimento científico foram atribuidas aos construtores de pirâmides de aproximadamente (3000 a.C.). Mas, todos os textos

disponiveis evidenciam uma matemática egípcia de objetivos muito limitados, embora com alguma sofisticação dentros desses limites Struik (1987).

2.5 Oriente Antigo - Os Sumérios na Mesopotâmia

Figura 8 – Área geográfica do Oriente Antigo.

Fonte: 2013 Encyclopedia Britannica Inc.

As matemáticas orientais surgiram como uma ciência prática com o objetivo do cálculo do calendário, a administração das colheitas. A ênfase inicial foi dada naturalmente à aritmética prática e à medição. Porém, uma ciência cultivada durantes séculos, cuja tarefa não é apenas aplicar, desenvolveu tendências para a **abstração**. E a **aritmética se transformou em álgebra**, porque possibilitava melhores cálculos práticos. Pelas mesmas razões, a medição deu origem aos começos da **geometria teórica**.

Sumérios viviam como nômades vagando pelo Planalto do Irã e no alto dos Montes Zagros. Provavelmente por falta de comida e água, por volta de 3500 a.C., os sumérios saíram das montanhas da Ásia Central à procura de terras férteis e chegaram ao sul da Mesopotâmia. Os Sumérios foram o primeiro povo a habitar a região da Mesopotâmia, compreendida entre os rios Tigre e Eufrates (atula Iraque). Por ser uma região com poucas chuvas, desde muito cedo os sumérios tiveram de aprender a desviar e armazenar as águas do Tigre e do Eufrates, e com isso puderam cultivar uma grande quantidade e variedade de alimentos. Com o tempo foram constituindo cidades. São as primeiras civilizações baseados nos povos que construíram e viveram em cidades. As primeiras cidades surgiram no Oriente e a primeira delas foi Uruk, por volta de 3200 a.C. Hoje essa cidade é Warka e fica no Iraque. A civilização **suméria** era composta por diversas cidades e possivelmente Uruk era a maior delas, mas todas eram bastante desenvolvidas para a época.

Atribui-se aos **sumérios**, a **invenção da escrita cuneiforme** na Mesopotâmia. Os **sumérios** escreviam em táboas feitas de argila, usando um estilete de extremidade triangular que deixava sinais em forma de cunha. Com isso, a escrita recebeu o nome

de **escrita cuneiforme**. Os **sumérios** constituiram uma civilização fantástica para a humanidade. A eles são atribuidos a invenção da roda e criação da história. A prova mais antiga do uso da roda, data de cerca de 3500 a.C., e vem de um esboço em uma placa de argila encontrada na região da antiga Suméria, na Mesopotâmia (atual Iraque), mas é provavel que sua utilização venha de períodos muito mais remotos.

As matemáticas mesopotâmicas atingiram um nível mais elevado do que as matemáticas egípcias Struik (1987). Na Mesopotâmia podemos identificar um certo progresso no decorrer dos séculos. Os textos mais antigos, datados do terceito milênio (2100 a.C) revelam uma grande habilidade para calcular. Esses textos contém tábuas de multiplicação nas quais um **sistema de numeração sexagegimal** bem desenvolvido se sobrepõe ao sistema decimal. Existiam símbolos cuneiformes Leite (2014) que indicavam 1, 60, 3600 e também $(60 * *(-1) = (1/60))$, $(60 * *(-2) = (1/(60 * *2)))$. Enquanto os egípcios indicavam cada unidade mais elevada, através de um símbolo, os sumérios usavam o mesmo símbolo, mas indicavam o seu valor pela sua posição. Assim, 1 seguindo outro 1 significava 61 e 5 seguido por 6 e por 3, devíamos escrever $(5, 6, 3)$ significava $(5 * 60 * *2 + 6 * 60 * *1 + 3 = 18363)$. Isto fez surgir os sistemas de numeração posicional. Tal sistema tinha vantagem enorme para o cálculo. O sistema de posição eliminou muitas das dificuldades da aritmética fracionária, tal como o sistema decimal o faz em relação à escrita de frações.

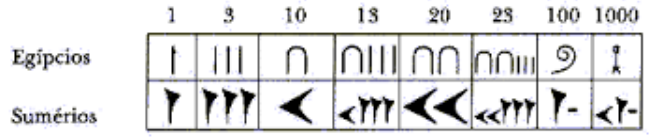


Figura 9 – Comparando algarismos egipcios e sumérios.

Fonte: matematica.br.

Na matemática **suméria**, existiam algumas ambiguidades no tipo de cálculo. O significado exato de cada símbolo nem sempre era claro em função de sua posição, a interpretação exata dependia do contexto. Também, a princípio eles não tinham um modo claro de indicar a opção "vazia" ou nula, que conhecemos hoje como o zero, as vezes deixavam de fato um espaço vazio o que gerava muita ambiguidade. Posteriormente apareceu um símbolo especial para representar o "vazio", representando o zero. A invenção do zero era um resultado lógico do sistema de posição. Também, a nossa divisão atual das horas em 60 minutos e em 3600 segundos, assim como a divisão do círculo em 360 graus data dos **sumérios** Struik (1987).

2.6 O Oriente Antigo - A Matemática Babilônica

Por volta de 1900 a.C. (século XX a.C.), um novo processo de invasão territorial dizimou a dominação dos **sumérios** na região Mesopotâmica. Dessa vez, os **amoritas**, povo oriundo da região sul do deserto árabe, fundaram uma nova civilização que tinha a **Babilônia** como sua cidade principal. A matemática babilônica se refere a

qualquer forma de matemática desenvolvida pelos povos da Mesopotâmia, desde os dias dos antigos **sumérios** até a queda da Babilônia em 539 a.C.

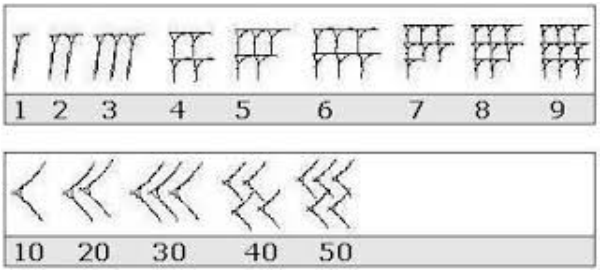


Figura 10 – Sistema de Numeração babilônico - Base 10, aditivo, numeração até 60, e posicional para números superiores.

Fonte: es.slideshare.net.

Nos textos desta época, encontramos **a aritmética transformada numa álgebra** já bem estabelecida. Embora os egípcios deste período fossem somente capazes de resolver equações simples (hoje, chamadas lineares), os babilônios da época de Hamurábi, já tinham a capacidade para manipular equações quadráticas. Resolviam as lineares e as quadráticas com duas variáveis, e até mesmo problemas com equações cúbicas e biquadráticas. Embora conhecessem a regra geral, formulavam os problemas apenas com valores numéricos específicos para os coeficientes. Ver exemplo em Struik (1987) (p.58).

O forte caráter aritmético-algébrico da matemática babilônica transparece também na geometria. Tal como no Egito, a geometria veio da fundamentação de problemas práticos relacionados com a medição, mas a forma geométrica de um problema era usualmente uma maneira de apresentar uma questão algébrica. o conhecimento sobre a matemática babilônica é derivado de 400 tábuas de argila. Gravadas em escrita cuneiforme (escrita dos **Sumérios**), as tábuas eram escritas quando a argila ainda estava úmida, e depois cozinhadas em fornos ou sob o calor do sol. A maioria das tábuas de argila datam de 1800 a.C até 1600 a.C, e cobre tópicos a quais incluem frações, álgebra, equações quadráticas e equações cúbicas além da ideias que reduda-ram na Grécia no século V a.C, sobre o teorema de Pitágoras. Assim, a matemática babilônica se manteve constante, em seu conteúdo por cerca de quase dois milênios (2000 anos).

A geometria babilônica se relaciona intimamente com a mensuração prática. A principal marca da geometria babilônica era seu caráter algébrico. A aritmética babilônica já havia evoluído para uma álgebra bem desenvolvida, já se resolviam equações quadráticas e já se discutiam algumas cúbicas e também biquadradas. Também foram encontrados problema interessantes sobre sequências numa tábua, datando por volta de 300 a.C., afirmando que:

$$1 + 2 + 2^2 + 2^3 + ... + 2^9 = 2^9 + 2^9 - 1$$

e outro diz que:

$1^2 + 2^2 + 3^2 + ... + 10^2 = [1.(\frac{1}{3}) + 10(\frac{2}{3})].55 = 385$

Os babilônios também deram aproximações interessantes, como de $\sqrt{2} = 1 + 24/60 + (51/60)^2 + (10/60)^3 = 1,4142155$ e de $\frac{1}{\sqrt{2}} = 17/24$.

2.7 A Matemática Grega

Egípcios, babilônicos e chineses, muito antes do século VI a.C. (anos 600 a.C), já eram já capazes de efetuar cálculos e medidas de ordem prática com grande precisão. Foram os gregos, no entanto, que introduziram o **método axiomático**: as rigorosas provas dedutivas e o encadeamento sistemático de teoremas demonstrativos que tornaram a Matemática uma Ciência.

A matemática grega clássica (matemática da Grécia Antiga) é o nome dado à matemática escrita em grego, desde 600 a.C. (época em que viveu Tales de Mileto) até o fechamento da Academia de Platão em 529 d.C.

A palavra "matemática", que é de origem grega, englobava o que hoje se chama de **aritmética** e **geometria**. Até o século VI a.C. a matemática grega não se destacava. Havia, como em outras civilizações da época, técnicas de contagem e medição. No século VI a.C. iniciam-se as duas escolas de pensamentos na Grécia antiga - A escola *jônica* (**Tales de Mileto**) e a escola *pitagórica* (**Pitágoras de Samos**). Os pitagóricos a dividiam em: aritmética, geometria, astronomia, e música. Na concepção de Aristóteles, apenas a aritmética e a geometria, as duas áreas teóricas que mais atraíram os gregos antigos, eram consideradas ciências puramente matemáticas.

A Matemática como uma ciência nasceu na Grécia Antiga. A Matemática nasceu na atmosfera do racionalismo *jônico*: uma matemática que colocava não só a questão "como", mas também o "porque"científico. Característica dessa fase era que os gregos verificavam a validade de suas teses nas áreas que abordavam: astronomia, óptica, música, geometria, e mais tarde, a mecânica, por meio de **modelos matemáticos**, o que lhes conferia poder de fazer previsões. Ao mesmo tempo, os gregos criaram a **metodologia matemática**. A base neste sistema, pela primeira vez tornou-se o **método dedutivo**, mostrando como apoiando-se sobre verdades bem conhecidas (axiomas), por meio do correto uso da Lógica aristotélica garante-se a verdade dos novos resultados, as conclusões (teoremas). As realizações dos matemáticos gregos são conhecidas, principalmente, pelos trabalhos de **Platão**, **Tales de Mileto**, **Pitágoras**, **Euclides** e **Aristóteles**. Tradicionalmente, o pai da Matemática grega é **Tales de Mileto**. A sua figura simboliza as circunstâncias sob as quais foram estabelecidos os fundamentos não só da matemática, mas também da ciência e da filosofia. Como matemático, **Tales de Mileto** fez surgir a geometria.

Os fatos geométricos muito conhecidos por nós, tem suas demonstrações atribuídas a Tales de Mileto.

Hipócrates de Quios (470 a.C-410 a.C) (não confundir com o médico, pai da medicina, Hipócrates de Cós, aproximadamante da mesma época) mostrou que os matemáticos gregos possuiam um sistema ordenado de geometria plana, em que o princípio da dedução lógica, que permitia deduzir uma afirmação a partir de outra, tinha sido inteiramente aceita. Era o início da *axiomática*, surgida em *Os Elementos*, título de todos os tratados axiomáticos gregos, incluindo o de **Euclides**. **Hipócrates** investigou as áreas das figuras planas delimitadas por retas ou por arcos circulares. A sua obra precede *Euclides*, e já se situava no que se chamava de tradição euclidiana.

O problema da *quadratura do círculo* (encontrar um quadrado de área igual à de um círculo dado), constituia um problema central na matemática grega; a *trisecção do ângulo* (dividir um ângulo dado em três partes iguais); a *duplicação do cubo* (encontrar o lado do cubo do qual o volume é o dobro do volume de um cubo dado), eram os três famosos problemas matemáticos da antiguidade. A importância destes três problemas consistia no fato de eles não podiam ser resolvidos geometricamente pela construção de um número finito de linhas retas e círculos, senão pela aproximação, constituindo um meio de alcançar novos campos da matemática.

Contemporâneo de Tales de Mileto, **Pitágoras de Samos** (571 a.C.-496 a.C.) foi um filósofo e matemático grego. **Pitágoras** foi o fundador de uma escola de pensamento grega denominada em sua homenagem de escola pitagórica. Segundo o pitagorismo, o princípio fundamental que forma todas as coisas é o **número**. **Pitágoras** descobriu em que proporções uma corda deve ser dividida para a obtenção das notas musicais no início, sem altura definida, sendo uma tomada como fundamental, e a partir dela, gerar-se-á a quinta e terça através da reverberação harmônica: os sons harmônicos. Prendendo-se a metade da corda, depois a terça parte e depois a quinta parte conseguiremos os intervalos de quinta e terça em relação à fundamental. A chamada *série harmônica*. À medida que subdividimos a corda obtemos sons mais altos e os intervalos serão diferentes. E assim sucessivamente. Descobriu ainda que frações simples das notas, tocadas juntamente com a nota original, produzem sons agradáveis. Já as frações mais complicadas, tocadas com a nota original, produzem sons desagradáveis (talvez, hoje, chamados de dissonantes). E assim, surgiu a música.

Um problema não solucionado na época de **Pitágoras** era determinar as relações entre os lados de um triângulo retângulo. O problema já era conhecido na Babilônia de Hammurabi, mas a primeira prova geral foi obtida na escola pitagórica. Enquanto os babilônios o consideravam basicamente como um resultado de medições, os pitagóricos concebiam-no como um teorema gemétrico abstrato. Pitágoras provou que o quadrado da hipotenusa é igual a soma dos quadrados dos catetos.

A descoberta mais importante atribuida a **Pitágoras** foi a dos números irracio-

nais, por meio de segmentos de retas incomensuráveis. Esta descoberta pode ter sido o resultado do seu interesse pela média geométrica. Qual era a média geométrica entre 1 e 2, na época dois símbolos sagrados? Esta questão conduziu ao estudo da razão entre a diagonal e o lado do quadrado e descobriu-se que esta razão não podia ser expressa por "números", isto é aqueles números que chamamos hoje de números racionais, os únicos números que eram conhecidos na época. O primeiro número irracional a ser descoberto foi a raiz quadrada do número 2, que surgiu exatamente da aplicação do teorema de Pitágoras em um triângulo de catetos valendo 1:

$$1^2 + 1^2 = x^2 = 2 \Rightarrow x = \pm\sqrt{2}$$

Os gregos não conheciam o símbolo da raiz quadrada e diziam simplesmente: "o número que multiplicado por si mesmo é 2". A partir da descoberta da raiz de 2 foram descobertos muitos outros **números irracionais**.

Aristóteles em *Analytica Priora*, sugere uma prova como um exemplo da prova como *redução ao absurdo*. A contradição encontrada, quando supôs que raiz de 2 poderia ser um número conhecido racional, não foi resolvida no Oriente, nem na Europa renascentista, por uma extensão do conceito de número, mas rejeitando a teoria dos números para tais casos e procurando uma síntese na geometria.

Esta descoberta que perturbou a harmonia entre aritmética e geometria, foi feita provavelmente nas últimas décadas do século V a.C. Struik (1987). Tal dificuldade surgiu de outra dificuldade que tinha emergido dos argumentos relacionados com a realidade da mudança (a razão só reconhece o ser absoluto, sendo toda mudança apenas aparente), argumentos que prenderam a atenção dos filósofos, desde essa época, até os tempos atuais. Esta dificuldade foi atribuida a **Zenão de Eleia** (490 a.C-430 a.C) em 450 a.C, um filósofo pré-socrático da escola *eleática* grega, que nasceu em Eleia, e que seu método consistia na elaboração de paradoxos. Isso passou a ter significado matemático quando os processos infinitos tiveram de ser estudados.

Aqui, os paradoxos de **Zenão** entravam em conflito com algumas concepções antigas e intuitivas sobre o infinitamente pequeno e o infinitamente grande. Acreditou-se sempre que a soma de um número infinito de quantidades se podia tornar-se tão grande quanto se quisesse, mesmo que cada quantidade fosse extremamente pequena ($\infty \times \epsilon = \infty$), e também que a soma de um número finito ou infinito de quantidades de dimensão zero era zero ($n \times 0 = 0, \infty \times 0 = 0$). **Zenão** desafiou estas concepções antigas e seus paradoxos criaram uma agitação, cujos efeitos ainda podem ser observado ainda hoje. Os paradoxos foram retomados por Aristóteles, e um deles é conhecido pelo nome de *Aquiles*. Os paradoxos de **Zenão** eram enunciados de maneira a salientar contradições existentes nos conceitos de movimento e de tempo, e nenhuma tentativa satisfatória foi feita, na época, para resolver as contradições. Os argumentos de **Zenão** mostravam que um segmento finito podia ser dividido num número infinito de pequenos segmentos, cada um deles com um comprimento finito. O raciocínio de **Zenão** influenciou o pensamento matemático de

muitas gerações, e começaram a preocupar ainda mais os matemáticos, depois da descoberta dos números irracionais. Era a matemática possível como ciência exata? E um verdadeiro escândalo lógico e crise na matemática grega apareceu, depois de **Zenão**. A crise do sistema social na Grécia (ver Struik (1987)) conduziu também à crise na matemática grega. A atmosfera intelectual reinante na época conduziu à discussão dos fundamentos da matemática: Ligados à Academia de **Platão**, atribui-se a *teoria dos irracionais*, a *teoria das proporções*, e o chamado *método da exaustão*, que permitiu o tratamento rigoroso dos cálculos de áreas e volumes. Esse método resolveu a crise na matemática grega; as suas formulações rigorosas ajudaram a determinar o rumo da axiomática grega, e de maneira considerável, da matemática grega como um todo. Tal método foi a resposta da *escola platônica* a **Zenão**. Isso evitava as dificuldades dos infinitesimais, pela redução dos problemas que conduziam a infinitesimais, a problemas que envolviam somente o uso da lógica formal, como em Struik (1987). Praticamente todo trabalho produtivo que chamamos "matemática grega"foi realizado no período entre 350 a. C-200 a. C.

Geometria é uma palavra que resulta dos termos gregos "geo"(terra) e "métron"(medir), cujo significado, em geral, é designar propriedades relacionadas com a posição e forma de objetos no espaço. A Geometria é a área da matemática que se dedica a questões relacionadas com forma, tamanho, posição relativa entre figuras ou propriedades do espaço, dividindo-se em várias subáreas, dependendo dos métodos utilizados para estudar os seus problemas.

Euclides de Alexandria, mestre, matemático da escola platônica (a ecola de Platão), e conhecido como o pai da Geometria, nasceu na Síria aproximadamente em 330 a.C. e realizou seus estudos em Atenas. Ele é até hoje, na história da Matemática, considerado como um dos mais estudiosos deste campo na antiga Grécia. Euclides tornou-se um matemático grego, cuja principal obra intitula-se *Os Elementos* (a.C). A obra "Os Elementos", atribuída a Euclides, é uma das mais influentes na história da matemática, servindo como o principal livro para o ensino de matemática (especialmente geometria) desde a data da sua publicação até o fim do século XIX ou início do século XX, como em Heath (1908), Heath (1908, 1956) e Heath (1981). Nessa obra, os princípios do que é hoje chamado de *geometria euclidiana* foram deduzidos a partir de um pequeno conjunto de axiomas.

A obra composta por treze volumes, sendo: (1) cinco sobre *geometria plana*, (2) três sobre *números*, (3) um sobre a *teoria das proporções*, (4) um volume sobre *incomensuráveis*, (5) e os últimos três sobre *geometria no espaço*. **Euclides** foi considerado um dos mais célebres gênios da matemática depois de escrito o seu mais revolucionário livro *Os Elementos*. Escrito originalmente em grego, a obra cobre toda a **aritmética**, a **álgebra** e a **geometria**, conhecidas até então no mundo grego, reunindo o trabalho de predecessores de Euclides. Sistematizou todo o conhecimento geométrico dos antigos, intercalando os teoremas já então conhecidos com a demonstração de muitos outros, que completavam lacunas e davam coerência e encadeamento lógico ao sistema por ele criado. Após sua primeira edição foi copiado e recopiado inúmeras

Figura 11 – Euklides - O criador da Geometria Euclidiana.

Fonte: prac.us.edu.pl.

vezes, tendo sido traduzido para o árabe em (774). A obra possui mais de mil edições desde o advento da imprensa, sendo a sua primeira versão impressa datada de 1482 (Veneza, Itália). Essa edição foi uma tradução do árabe para o latim. Tem sido considerado como responsável por uma influência sobre a mente humana maior que qualquer outro livro, com exceção da Bíblia Morris (1980). Embora muitos dos resultados descritos em *Os Elementos* originarem-se em matemáticos anteriores, uma das reconhecidas habilidades de Euclides foi apresentá-los em uma única estrutura logicamente coerente, tornando-a de fácil uso e referência, incluindo um sistema rigoroso de provas matemáticas que continua a ser a base da matemática 23 séculos mais tarde.

Designa-se por **período helenístico**, o período da história da Grécia e de parte do Oriente Médio compreendido entre a morte de Alexandre o Grande em 323 a.C. e a anexação da península grega e ilhas, pelos romanos em 146 a.C.. Caracterizou-se pela difusão da civilização grega numa vasta área que se estendia do mar Mediterrâneo oriental à Ásia Central. De modo geral, o helenismo foi a concretização de um ideal de Alexandre: o de levar e difundir a cultura grega aos territórios que conquistava. Foi naquele período que as ciências tiveram seu primeiro e grande desenvolvimento. Foi o tempo de **Euclides** e **Arquimedes** na Grécia. O **helenismo** marcou um período de transição para o domínio e o apogeu posterior do Império Romano. Também é relevante o fato de o maior progresso da matemática helenística ter ocorrido no Egito e não na Mesopotâmia.

O desenvolvimento histórico contínuo da **aritmética moderna** começa com a civilização helenística da Grécia antiga, embora tenha se originado muito mais tarde do que os exemplos dos babilônios e dos egípcios Karlson (1961). Depois das operações aritméticas tradicionais como a adição, a subtração, a multiplicação e a divisão, outras operações mais avançadas, tais como as porcentagens, raiz quadrada, exponenciação e funções logarítmicas, também foram incluídas neste ramo da matemática.

2.8 O Sistema de Numeração Romano

A Península grega ficou sob domínio romano a partir de 146 a.C., e a queda do Império Romano refere-se ao fim do Império Romano do Ocidente, ocorrido em 476 d.C. (século V), embora a parte oriental do Império, denominada de Império Bizantino, continuou a existir por quase mil anos, até 1453, que marcou o fim da Idade Média na Europa, quando ocorreu a queda de Constantinopla (fundada em 330 a.C.), hoje, oficialmente renomeada Istambul pela República da Turquia.

A partir deste período, até o final do século XI d.C., os povos cristãos mergulharam na maior desordem política, na recessão econômica e no obscurantismo. A Europa custou a se recuperar da queda do Império Romano (476 d. C) e das invasões bárbaras. Seus conhecimentos científicos eram elementares, para não dizer inexistentes. O ensino da *aritmética teórica*, em particular, buscava suas principais informações numa obra atribuída a **Boécio** (480-525) (século V d.C.), que por sua vez se inspirou amplamente numa obra matemática de qualidade medíocre atribuída ao grego **Nicômaco de Gerasa** (60-120) (século II d.C.). Nicômaco não era muito habilidoso com a matemática, portanto ocupava-se apenas com as propriedades elementares dos números. A introdução à Aritmética continha erros bastante elementares, pois Nicômaco não dava provas dos resultados. Algumas vezes enunciou resultados que na verdade são falsos, baseado em exemplos numéricos como evidência. Deste modo, a *aritmética prática* consistia essencialmente no uso da numeração arcaica do povo romano, tanto no modo de contar com os dedos quanto na prática de operações através de pedras ou de fichas nos velhos *Abacus*, também legados pela civilização romana.

Como a maior parte dos sistemas da antiguidade, a *numeração romana*, o sistema dos algarismos romanos (I, V, X, L, C, D, M) era regida pelo princípio da adição. Como são conhecidos até hoje, os numerais romanos parecem à primeira vista ter sido definidos em cima do alfabeto latino (I = 1, V = 5, X = 10, L = 50, C =100, D = 500, M = 1.000). Esses numerais são independentes uns dos outros e sua justaposição implicava geralmente como a soma dos valores correspondentes. Como no exemplo: $MMDCCXXVI = 1000+1000+500+100+100+10+10+5+1 = 2726$. Apesar disso, os romanos acabaram complicando esse sistema, introduzindo a regra segundo a qual, todo número colocado à esquerda de um algarismo de valor superior é dele abatido. Foi assim que os números 4, 9, 19, 40, 90, 400 e 900, por exemplo, foram frequentemente representados como nos exemplos: (a) (IV = 5 - 1) (b) (IX = 10 - 1). O sistema romano tem o agravante de serem dificeis de se calcular com esses números. Além disso, como a notação é puramente aditiva, mais e mais símbolos são necessários para representar uma quantidade, à medida que o número representado aumenta.

Uma observação sobre o ábaco é que esses artefatos nem sempre revelam o processo específico usado para resolver problemas, mas as características do sistema de numeração em particular influenciaram fortemente a complexidade dos métodos. O

sistema de hieróglifos para numerais egípcios, como os numerais romanos posteriores, descendem de marcas de contagem usado para contar Ifrah (1997), Ifrah (2005). Em ambos os casos, esta origem resultou em valores que usavam uma base decimal, mas não incluiam a notação posicional. Cálculos complexos com algarismos romanos exigiram o auxílio de uma placa de contagem ou o *ábaco romano* para obter os resultados Gonick (1984).

2.9 A Contagem dos Povos Primitivos da América

Muito antes do final do século XV d.C., a América já era ocupada por vários povos, que viviam de variadas formas, as quais iam da sua organização tribal, até aos vastos impérios, como era o caso dos *Astecas*. Muitas dessas civilizações desapareceram em conseqüência da colonização, que se iniciou no final do século XV, mas deixaram heranças históricas que marcaram o nosso continente até os dias de hoje.

Os *Astecas* e os *Maias* conheciam a escrita e registravam regularmente o seu cotidiano. Os *Incas*, por sua vez, criaram um interessante e eficiente sistema de contagem: o *quipo*. Este instrumento era feito de cordões coloridos, onde cada cor representava a contagem de algo. Com o quipo, registravam e somavam as colheitas, habitantes e impostos. Mesmo com todo desenvolvimento, este povo não desenvolveu um sistema de escrita. Uma curiosidade: já nos tempos primitivos da América Eels (1913), dos 307 sistemas de numeração investigados, 146 eram decimais, 106 de base 5 (cinco dedos das mãos) ou 20. A base 20, na sua forma mais carcterística, foi usada pelos *Maias* no México (antiga região Mesomérica) e pelos *Celtas* na Europa.

2.10 O Sistema de Numeração Hindu-Arábico

Com primeira presença atestada no século III a.C., havia o *sistema de numerais brahmi*, o qual não seguia o conceito de posições fixas para os símbolos. Os *numerais brahmi* eram um sistema de numeração originário da Índia, São ancestrais gráficos diretos dos atuais numerais Hindus e ainda dos algarismos arábicos (ou indo-arábicos). Porém eram conceitualmente diferentes do sistema posterior, pelo fato de não usarem sistema posicional com zero, algo recente, se comparado com outros sistemas decimais não posicionais.

A ideia do sistema de notação posicional de base 10 se originou na Índia, onde os primeiros conceitos de numeração posicional foram desenvolvidos. Os primórdios de um sistema de numeração decimal posicional teriam ocorrido por volta de 500 a.C. Havia, porém, como na numeração romana (não verdadeiramente posicional), símbolos adicionais para as dezenas centenas e milhares. Esse sistema posicional, da Índia se disseminou pela vizinha Pérsia, de onde foi tomado pelos árabes. O sistema dos numerais indianos é comumente conhecido no Ocidente como *hindu-arábico* ou simplesmente *algarismos arábicos*, uma vez que chegaram à Europa trazidos pelos árabes.

Como contado em Ifrah (2005), numa escuridão cultural quase total, os ocidentais tinham perdido até a memória das artes e das ciências. Os príncipes europeus desta época se preocupavam muito pouco com a cultura. A célebre biblioteca de Alexandria, a mais rica da antiguidade grega, foi destruída duas vezes: uma primeira no século IV, por vândalos cristãos e outra vez, paradoxalmente, por muçulmanos fanáticos do século VII. Vários manuscritos originais vieram a desaparecer e várias obras-primas da literatura e da ciência gregas teriam sido perdidas para a posteridade, se já não tivessem sido recolhidas e traduzidas em língua árabe. Isso foi possível, graças às obras do árabe **Ibn Roshd** (**Averroès**) (1126-1198). Os árabes se interessavam também pelas culturas orientais. Com relação aos números, primeiro eles se dedicaram às numerações alfabéticas grega e judia, cujo uso foi adaptado às 28 letras de seu próprio alfabeto.

O sistema de numeração hindu-arábico foi trazido da India, em torno de 825 d.C. (século IX d.C.) pelo matemático árabe, **Abu Abd Allah Muhammad ibn Musa al-Khwarizmi** (com acentuação árabe modificada dada a dificuldade no nosso sistema de impressão) foi um matemático, astrônomo, astrólogo, geógrafo e autor persa. Conhecem-se poucos detalhes de sua vida. Era um erudito na Casa da Sabedoria em Bagdade.

Figura 12 – Al-Khwarazmi - O difusor do sistema indu-arabic na Europa.

Fonte: Fonte: http://pt.wikipedia.org/wiki/Al-Khwarizmi .

Quando eles (árabes) tiveram acesso às descobertas Hindus, foi como ter encontrado uma luz na escuridão. Como proclamava com entusiasmo o autor de uma obra árabe da época, este sistema "*é o método mais resumido e prático, mais fácil de entender e mais cômodo de aprender. Ele comprova, sem dúvida, um espírito penetrante, um belo talento criador e a superioridade de discernimento e de gênio inventivo dos Hindus*".

Uma vez conhecida pelos árabes, a *aritmética hindu*, graças às múltiplas relações

desses povos, ganhou também rapidamente o ocidente. Quando se viram diante da numeração e dos métodos de cálculo vindos da Índia, os árabes tiveram suficiente presença de espírito para apreciar suas vantagens, reconhecer sua superioridade e adotá-los. Ao contrário, os cristãos da Europa que ficaram agarrados a seus sistemas arcaicos e foram tão reticentes diante da novidade, que foi preciso esperar durante séculos, até que o triunfo do "*algoritmo*", como era então denominado o cálculo escrito, fosse finalmente total e definitivo Ifrah (2005). A evolução do sistema hindu-arábico é motrada na Figura 13, desde o século VI na Índia, até o século XV, já introduzido na Europa.

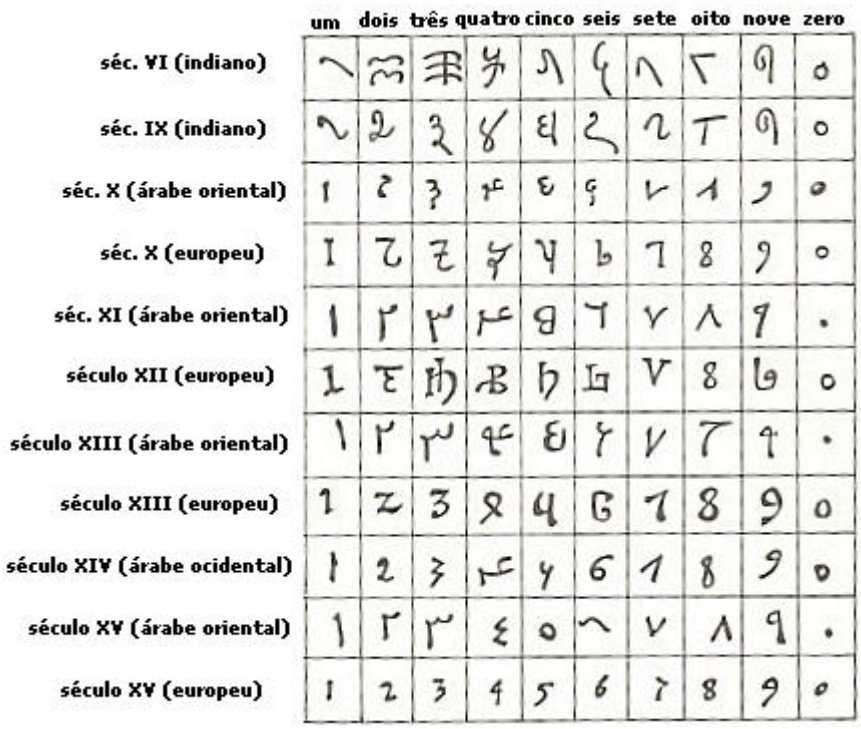


Figura 13 – A evolução no tempo, do sistema hindu-arábico.

Fonte: invivo.fiocruz.br.

Nosso sistema de numeração *Hindu-Arábico* é um sistema de numeração posicional de base 10. Ele é preciso e não apresenta ambiguidades, justamente porque temos o símbolo 0 (zero) para representar ausência de uma casa. O nome **Al Khawarismi** deu surgimento a palavra "algarismo".

Qualquer sistema de números, por mais elementar que seja, supõe a adoção de alguns símbolos, estruturados em dois princípios: o princípio de ordenamento , que permite distinguir o primeiro símbolo (um), do segundo (dois), e eventualmente do terceiro (três), e assim por diante; e o princípio de agrupamento , que interrompe a produção de símbolos individuais diferentes, estabelecendo um símbolo de ordem superior, cuja combinação com os precedentes permite reiniciar o sistema. Assim,

"um, dois, três, ..., dez, dez-um, dez-dois, ..., dez-dez ou cem, cento-um, cento-dois, ..."deu origem ao sistema baseado em 10, ou seja, um sistema decimal, como o hindus entenderam como numerar.

A partir do final do século XI, a atividade dos tradutores e dos compiladores de obras árabes, gregas ou hindus floresceu na Europa. Os contatos culturais entre os dois mundos passaram a ser ali cada vez mais frequentes, com o desembarque considerável de europeus desejosos de se instruir em matemática, astronomia, ciências naturais e filosofia. Paulatinamente, este período (séculos XII-XIII) trouxe ao conhecimento da Europa as obras de **Aristóteles** (384 a.C-322 a.C), **Euclides** (365 a.C-300 a.C), **Ptolomeu** (90 d.C-168 d.C), **AlKhowarizmi** (780 d.C-850 d.C), **Al-Biruni** (973 d.C-1048 d.C) e de tantos outros. Foi a vez dos cristãos traduzirem em latim tudo o que lhes chegava às mãos, e assinaram, deste modo, num prazo mais ou menos curto, o fim do *abacismo* (o cálculo com ábaco). A partir de então, o cálculo e a ciência moderna puderam se desenvolver sem entraves.

2.10.1 Depois do Século XI - O Sistema Decimal - Base 10

Leonard Fibonacci (1170-1250) ficou conhecido pela introdução dos algarismos Hindu-Arábicos na Europa. Com outros matemáticos do seu tempo, contribuiu para o renascimento das ciências exatas, após a decadência do último período da antiguidade clássica e do início da Idade Média. **Fibonacci** destacou-se ao escrever o *Liber Abaci*, o Livro do Ábaco, em 1202, sendo obra importante sobre matemática. **Liber Abaci** introduziu os numerais *Hindu-Arábicos* na Europa, além de discutir muitos problemas matemáticos.

Figura 14 – Fibonacci: o primeiro grande matemático europeu da Idade Média.

Fonte: en.wikipedia.org/wiki/Leonardo_Fibonacci.

No *Liber Abaci* (1202), **Fibonacci** apresenta o chamado *modus Indorum* (método

dos Hindus), hoje conhecido como *algarismos arábicos* (Sigler 2003; Grimm 1973). O livro defendia a numeração com os dígitos 0-9 e a notação posicional, esclarecendo o sistema de posição árabe dos números, incluindo o número zero. O livro mostrou a importância prática do novo sistema numeral, aplicando-o à contabilidade comercial, conversão de pesos e medidas, o cálculo de juros, taxas de câmbio e outras aplicações. O livro foi bem recebido em toda Europa e teve um impacto profundo no pensamento europeu. Esse elegante sistema de sinais numéricos, em breve, substituiria o não mais oportuno sistema de algarismos romanos.

Liber Abaci também colocou e resolveu um problema que envolve o crescimento de uma população hipotética de coelhos com base em pressupostos idealizados. A solução, de geração em geração, foi uma sequência de números mais tarde conhecida como a sequência de **Fibonacci**: $\langle 1, 1, 2, 3, 5, 8, 11, ... \rangle$. A seqüência numérica era conhecida por matemáticos indianos já no século VI, mas foi o *Liber Abaci* que a introduziu no Ocidente.

2.10.2 Representando Números na Base 10

Seja qual for a razão, usamos o sistema decimal de numeração com os algarismos: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Existe, então, uma regra geral de representação para qualquer qualquer N inteiro ou fracionário :

$$N = a_n.10^n + a_{n-1}.10^{n-1} + a_{n-2}.10^{n-2} + ... + a_1.10^1 + a_0.10^0$$

onde n é um inteiro positivo ou negativo ($n \in \mathbb{Z}$). Portanto, qualquer número decimal inteiro ou fracionário pode ser representado segundo esta fórmula.

Exemplos (**Decomposição de números reais**)

$$7236,81 = 7 \times 10^4 + 2 \times 10^3 + 3 \times 10^2 + 6 \times 10^1 + 8 \times 10^{-1} + 1 \times 10^{-2}$$

$$1537 = (1537)_10 = 1 \times 10^3 + 5 \times 10^2 + 3 \times 10^1 + 7 \times 10^0$$

$$36,189 = (36,189)_10 = 3 \times 101 + 6 \times 100 + 1 \times 10 - 1 + 8 \times 10 - 2 + 9 \times 10 - 3$$

$$6,032 \times 10^{23} = (6,032 \times 10^{23})_10 = 6 \times 10^{23} + 0 \times 10^{22} + 3 \times 10^{21} + 2 \times 10^{20}$$

O sistema de numeração decimal Stein (2008), é semelhante a um dicionário. Em vez de letras, o sistema de numeração decimal usa os caracteres $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Estes dez caracteres formam todas as palavras que podem ser usadas para descrever quantidades. É um dicionário simples: por exemplo o número $384,07$ é na verdade definido por $3 \times 10^2 + 8 \times 10^1 + 4 \times 10^0 + 0 \times 10^{-1} + 7 \times 10^{-2}$. O valor quantitativo da palavra $384,07$ é dedutível das letras (dígitos) usadas e de suas posições na palavra (número decimal).

Uma maneira de definir os números reais é o conjunto de todas as representações decimais da forma anterior, em que somente é permitida uma quantidade finita de números à esquerda do ponto decimal, mas uma quantidade infinita para o outro lado. Com essa convenção, $384,07 = 384,7000000\ldots$.

Os racionais são todos aqueles números, tal como, $25,512121212\ldots$ que eventualmente se acomodam em um padráo repetitivo à direita do ponto decimal. Pode-se verificar que $0,5121212\ldots = 507/990$.

Um *número normal* de base 10 é aquele no qual, em média, cada dígito decimal, tal como 5, aparece 1/10 das vezes. Cada par de dígitos decimais sucessivos, digamos 57, aparece 1/100 das vezes, cada tripla de dígitos decimais sucessivos, tal como 571,, aparece 1/1000 das vezes, e assim por diante. Esse é o equivalente matemático da moeda "aleatória ideal", no lugar de uma moeda aleatória ideal com dois lados, cujos arremessos gerariam um número normal na base 2. O caso de base 10, pode ser imaginado a uma roleta perfeitamente equilibrada com 10 números, de 0 a 9. É possivel formular uma definição equivalente de normalidade para qualquer base de um sistema de numeração. Em Stein (2008), capítulo 10, p.200-202, existe mais informação sobre números normais conhecidos. Uma observação interessante é que há muitos poucos exemplos de númerosnormais em todas as bases; todos os que são conhecidos são altamente artificiais, pois não são encontrados no mundo real. Também que, esses números normais, não aparecem quando estamos medindo coisas.

Em de vez de 10, que usamos no sistema decimal, é possível usarmos, como base de um sistema de numeração, qualquer inteiro positivo maior que 1. Quando "2"assume o lugar de "10"no sistemas decimal, temos como resultado o sistema de numeração binário de base 2, com o alfabeto consistindo dos dígitos $\{0, 1\}$.

2.11 Representando Números na Base 2

A aritmética babilônica (2100 a. C) baseava-se no número 60, e nos costumes e linguagem dos povos que falam inglês, estão submersos os remanescentes de um sistema de base 12, que em certa época imperou nas ilhas britânicas: 12 meses num ano, 12 polegadas num pé, dois períodos de 12 horas num dia, medidas em grupos de dúzias, entre outros exemplos. Inspirado no número de dedos no par das mãos humanas, o sistema decimal terminou por ofuscar todos os outros meios de numeração, pelo menos no ocidente.

Pingala foi um antigo matemático indiano, famoso por sua obra, o *Chandas Shastra*, um tratado *sânscrito* (ou língua sânscrita é uma língua da Índia, com uso litúrgico no hinduísmo, budismo e jainismo. O sânscrito faz parte do conjunto das 23 línguas oficiais da Índia.) sobre **prosódia** (é a parte da linguística que estuda a entonação, o ritmo, o acento - a intensidade, altura, duração - da linguagem falada e demais atributos correlatos na fala. A prosódia descreve todas as propriedades

acústicas da fala que não podem ser preditas pela transcrição ortográfica) considerado parte do *Vedanga* (Os Vedanga são seis disciplinas auxiliares para a compreensão e tradição dos Vedas, textos sagrados do Hinduísmo). Na tradição literária Indiana, **Pingala** é identificado como o irmão mais novo do **Panini**, o grande gramático do século V a.C. Outras tradições o identificam com **Patanjali**, o autor do *Mahabhashya*.

Mylius (1983:68) considera o Chandas-shastra "muito posterior"no corpo Vedanga. Isso o colocaria próximo à Era Comum, provavelmente pós-datando os tempos do Império Máuria (R. Hall, Mathematics of Poetry, tem "c. 200 a.C.").

O *Chandas Shastra* é dividido em oito capítulos. Foi editado por **Weber** (1863). Está na transição entre a métrica védica e a métrica clássica dos épicos sânscritos. O matemático do século X, **Halayudha**, o comentou e expandiu. Neste contexto, **Pingala** apresenta a primeira descrição conhecido de um sistema numérico binário. Ele descreveu o sistema numérico binário em conexão à listagem das métricas védicas com sílabas longas e curtas. A sua discussão sobre a combinação de métrica corresponde ao teorema binomial. O comentário de **Halayudha** inclui uma apresentação do triângulo de Pascal (chamado de meru-prastaara). A obra de **Pingala** também contém as idéias básicas de números de **Fibonacci** (chamados de *maatraameru*).

O uso do zero é às vezes erroneamente designado a **Pingala** devido à sua discussão sobre números binários, geralmente representados usando 0 e 1 na discussão moderna, mas Pingala usou sílabas longas e curtas. Quatro sílabas curtas (em binário, "0000") no sistema de **Pingala**, contudo, representam o número um, e não o zero. Uso posicional do zero data de séculos posteriores e teria sido familiar a **Halayudha**, mas não ao **Pingala**.

Da ideia de **Pingala** no século III a.C., o sistema binário foi refinado por **Leibniz**, no século XVII.

2.11.1 Leibniz e o sistema binário

Leibniz não inventou o código binário, mas foi um dos precursores no uso no contexto de uma lógica. Certos pensadores ocidentais pós-renascentistas, no entanto, fascinaram-se pela simplicidade dos dois estados da numeração binária. Lentamente, o conceito infiltrou-se em disciplinas científicas isoladas, da lógica e da filosofia à matemática e à engenharia, ajudando a anunciar a aurora da era do computador digital. **Leibniz** foi um dos primeiros defensores do sistema binário, que chegou a ele de uma maneira indireta. Em 1666, enquanto completava seus estudos universitários, e bem antes de inventar sua calculadora de rodas dentadas, **Leibniz**, então com 20 anos, esboçou um trabalho que, modestamente, dissertava sobre sistemas binários, denominado "*De Arte Combinatoria*"(Sobre a Arte das Combinações), esse pequeno trabalho delineava um método geral para reduzir todo pensamento - de qualquer tipo e sobre qualquer assunto - a enunciados de perfeita exatidão. A *lógica* (ou, como ele a chamava, as *leis do pensar*) seria então transposta do domínio verbal, que é

repleto de ambiguidades, ao domínio da matemática, que pode definir com precisão as relações entre objetos ou enunciados. Além de propor que todo pensamento racional se tornasse matemático, **Leibníz** invocava "*uma espécie de linguagem ou escrita universal*", mas infinitamente diversa de todas as outras concebidas até aquele tempo, isso porque os símbolos e até mesmo as palavras nela envolvidas dirigir-se-iam à razão, e os erros, exceto os fatuais, seriam meros erros de cálculo. Seria muito difícil formar ou inventar essa linguagem, mas também seria muito fácil compreendê-la.

2.11.2 Refinamento do Sistema Binário

Seus contemporâneos, talvez perplexos, talvez sentindo-se inferiorizados por suas idéias, ignoraram esse ensaio, e o próprio **Leibniz**, ao que parece, nunca voltou a retomar a idéia da sua nova linguagem. Uma década mais tarde, porém, ele começou a explorar uma nova maneira as potencialidades da matemática, concentrando-se em aprimorar o sistema binário. Enquanto trabalhava, transcrevendo laboriosamente números decimais transformados em binários, era estimulado por um manuscrito secular que lhe chamara a atenção. Tratava-se de um comentário sobre o venerável livro chinês *I Ching* ou "Livro das Mutações", que procurava representar o universo e todas as suas complexidades por meio de uma série de dualidades, contrastando luz e trevas, macho e fêmea. Encorajado por essa aparente validação de suas próprias noções matemáticas, **Leibniz** continuou aperfeiçoando e formalizando as intermináveis combinações de uns e zeros, que constituíram o moderno *sistema binário*. E hoje, qualquer computador digital atual, independente do tamanho ou da finalidade a que se destina, significa, ter em sua essência, um sistema de tráfego de informações expresso em zeros e uns. Um código de dois símbolos não era a única alternativa ao sistema decimal.

Neste sistema binário, como é conhecido hoje, usa-se a base 2, portanto requerendo apenas dois símbolos: "0"e "1".

O uso do sistema binário é inadequado para o nosso dia-a-dia, mas é ideal para a construção dos computadores, pois só tem dois algarismos, e são ótimos para representar dois estados, tais como "ligado/desligado", "aberto/fechado", "sim/não"ou "falso/verdadeiro".

Neste caso:

$N_2 = a_n.2^n + a_{n-1}.2^{n-1} + a_{n-2}.2^{n-2} + ... + a_1.2^1 + a_0.2^0$

onde n é um inteiro positivo ou negativo ($n \in \mathbb{Z}$). Portanto, qualquer **número binário** pode ser representado segundo esta fórmula.

Em binário 100 (decimal) será: $1010_2 = 1x2^3 + 0x2^2 + 1x2^1 + 0x2^0 = 1x8 + 1x2 = 10_2$

Exemplos (**Decomposição de números binários**)

$(10111)_2 = 1x2^4 + 0x2^3 + 1x2^2 + 1x2^1 + 1x2^0$

$(10,1)_2 = 1x2^1 + 0x2^0 + 1x2^{-1}$

2.11.3 Os Sistema Binário e a Ideia dos Cartões Perfurados

No século XIX, em 1801, apareceu o tear controlado por cartão perfurado, invenção de **Joseph Marie Jacquard** (ver no Volume II, capítulo sobre Calculadoras Mecânicas, a Pré-História dos Computadores), no qual as perfurações indicavam os 1's e os locais não perfuradas, indicavam os 0's. O sistema está longe de ser um computador, mas ilustrou que as máquinas poderiam ser controladas pelo sistema binário. Cartões perfurados perduraram até o século XX, meados dos anos 70. Atualmente, no processamento de todos computadores modernos, a ideia do cartão perfurado tem sido substituída pelo sistema similar, mas de leitura ótica sobre *marcas* no cartão, indicadas pelo usuário, correspondendo a sequências específicas de 0's e 1's, podendo representar qualquer informação. Como por exemplo, empregado na Mega-Sena da CEF ou em grandes vestibulares ou exames nacionais da educação brasileira.

2.11.4 As Aplicações dos Números Binários

Em Stein (2008), temos que o sistema binário é o de uso natural para o armazenamento de informações em um computador digital. Originalmente, a informação era exibida por meio de uma sequência de luzes: acesa (1) e apagada (0). Computadores, no passado dos anos 50-70, aimda armazenavam informações de forma magnéticamente: magnetizado (1), não-magnetizado (0).

Em outro fato, considere uma moeda como em Stein (2008), em que o sistema binário surge, diante dos lançamentos da moeda ao acaso. Há uma correspondência simples entre uma sequência infinita de caras ou coroas e representações binárias de números 0 e 1. Mais precisamente de representações binárias entre 0 e 1. Dada uma sequência de caras ou coroas, substitua cara por 0, coroa por 1, remova as vírgulas, e coloque uma vírgula decimal à esquerda do primeiro dígito. A sequência infinita de caras ou coroas que alterna cara e coroa (Ca, Co, Ca, Co, ...) torna-se um número binário $0,01010\ldots$. Também é possível fazer o procedimento reverso: a partir de um número binário entre 0 e 1, construir uma sequência infinita de caras ou coroas. Neste caso, a procura por uma moeda aleatória ideal, se transforma na procura por um número binário. A exigência de que cada sequência específica de n jogadas ocorra $1/(2^n)$ das vezes, se torna a exigëncia de que cada sequëncia específica de n dígitos binários (0s e 1s) ocorra $1/(2^n)$ das vezes. Um número que possui essa propriedade é chamado normal de base 2.

Outra aplicação de binários em Stein (2008), é o de haver um dicionário que traduza blocos de números para os caracteres da linguagem na qual uma mensagem seja apresentada. Este é o caso, do código ASCII (*American Standard Code for Information Interchange*), o código que traduz blocos de oito dígitos binários armazenados em

um computador para caracteres imprimíveis ou tecláveis que se originam a partir do teclado de um computador. Um exemplo é o caso da do bloco binário "01000001"(cuja representação decimal é 65, armazenado em 1 byte de 8 bits), corresponde ao caracter "A".

2.12 Nos Dias de Hoje ...

Além das operações elementares de somar, subtrair, multiplicar e dividir, os matemáticos, de hoje, por vezes, usam o termo "aritmética superior"Davenport (1999), quando se refere a resultados mais avançados relacionados à **Teoria dos Números**. Esta inclui as propriedades dos inteiros relacionados com, a **divisibilidade**, a **primalidade** e a **solução de equações em inteiros**. É neste contexto que se pode encontrar o **Teorema Fundamental da Aritmética** e as **Funções Aritméticas** Monteiro (1969). O livro *A Course in Arithmetic* de **Jean-Pierre Serre** reflete esse uso, assim como termos, como a *aritmética de primeira ordem* Serre (1973).

2.13 Bibliografia e Fonte de Consulta

Florain Cajori - Uma História da Matemática, Editora Ciência Moderna, 2007.

Michel Janos - Matemática e Natureza, Editora Gradiva, 2009.

Dirk Struik - História concisa das matemáticas. Gradiva. 1987.

Sistemas de numeração - ⟨http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/1384/2012_01186_CLAUDECIO_GONCALVES_LEITE.pdf?sequence=1⟩

Matematica árabe - http://www.somatematica.com.br/historia/oriental2.php

Matemática hindu - http://www.somatematica.com.br/historia/oriental4.php

Pingala - https://pt.wikipedia.org/wiki/Pingala

James D. Stein - Como a Matemática Explica o Mundo, Editora Campus, 2008.

Boyer, Carl B. (1996). História da matemática. 2ª Edição. São Paulo. Edgard Blücher ltda. ISBN 85-212-0023-4.

Georges Ifrah, The Universal History of Numbers: From Prehistory to the Invention of the Computer. Translated by David Bellos, Sophie Wood, pub. J. Wiley, 2000.

Karl Menninger, Number Words and Number Symbols - A Cultural Hystory of Numbers ISBN 0-486-27096-3

David Eugene Smith and Louis Charles Karpinski, The Hindu-Arabic Numerals (1911)

A. Weber, Indische Studien 8, Leipzig, 1863.

Bibliotheca Indica, Calcutta 1871-1874, reprint 1987.

2.14 Referências - Leitura Recomendada

Howard Eves. Introdução à História da Matemática. Editora da Unicamp.

Hieróglifos gregos: http://discoveringegypt.com

Matemática. Benigno Barreto e Claudio Xavier - Editora FTD.

Lewy, H. (1949)."Studies in Assyro-Babylonian mathematics and metrology". Orientalia (NS) 18, 40-67; 137-170.

Bruins, E.M. (1953). La classification des nombres dans les mathématiques babyloniennes. Revue d'Assyriologie 47, 185-188.

Matemática babilônica: "The culture of Babylonia: Babylonian mathematics, astrology, and astronomy". The Assyrian and Babylonian Empires and other States of the Near East, from the Eighth to the Sixth Centuries B.C. Eds. John Boardman, I. E. S. Edwards, N. G. L. Hammond, E. Sollberger and C. B. F. Walker. Cambridge University Press, (1991).

BOYER, Carl B. - História da matemática. 2º ed. SP. Edgard Blucher, 2003.

EVES, Howard. Introdução à história da matemática. 2º ed. UNICAMP, 2002.

LINTZ, Rubens G. História da matemática. FURB. 1999.

STRUIK, História Concisa das Matemáticas. Gradiva. 1987.

Jean van Heijenoort (1889) - "Os princípios da aritmética, apresentados por um novo método"em 1967. Um Livro Fonte em Lógica Matemática, 1879-1931. Harvard Univ. Imprensa: 83-97.

Kennedy, Hubert C. - Os trabalhos selecionados de Giuseppe Peano, ed. e transl. Com um esboço biográfico e bibliografia. London: Allen & Unwin. 1973.

Gillies, Douglas A., 1982. Frege, Dedekind e Peano sobre os fundamentos da aritmética. Assen, Holanda: Van Gorcum.

Ivor Grattan-Guinness, 2000. A busca das raízes matemáticas 1870-1940. Princeton University Press.

Kennedy, Hubert C., 1980. Peano: vida e obra de Giuseppe Peano. Reidel. Biografia com bibliografia completa (p. 195-209).

George Gheverghese Joseph. The Crest of the Peacock: Non-European Roots of Mathematics, Penguin Books, 2000.

Euclid (Greek mathematician) Encyclopædia Britannica, Inc (2008). Visitado em 2008-04-18.

Artmann, Benno (1999). Euclid: The Creation of Mathematics. New York: Springer. ISBN 0-387-98423-2.

Ball, W.W. Rouse (1960) [1908]. A Short Account of the History of Mathematics (4th ed.). Dover Publications. pp. 5062. ISBN 0-486-20630-0.

Boyer, Carl B. - A History of Mathematics. 2nd ed. [S.l.]: John Wiley Sons, Inc., 1991. ISBN 0471543977

Heath, Thomas (ed.) - (1956) [1908]. The Thirteen Books of Euclid's Elements. 1. Dover Publications. ISBN 0-486-60088-2.

Heath, Thomas L. (1908), "⟨EuclidandtheTraditionsAboutHim⟩", in Euclid, Elements (Thomas L. Heath, ed. 1908), 1:16, at Perseus Digital Library.

Heath, Thomas L. (1981). A History of Greek Mathematics, 2 Vols. New York: Dover Publications. ISBN 0-486-24073-8 / ISBN 0-486-24074-6.

Kline, Morris (1980). Mathematics: The Loss of Certainty. Oxford: Oxford University Press. ISBN 0-19-502754-X.

Struik, Dirk J. (1967). A Concise History of Mathematics. Dover Publications. ISBN 486-60255-9.

Amulya Kumar Bag, 'Binomial theorem in ancient India', Indian J. Hist. Sci. 1 (1966), 6874.

George Gheverghese Joseph. The Crest of the Peacock: Non-European Roots of Mathematics, Penguin Books, 2000.

Klaus Mylius, Geschichte der altindischen Literatur, Wiesbaden (1983).

EVES, Howard. Introdução à História da Matemática. Traduzido por Hygino H. Domingues. 5 ed. Campinas: Editora da Unicamp, 2011.

CAPÍTULO 3

Os Números

Onde e quando esta fantástica aventura da inteligência humana começou? Não sabemos de nada. O acontecimento se perde nos tempos pré-históricos, e dele não resta hoje traço algum.

Surgida sem dúvida sobre bases empíricas, a invenção dos números deve ter correspondido a preocupações de ordem prática e utilitária. Aqueles que guardavam rebanhos, precisavam ter certeza de que, ao voltar do pasto, todos os animais tinham entrado no curral. Os que estocavam ferramentas, ou armas, ou que mantinham reservas alimentares para atender a uma vida comunitária, deviam estar aptos a verificar se a disposição dos víveres, armas ou instrumentos era idêntica à que eles haviam deixado anteriormente.

Tudo começou com este artifício conhecido como *correspondência um a um*, que confere, mesmo aos espíritos mais desprovidos, a possibilidade de comparar com facilidade duas coleções de seres ou de objetos, da mesma natureza ou não, sem ter de recorrer à contagem abstrata. Foi sem dúvida graças a este princípio que, durante milênios, o homem pré-histórico pôde praticar a aritmética antes mesmo de ter consciência e de saber o que é um número abstrato.

Os números devem ter surgido pela necessidade de se contar ou conhecer coisas importantes para a sobrevivência dos homens da antiguidade. Situações diferentes precisavam de números diferentes. E, então, surgiram os vários tipos de números: naturais, inteiros, racionais, irracionais (algébricos, transcedentais e incomputáveis), reais e complexos. Cada tipo servindo para determinada situação. Estes tipos de números serão explicados nas seções seguintes, mas observando no capítulo 2, a evolução dos sistemas numéricos, desde os egípcios aos hindu-arábicos que usamos.

3.1 Números Naturais

A dualidade de todas as coisas é uma noção importante na maioria das culturas. Os números naturais tiveram suas origens nas palavras utilizadas para a contagem de objetos, começando com o número dois, e daí por diante. Uma abstração seguinte foi identificar o número 1 (**Bertrand Russel** em "A série dos números naturais", Introdução à filosofia matemática.

O avanço seguinte na abstração foi o uso de numerais para representar os números. Isto permitiu o desenvolvimento de sistemas para o armazenamento de grandes números. Por exemplo, os babilônicos desenvolveram um sistema de atribuição de valor baseado essencialmente nos numerais de 1 a 10. Os egípcios antigos possuíam um sistema de numerais com hieróglifos distintos para 1, 10, e todas as potências de 10 até um milhão. Uma gravação em pedra encontrada em Karnak, datando de cerca de 1500 a.C. e atualmente no Louvre, em Paris, representa 276 como 2 centenas, 7 dezenas e 6 unidades; e uma representação similar para o número 4622, como em **Georges Ifrah**, na HISTORIA UNIVERSAL DOS ALGARISMOS.

Um avanço muito posterior na abstração foi o desenvolvimento da ideia do zero como um número com seu próprio numeral, como em **Célia Maria Carolino Pires**, "Números Naturais e Operações". Um dígito zero tem sido utilizado como notação de posição desde cerca de 700 a.C. pelos babilônicos, porém ele nunca era utilizado como elemento final. O conceito da forma como ele é utilizado atualmente se originou com o matemático indiano **Brahmagupta** em 628. Contudo, o *zero* foi utilizado como um número por todos os *computus* (calculadoras da idade média) começando com **Dionysius Exiguus** (470 d.C-544 d.C) em 525, quem escreveu um tratado de matemática elementar, porém no geral nenhum numeral romano foi utilizado para escrevê-lo. Ao invés disto, a palavra latina para "nenhum", "nullae", foi empregada pelos romanos.

O primeiro estudo esquemático dos números como abstração (ou seja, como entidades abstratas) é comumente atribuído aos filósofos gregos **Pitágoras**(570 a.C-495 a.C) e posteriormente por **Arquimedes**(287 a.C-212 a.C). Entretanto, estudos independentes também ocorreram por volta do mesmo período na Índia, China, e Mesoamérica (região atual da América Central).

No século XIX, uma definição do conjunto teórico dos números naturais foi desenvolvida. Com esta definição, era mais conveniente incluir o zero (correspondente ao *conjunto vazio*) como um número natural. Esta convenção é seguida pelos teorizadores de conjuntos, logicistas, e cientistas da computação. Outros matemáticos, principalmente os teorizadores dos números, comumente preferem seguir a tradição antiga e excluir o zero dos números naturais, Daí a notação $\mathbb{N}^*$ para indicar a exclusão do zero.

Os números devem ter se originado na necessidade de se contar, mas o conceito

abstrato de número surgiu muito depois. Números naturais são abstrações criadas pelos humanos para contar objetos. O conjunto dos `\index{números naturais}`, denotado por $\mathbb{N}$ é dado por $\{1, 2, 3, ...\}$.

A palavra grega "**axioma**" é usada na matemática com o significado que deve ser, por princípio, aceita como uma verdade. ou seja, é uma **premissa** ou um **postulado**. As raizes da matemática são os axiomas. Todas as **teorias** são baseadas nos seus axiomas.

Uma construção consistente do Conjunto dos Números Naturais foi desenvolvida no século XIX por **Giuseppe Peano**. Essa construção, comumente chamada de Axiomas de Peano, é uma estrutura simples e elegante, servindo como um bom exemplo, de construção de conjuntos numéricos.

Giuseppe Peano (1858-1932) foi um matemático Italiano que contribuiu bastante sobre a notação que hoje é usada. A axiomatização padrão dos números naturais é chamada de , em sua homenagem. Como parte desse esforço, ele fez contribuições fundamentais para o tratamento rigoroso e sistemático do método de prova da . Ele passou a maior parte da sua carreira ensinando matemática na Universidade de Turim, na Itália.

Figura 15 – Peano - Os princípios da aritmética, apresentados por um novo método.

Fonte: pt.wikipedia.org.

3.1.1 Os Axiomas de Peano

Descrito informalmente:

1. Zero é um número.

2. Se a é um número, então o sucessor de a é um número chamado de $s(a)$.
3. Zero não é sucessor de nenhum número.
4. Não existem dois números com o mesmo sucessor.
5. Se uma propriedade pertence a zero, e também ao sucessor de todo número, então todos os números tem essa propriedade (**Axioma da Indução**).

Agora, considerando-se também o 0 e os números naturais $\{1, 2, 3, ...\}$, os axiomas de Peano e as operações de soma e multiplicação, toda a álgebra pode ser desenvolvida. Uma observação interessante é que tendo-se a e seu sucessor b descrito como uma função s, tala que $s(a) = b$, pode-se definir as operações da aritmética com os números naturais Janos (2009):

1. $a + b = b + a$ (comutatividade da adição, para um número **finito** de parcelas)
2. $a.b = b.a$ (comutatividade da multiplicação)
3. $a + (b + c) = (a + b) + c$ (associatidade da adiçao)
4. $a.(b.c) = (a.b).c$ (associatividade da multiplicação)
5. $a.(b + c) = a.b + a.c$ (distributividade da multiplicação, em relação à adição)

Aqui, a multiplicação é definida como $a.b = axb = b + b + ... + b$, onde b é somado tantas vezes quanto for o valor de "a". Exemplo: $4x3 = 3 + 3 + 3 + 3 = 12$, ou seja, uma multiplicação significa somar 4 vezes o valor 3. Também pode-se ver uma soma s como uma função que para cada dois naturais $[a, b] \rightarrow a + b$. O mesmo para a multiplicação que associa dois operandos $(a, b) \rightarrow a.b = axb$.

As leis da aritmética para os números naturais parecem óbvias porque estamos acostumados com elas. Mas, precisamos ter em mente que existem outras aritméticas em que estas leis podem não ser válidas. Por exemplo, na aritmética das matrizes, a propriedade (2) não á válida, pois a multiplicação de matrizes não é comutativa.

3.1.2 A operação de subtração e os números negativos

Das propriedade de (1) a (5) podemos definir a **relação de desigualdade**. Esta é uma relação de ordem sobre $\mathbb{N}$. A relação entre dois números naturais, $b > a$ ("b"maior que "a") significa que, a partir de "a", pode obter "b", adicionando-se um quantidade "c"ao conteúdo "a", isto é, $b = a + c$. Isto é que nos leva a operação de **subtração**, $c = (b - a)$. Então, a diferença $(b - a)$ de dois números naturais é o número natural c. Entretanto, no domínio dos naturais, isto só e válido, se $b > a$.

A relação de desigualdade $b > a$ ou que $a < b$, ou mesmo que $a \leq b$, pressupõe, intuitivamente, uma **relação de ordem** sobre o conjunto dos números naturais $\mathbb{N}$. Num capítulo posterior é mostrado o que é, formalmente, uma **relação de ordem**

sobre um conjunto, ou uma **relação de ordem parcial** sobre $\mathbb{N}$.

Ocorreu um enorme avanço quando esta restrição foi resolvida pela introdução do "0"e do "1", fazendo-se aparecer que:

- $a + 0 = a$ ("0"é um elemento distinguido e neutro para a adição)
- $a - a = 0$ (isto pode ser provado, como está JACY MONTEIRO (1969), p.75.
- $a.0 = 0$ (por definição de multiplicação)

e a introdução dos números negativos -1, -2, -3, ..., em conjunto com a definição $(b-a) = -(a-b)$. Só assim, puderam ser representadas algebricamente, os atrasos, os delocamentos em sentido contrário, os débitos financeiros, as temperaturas negativas (frias). Historiadores acreditam que o "0"apareceu por volta de 300 a.C, para significar, por exemplo, o "não sobrou nenhum ..."e o uso do "0"para diferenciar, por exemplo 87 de 807, surgiu muito tempo depois Janos (2009). E o outro elemento importante de $\mathbb{N}$ é "1".

3.1.3 Princípio da Indução Finita sobre $\mathbb{N}$

Indução é muito comum em matemática (quando se envolve os números naturais), para uso em definições e provas matemáticas, mas também típica, para ser aplicada em várias partes da **ciência da computação**.

Definições indutivas são especialmente adequadas para uso com conjuntos infinitos. Além disso, **conjuntos definidos por indução**, ganham, implicitamente, uma estrutura que pode servir como base para a **definição indutiva de funções** sobre esses conjuntos. **Provas indutivas** são especialmente adequadas para propriedades de conjuntos com elementos, de comprimento ilimitado.

Consideremos as seguintes duas formulações equivalentes do princípio da indução finita sobre $\mathbb{N}$:

1. P ocorre para $n = 0$.
2. Se P ocorre para um $n \in \mathbb{N}$, então P também ocorre para $n + 1$.

Ou de outra forma:

1. P ocorre para $n = 0$.
2. Se $n \in \mathbb{N}$, $n \neq 0$ e P ocorre para todo $m \in \mathbb{N}$, tal que $m < n$, então P também ocorre para n.

Mais sobre a construção formal dos números naturais $\mathbb{N}$ e a prova de vários teoremas sobre $\mathbb{N}$, o leitor por estudar em Monteiro (1969), Capítulo II, 2, seção 2.1, p.10.

3.2 Números Inteiros

Os *números inteiros* são contruídos e simbolizados por $\mathbb{Z}$, a partir do conjunto $\mathbb{N}$ dos números naturais, pelo processo da simetrização da adição definida sobre $\mathbb{N}$. Simetria é algo que aparece em muitas situações na natureza, sendo muitas vezes usada pelo homem na construção de coisas físicas. É mostrado que $\mathbb{N}$ pode ser considerado uma parte de $\mathbb{Z}$.

É mostrado na subseção anterior, que acrescentando-se o "0"e os números negativos dos números naturais (os simétricos dos números naturais), obtém-se os números inteiros $\mathbb{Z}$:

$$... - 3, -2, -1, 0, 1, 2, 3, ...$$

A construção formal dos números inteiros $\mathbb{Z}$ e a prova de vários teoremas sobre $\mathbb{Z}$, o leitor por estudar em Monteiro (1969), Capítulo III.

3.3 Números Inteiros e Frações

Com a aparição dos números inteiros negativos e do "0", pode-se, agora, **somar**, **subtrair** e **multiplicar números inteiros**. Mas, para **dividir** dois inteiros, precisamos definir o conceito de **fração**. O aspecto mais notável da aritmética egípcia é o seu cálculo de frações.

Por exemplo para dividir 21 em 3 partes iguais , fazemos $21 = 7 + 7 + 7$. Mas, dividir 21 em 4 partes iguais é impossível com números inteiros. Por isso, definimos e representamos frações tais como, $21/4$, $7/3$, como relações entre inteiros. Usando-se **inteiros**, o máximo que dá para dizer é que, $21/4 = 5$ e resta 1, ou que $7/3 = 2$ e resta 1, ou mesmo que $17/5 = 3$ e resta 2. Claramente, $21/4$ representa a fração "a quarta parte de um todo que é 21", e "7/3 representa um terço de um todo que é 7". Definimos frações, como relações entre inteiros. Os pontos na reta dos números, que representam frações, são obtidos através da subdivisão de cada intervalo em frações decimais, usando-se o sistema de numeração decimal.

Qualquer fração decimal pode ser escrita como:

$$N = n_0 + \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + ... + \frac{a_n}{10^n}$$

3.4 Ampliando a Aritmética

Agora, usando-se 0 e 1, os números negativos e as frações, podemos ampliar as **leis da aritmética** com:

1. $a + 0 = 0 + a = a$

2. $a.1 = 1.a = a$ ("1"é um elemento distinguido e neutro para a multiplicação, onde neste caso, a é tomado na soma da multiplicação, apenas 1 vez.)
3. $a + b = a + c \Rightarrow b = c$
4. $a + (-a) = +(a) + (-a) = 0$
5. $(a).(1/a) = (1/a).(a) = 1$ se $a \neq 0$

Como pode ser visto, o resultado da divisão de dois números inteiros pode ser um valor exato, como por exemplo, $2/5 = 0,4$ ou uma fração cujos termos decimais se repetem indefinidamente, como por exemplo, $1/3 = 0,3333333...$e $1/13 = 0,076923076....$ Toda fração representando um número racional, tem de ser de uma destas formas. Uma fração não pode ser uma expressão decimal que nunca se repete, como por exemplo: 0,12123123412345...

3.5 Números Racionais

Um número **racional**, é um número que pode ser escrito na forma p/q (isto é, uma **razão** ou **fração**), onde p e q são dois números inteiros. O conjunto do números racionais é denotado por $\mathbb{Q}$, onde:

$\mathbb{Q} = \{p/q \mid p \in \mathbb{Z};\ q \in \mathbb{Z}^*\}$, onde $\mathbb{Z}^* = \mathbb{Z} - \{0\}$

Náo é claro os argumentos filosóficos dos gregos que fizeram dos números racionais, o âmago da matemática. Uma propriedade que distingue os racionais dos inteiros é que eles são "densos".

Definição (**Conjunto Denso**)

Sejam a e b dois elementos quaisquer de um conjunto D. Diz-se que o conjunto D é denso, se podemos inserir outro elemento d, pertencente a D, tal que d se encontra entre a e b.

Ser denso reflete a forma como os números racionais são distribuídos ao longo de uma reta numerada. Qualquer segmento de reta, não importa quão pequeno seja, será sempre ocupado por infinitos números racionais. Deste modo, pode-se concluir como os gregos fizeram, que a reta inteira é ocupada por números racionais.

Contudo, em matemática, a intuição, muitas vezes, pode conduzir a uma conclusão falsa. Um dos acontecimentos mais fantásticos na história da matemática foi a descoberta que os números racionais, apesar de densos, deixam "buracos"na reta; existindo pontos que não correspondem a números racionais. E assim o conjunto $\mathbb{Q}$ náo é tão denso como se pensava.

Terminou-se por descobrir que o número $\sqrt{2}$ não é um número racional. Conta

a história que a escola pitagórica ficou desapontada, pois neste caso, havia-se chegado a um ponto que podia ser marcado na reta, mas que não era um número racional. A revolta foi tão significativa que os pitagóricos se recusaram a admitir $\sqrt{2}$ como um número, e como a diagonal de um triângulo retângulo de lados iguais a 1 é $\sqrt{2}$, diziam os pitagóricos que a diagonal desse triângulo retângulo era indefinível. Uma prova, fácil de se entender, de que $\sqrt{2}$ é irracional, se encontra no capítulo 3 de Janos (2009) e que π e π^2 são irracionais, onde uma prova, bem mais complexa, pode ser encontrada no teorema 1 do capítulo, volume II de Spivak (1970).

No caso do conjuntos dos números racionais $\mathbb{Q}$, entre duas frações quaisquer, não importa quão próximas sejam, sempre se pode inserir outra fração. Genericamente, se temos as frações $1/p$ e $1/q$, sempre se pode inserir infinitas novas frações, e neste caso, podemos inserir $(1/p + 1/q)/2$. Consequentemente, qualquer resultado de uma medição, pode ser expressa em termos de números racionais, porque a precisão de uma medição é limitada pela construção dos instrumentos de medição Janos (2009). O que se pode esperar é, no máximo, alcançar um resultado aproximado, no que os números racionais são suficientes.

3.6 Números Irracionais

A descoberta atribuída a Pitágoras (571 a.C.-496 a.C.), filósofo e matemático grego que viveu entre os séculos VI-V a.C, foi a dos números **irracionais**, por meio de segmentos de reta incomensuráveis. Isto pode ter sido o resultado de seu interesse pela ideia de média geométrica. A média geométrica de um conjunto de números positivos é definida como o produto de todos os membros do conjunto, elevado ao inverso do número de membros. Qual era a média geométrica de 1 e 2, os dois símbolos sagrados na época de Pitágoras ? Esta questão conduziu ao estudo da razão entre a diagonal e o lado de um quadrado, hoje conhecida por $\sqrt{2}$, seguindo a ideia do cálculo de média geométrica de Pitágoras, descobriu-se que esta razão não podia ser expressa pelos números **racionais** da época, os únicos números que eram reconhecidos como tal Struik (1987).

Veja a explicação em JANOS (2009). Podemos procurar números **irracionais** na reta dos números, usando uma sequência de **intervalos aninhados**, onde cada intervalo é inserido dentro de uma intervalo maior.

O conceito de números reais surgiu a partir da utilização de **frações** comuns pelos Egípcios, por volta do ano 1000 a.C. O desenvolvimento da noção manteve-se com a contribuição dos gregos, que proclamaram a existência dos números irracionais.

Os números **reais** são os que podem ser expressos por um número inteiro (3, 28, 1568) ou decimal (4,28; 289,6; 39985,4671). Significa que abarcam os números **racionais** (que podem ser representados como o quociente de dois inteiros com denominador diferente de zero) e os números **irracionais** (os que não podem ser expressos como

uma fracção de números inteiros com denominador diferente de zero).

Considere que um número **real** está definido por um decimal como 3,5712... . A vírgula (ponto) decimal nos fornece uma sequência de aproximações racionais do número 3; ou seja, 3,5; 3,57; 3,571; ... Isto é, cada aproximação fornece um novo ponto na reta dos números no intervalo [3,0 - 4,0], depois [3,5 - 3,6], depois [3,570 - 3,571], e assim por diante. A palavra "aninhado"significa que cada novo intervalo est[a compreendido no intervalo anterior. Assim, os comprimentos desses intervalos aninhados vão diminuindo (1; 0,1; 0,01; 0,001; ...). Como estamos considerando um decimal com infinitos termos, estes intervalos serão tão pequenos quanto desejarmos, ou que, o comprimento dos intervalos corresponde a um sequência que tende a 0.

Considerando, agora, o seguinte axioma:

"Cada sequência de intervalos aninhados corresponde precisamente a um **único** ponto na reta dos números, que é contido por todos esses intervalos."

Se considerarmos que existe **mais de um** ponto comum a todos os intervalos aninhados, e os intervalos tendem para 0, será impossível ter **dois** pontos contidos num intervalo com comprimento menor que a distância entre eles.

Portanto, por definição, este ponto é chamado de um **número real**. Se esse número **real** não for **racional**, ele será **irracional**.

Por que se deve aceitar este axioma, e o que é esse ponto pertencente a todos os intervalos? Porque ele gera conclusões úteis e consistentes dentro da teoria matemática. Aceitamos este axioma, da mesma forma que aceitamos que "dois pontos definem uma única reta", ou que "todo número natural tem um sucessor"Janos (2009).

Agora, supondo que o número procurado p, se encontra no intervalo [2,7 - 2,8]. Procurando p no intervalo, vamos, através dos intervalos aninhados, construindo a sequência de comprimentos dos intervalos tendendo a 0: [2,7 - 2,8], [2,71-2,72], [2,715-2,716], e assim por diante, com os comprimetos dos intervalos tendendo a 0. Então, se, em em dos passos p estiver em um dos pontos extremos de um intervalo, p será um número racional do tipo 2,71515, isto é, 2,7151000... Mas, **se p não for um desses extremos**, **então p será irracional**.

Os números irracionais, que são representados por **expressões decimais não periódicas** pode ser representado por **frações contínuas**. Por exemplo:

$$\sqrt{6} = 2 + \cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ldots}}}}}$$

que escrevemos $\sqrt{6} = [2, 2, 4, 2, 2, 4, ...]$

Muitos números **algébricos irracionais** produzem frações contínuas periódicas relativamente simples. Por exemplo:

$\sqrt{2} = [1, 2, 2, 2, ...]$

$\sqrt{3} = [1, 1, 2, 1, 2, 1, 2]$

O número π também pode ser representado como uma **fração contínua**, neste caso, **não-periódica**.

$\pi = [3, 7, 15, 1, 292, 1, 1, ...]$ ou $\pi = 3 + \cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292+\cfrac{1}{\cdots}}}}}$

Porém, **como encontrar um ponto não extremo ?** A resposta está nos **cortes de Dedekind**, como será descrito a seguir.

Encontrando irracionais - Cortes de Dedekind

Uma forma equivalente de encontrar números **irracionais**, foi apresentada pelo matemático alemão. **Julius Wilhelm Richard Dedekind** (1831-1916).

Figura 16 – Dedekind - O método para encontrar irracionais.

Fonte: https://www.wikipedia.org/wiki/Richard$_D$*edekind*.

Em Janos (2009), Capítulo 1, p.8, é mostrado o método de **Dedekind** para encontrar números irracionais.

A teoria dos irracionais atula, desenvolvida por **Dedekind** e **Weierstrass** (), segue literalmente o modo de pensar grego de **Eudoxo** (a quem é atribuida a teoria das proporções, mas com os métodos da artimética moderna, que avriram perspectivas mais amplas.

3.7 Números Reais

Muito tempo depois, o conjunto dos números **irracionais** foi unido ao conjunto dos **racionais** $\mathbb{Q}$, gerando os números reais $\mathbb{R}$. Um número **real** é aquele que pode ser escrito na forma decimal, sejam as casas decimais finitas, como por exemplo, $7,2$ ou com infinitas repetições, como em $1,235235235...$, ou mesmo os que nunca se repetem, como em, $1,101001000100001...$, em que depois de cada 1 segue um número maior de zeros.

É bem conhecido que os números que terminam com decimais finitas ou com repetições são **racionais**. E os que nunca se repetem são **irracionais**.

O *continuum* dos números reais é composto pela totalidade dos números decimais finitos e infinitos. Os racionais infinitos são os que contém decimais periódicas (dízimas periódicas), por maior que seja esses períodos, e os irracionais os não periódicos.

A **aritmética** abrange o estudo de **procedimentos manuais** para a realização de operações com os números **naturais**, **inteiros**, **racionais** e **reais**.

3.7.1 Números Algébricos

A maioria dos números que encontramos quando estudamos álgebra podem ser imaginados como soluções de equações algébricas. Por exemplo:

O número 1, $2/3$, $\sqrt{2}$ e $i = \sqrt{-1}$ são soluções das equações:

$x - 1 = 0$, $3x - 2 = 0$, $x^2 - 2 = 0$, $x^2 + 1 = 0$

Números reais ou complexos (será visto adiante), como os acima, são uma solução de uma **equação polinomial** com coeficientes inteiros, são chamados **algébricos**. Desta forma, qualquer número **racional** a/b é **algébrico**, pois satisfaz a equação $bx - a = 0$. Logo,, se um número é **não-algébrico**, isto é, não é da forma a/b, então ele não será **racional**, e portanto será **irracional**. Contudo, um número **irracional** também pode ser **algébrico**. Veja o exemplo da solução da equação $x^2 - 2 = 0$.

Um número que a solução da equação polinomial $a_0.x^n + a_1.x^{n-1} + a_2.x^{n-2} + ... + a_{n-1}.x + a_n = 0$, onde $a_0 \neq 0$, a_1, a_2, ..., a_n são inteiros e n um inteiro positivo, chamado de grau da equação, é um número **algébrico**.

A questão que surge é: existem números **irracionais**, **não-algébricos** ? Ou de outra forma, existem números que não são raízes de uma equação polinomial com coeficientes inteiros ?

3.7.2 Números Transcendentais

O que se sabe é que por volta de 1850 um novo tipo de número foi descoberto (pelos platonistas): os números transcedentais.

Joseph Liouville (1809-1882) foi um matemático francês que provou a existência de **números não algébricos**. Considere o número 0,12345678910111213... cuja parte decimal é a sequência dos naturais, ele é **não-algébrico**. Tais números foram chamados de **transcendentais**, porque transcendem aos números que podem ser soluções de equações polinomiais.

Figura 17 – Joseph Liouville e os números transcedentais.

Fonte: https://pt.wikipedia.org/wiki/Joseph$_L$*iouville*.

Liouville fundou o *Journal de Mathématiques Pures et Appliquées*. Embora tenha trabalhado em todas as áreas da matemática pura e aplicada, é sobretudo conhecido por ter sido o autor da primeira demonstração da existência de números **transcendentes**.

Os números **transcedentais**, inicialmente, eram considerados como números raros. Mas, aos poucos, foram sendo descobertos, como os dois casos mais famosos na matemática: os números π e o número e.

Também, não é nada fácil provar que um número é **transcedental**, pois para isso, deve-se provar que ele é não-algébrico, isto é, ele não é solução de nenhuma equação polinomial. Em 1929 foi provado que e^{π} é transcedental.

Quando falamos de números transcedentais, estamos falando dos definidos como números **normais**. Um número normal na base 10 (decimal) é aquele que, em média, cada dígito decimal aparece 10 por cento das vezes. Como também, um par de dígitos sucessivos, como por exemplo, 75, aparecerá 1 por cento das vezes, e cada tripla de digitos, como por exemplo, 763 aparecerá 0,1 por cento das vezes, e assim por diante. O conceito de números normais vale em qualquer base, e os números **transcedentais** são, provavelmente, números **normais**.

Embora não seja o que nossa intuição mostre, mas, na verdade, o que se conhece é que existem mais números **irracionais** do que **racionais**. E existem mais números **transcedentais** do que **algébricos**. Interessante, que além de não serem nada raros, os números **transcedentais** são a maioria entre os **irracionais**, como menciona Janos (2009).

3.7.3 O Números Incomputáveis

Ao surgir a Ciência da Computação, veremos que um novo tipo de número, no conjunto dos números reais, apareceu: os **números computáveis**. Esses números são os que podemos calcular com uma quantidade finito de operações dentro do que veio a ser chamado de **algoritmo**, uma sequência finita de passos (computacionais) para se chegar a conclusão de alguma tarefa. Por exemplo, o número π é um exemplo, calculado pela divisão do comprimento de uma crcunferência pelo seu diâmetro. Contudo, como veremos no capítulo sobre "**Computabilidade**", existem números reais que não podem ser calculados a partir de um **algoritmo**. Esses são chamados de **números incomputáveis**. Esse tipo de número é importante, para a ciência da computação, pois surgiram das limitações de uma máquina computacional ou, em outros termos, **limitações dos sistemas computacionais**, como descoberto por, **Alan Turing** e **Alonzo Church** no século XX, meado da década de 30.

3.8 Os Números Complexos

A sequência de tipos de números começou com os inteiros positivos e expandiu para os inteiros negativos, depois os racionais e depois os irracionais, advindo, então, os reais e por fim, culminaram com os **números complexos**. Por exemplo, resolver a equação $x^2 - 2 = 0$, tornou necessário a introdução de números irracionais (no caso, $x = \sqrt{2}$ é raiz desta equação), o que faz aparecer um irracional ($\sqrt{2}$) algébrico. Em outro caso, temos a equação quadrática do tipo $x^2 + 1 = 0$, não possui soluções nos números reais, porque tem-se $x = \sqrt{-1}$, e não se pode calcular a raiz quadrada de um número negativo. Assim, ou se considerava que este tipo de equação era insolúvel ou o conceito de número, outra vez, deveria ser estendido para um novo conjunto mais amplo, com um novo símbolo que permitisse que a equação tivesse uma solução. Foi exatamente isto que foi feito, quando se definiu $\sqrt{-1}$ e foi introduzido o símbolo **i**, definido como $i^2 = -1$, a **unidade imaginária**, como Descartes disse ser esses números.

Assim, os sistemas de números, nem sempre estão ligados aos números **reais**. Este é o caso dos números **complexos** que não se prestam para "**contar**". Sua existência é devido à necessidade de se expandir o campo dos números **reais**, oferecendo um novo tipo de número, uma nova ferramenta consistente que atende às regras da aritmética com esses números.

O conceito de **número complexo** teve um desenvolvimento gradual. Começaram

a ser utilizados formalmente no século XVI (anos 1500) em fórmulas de resolução de equações de terceiro e quarto graus Cerri e Monteiro (2001). Os primeiros que conseguiram dar soluções a equações cúbicas foram **Scipione del Ferro** e **Tartaglia**. Este último, depois de ter sido alvo de muita insistência, passou os resultados que tinha obtido a **Girolamo Cardano**, que prometeu não divulgá-los. **Cardano**, depois de conferir a exatidão das resoluções de **Tartaglia**, não honrou sua promessa e publicou os resultados em sua obra *Ars Magna* em 1545.

A impossibilidade de se resolver equações do tipo $x^2 + a = 0$, quando a é positivo, era conhecida há séculos. E em 1545, **Cardano** tentou descobrir dois números cuja soma era 10 e cujo produto era igual a 40. Isto o levou à equação quadrática:

$x + y = 10 \; xy = 40$

$y = 10 - x = \frac{40}{x}$

$10x - x^2 = 40$

$x^2 - 10x + 40 = 0$, que fornece duas soluções $5 + \sqrt{-15}$ e $5 - \sqrt{-15}$

Inicialmente, **Cardano** não soube o que fazer com estas "soluções". Ele não sabia os que estes valores significavam. Mas, intrigado, Cardano resolver dar a estas o tratamento ordinário da álgebra, e notou que ambas as soluções satisfaziam as condições iniciais do problema, isto é:

$(5 + \sqrt{-15}) + (5 - \sqrt{-15}) = 10$ e $(5 + \sqrt{-15})(5 - \sqrt{-15}) = 40$.

É mesmo ? Façam as contas.

Hoje, quando temos equações cúbicas do tipo $ax^3 + bx^2 + cx + d = 0$, sabemos que elas requerem soluções nos números **complexos**, mesmo que as soluções sejam números **reais** (pois eles fazem parte do conjunto dos números **complexos**).

Em 1835, Hamilton deu um tratamento formal aos números complexos, definindo-os como uma par ordenado (x,y), sendo x e y reais e obedecendo aos axiomas:

1. Dois números complexos (a, b) e (c, d) são iguais se $a = c$ e $b = d$.
2. $k(a, b) = (ka, kb)$
3. $(a, b) + (c, d) = (a + c, b + d)$
4. $(a, b)(c, d) = (ac - bd, ad = bc)$

Sobre os números complexos é possível provar que os números complexos são **completos**, ou o que é o mesmo de dizer que representam um **conjunto fechado**, o que significa que qualquer operação com números complexos resultará também em um número complexo. Isto não acontece com os **inteiros**, pois quando dividimos dois inteiros, o resultado não é outro inteiro. E também isto não acontece com os reais, pois a raiz quadrada de -1 (um número real), o resultado não é real, ou seja é um número complexo. Assim, os **reais** não formam um **campo ou corpo fechado**, ou seja, não são **completos**.

E o resultado mais surpreendente da álgebra, chamado o **Teorema Fundamental da Álgebra**, prova que:

"**Todo polinômio de grau n tem sempre n raízes complexas**"

O que dá importância ao fato, de que é importante existir **números complexos**. O leitor encontrará mais sobre este teorema, no capítulo sobre que explica os **anéis de polinômios**.

Durante o século XIX muitos esforços foram feitos para se obter base mais sólida para a álgebra. Portanto, o sistema de números passou a ser visto de uma maneira integrada, onde diferentes classes de números foram organizadas de foma mais consistente, mostrando-se cada classe como subconjunto de outras como está em $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ e que também $\{\mathbb{Q} \cup \mathbb{I}\} \subset \mathbb{R}$

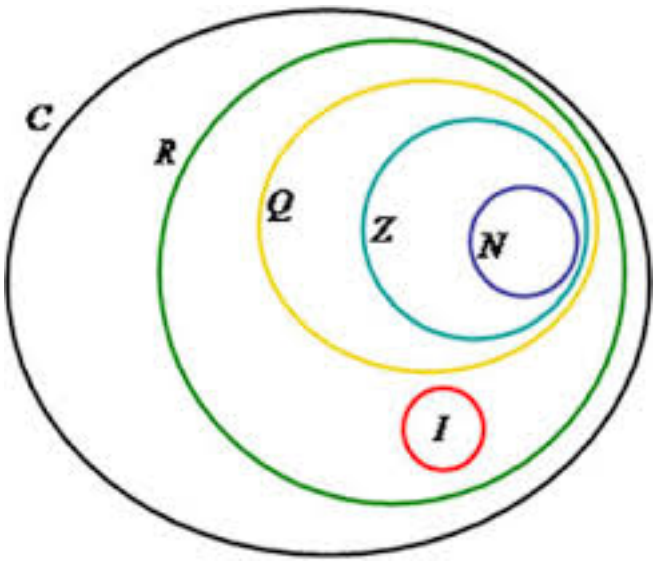


Figura 18 – Os conjuntos de números: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$.

Fonte: www.brasilescola.com.

3.9 Mais Números

Neste ponto, outras perguntas podem ser levantadas:

1. Além do números complexos, são necessários outros tipos de números ?
2. Podem os números complexos fazer parte de outro tipo ainda mais abrangente ?

Para a álgebra clássica (elementar) não é preciso de tal extensão. De fato, pode ser provado que o conjunto $\mathbb{C}$dos números complexos não pode ser estendido. Números complexos são necessários e suficientes para resolver qualquer problema da álgebra clássica no plano (em duas dimensões), ou seja no espaço $\mathbb{R}^2$. Se a dimensão do espaço for maior que 2, o caminho deve ser outro.

Para um estudo mais aprofundado sobre esta questão, o leitor pode estudar o trabalho de **Hamilton**. **William Rowan Hamilton** (1805-1865) foi um matemático, que contribuiu com trabalhos fundamentais ao desenvolvimento da álgebra. A sua descoberta mais importante em matemática é a dos **quaterniões**, uma quadra ordenada $q = (a, b, c, d)$, para representar pares de números complexos $(a + bi, c + di)$, em que a, b, c, d são números reais. Esse novo sistema de números teria que ser consistente com os axiomas e as operações fundamentais da aritmética. Assim, **Hamilton** pode introduzir os **quartenions** no plano tridimensional. A motivação que o levou a desenvolver um novo sistema de números foi originada no problema da multiplicação de dois vetores num espaço vetorial tridimensional $(3D)$.

3.10 Classificacão dos Números

Para resumir: um número é a expressão de uma quantidade em relação à sua unidade. O termo vem do latim e refere-se a um símbolo ou um conjunto de símbolos. A Teoria dos Números agrupa estes símbolos em distintos conjuntos. Pode-se, por fim, organizar os números (os mais usados por nós) dividindo-os em sistemas como na classificação abaixo. De forma geral, os tipos de números mais importantes, para os matemáticos e para os cientistas da ciência da computação são classificados como:

- Números: **Reais** ou **Complexos**;
- **Reais**: **Racionais** ou **Irracionais**;
- **Racionais**: **Inteiros** (incluindo os naturais) ou **Frações Puras** (1/2, 1/3/, 1/4, ...);
- **Irracionais**: **Algébricos** ($\sqrt{2}$), **Transcedentais** (π, e, ...) ou **Incomputáveis** (**???**);
- **Naturais**: **Pares** ou **Ímpares**;

- **Naturais**: **Primos** ou **Não-Primos**.

Desta classificação, podemos destacar os tipos de números que são **computáveis**: reais racionais (inteiros e frações puras) ou reais irracionais (algébricos e transcedentes).

3.11 Outros Números

Número perfeito: número cuja soma de seus divisores (excluído o próprio número) é igual a ele mesmo (p. ex.: 6). O número 26 é o único que existe que se encontra entre um quadrado ($25 = 5^2$) e um cubo ($27 = 3^3$) (provado por Pierre de Fermat). O número 69 é o único que existe cujos algarismos que compõem seu quadrado ($69^2 = 4761$) e seu cubo ($69^3 = 328509$) formam todos os números entre 0 e 9 sem repetição. O número de **Skewes** ($10^{10^{10^{34}}} = 10^{10^{10.000.000.000.000.000.000.000.000.000.000.000.000}}$) é um dos maiores números que já serviram a algum propósito em Matemática. O número de **Graham**, ainda maior, aparece em problemas de combinatória.

3.12 Definições de Números

O conceito de número, na sua forma mais simples, é claramente abstrata e intuitiva. Entretanto, foi objeto de estudo de diversos pensadores. **Pitágoras de Samos** (cerca de 571 a.C. ou 570 a.C.-497 a.C. ou 496 a.C.), por exemplo, considerava o número a essência e o princípio de todas as coisas; para **Arthur Schopenhauer** (1788-1860) o conceito numérico apresenta-se como a ciência do tempo puro.

Outras definições de *número* são:

- Número é a relação entre a quantidade e a unidade, **Isaac Newton** (1643-1727).
- Número é um composto da unidade, **Euclides de Alexandria** (360 a.C.-295 a.C.).
- Número é uma coleção de objetos de cuja natureza fazemos abstração, **Émile Boutroux** (1845-1921).
- Número é o resultado da comparação de qualquer grandeza com a unidade, **Benjamin Constant** (1767-1830).
- Número é o movimento acelerado ou retardado, Aristóteles (384 a.C.-322 a.C.).
- Número é uma coleção de unidades, **Tales de Mileto** (cerca de 624 ou 625 a.C.-556 ou 558 a.C.) e **Marie Jean Antoine Nicolas Caritat** (1743-1794).
- Número é a razão entre uma quantidade abstrata e uma outra quantidade da mesma espécie, Isaac Newton (1643-1727).
- Número é a classe de todas as classes, equivalente a uma dada classe, **Bertrand Russell** (1872-1970) em Principia Mathematica).

3.13 Bibliografia e Fonte de Consulta

Luiz Henrique Jacy Monteiro - Elementos de Álgebra, IMPA, 1969.

Michel Janos (2009). Matemática e Natureza. Editora da Física.

Teoria dos Números - https://pt.wikipedia.org/wiki/Teoria_dos_números

Rosana Madjarof e Carlos Duarte. Pitágoras de Samos Mundo dos Filósofos (http://-www.mundodosfilosofos.com.br/pitagoras.htm). Visitado em 27 de Outubro de 2015.

Guilherme Marconi Germer (Segundo semestre 2010). O conhecimento do belo em Schopenhauer. Revista Voluntas: estudos sobre Schopenhauer-Vol. 1-N2-ISSN:2179-3786-pp.89-97.

Salahoddin Shokranian. Uma breve história da teoria dos números. : Ciência Moderna.

Humberto José Bortolossi (21 de março de 2011). Pré Cálculo (). Departamento de Matemática Aplicada, Universidade Federal Fluminense. Visitado em 27 de Outubro de 2015.

Alfred North Whitehead and Bertrand Russell (1910). Principia mathematica (vol I) (em inglês) Cambridge: University Press. Visitado em 27 de Setembro de 2015.

Alfred North Whitehead and Bertrand Russell (1910). Principia mathematica (vol II) (em inglês) Cambridge: University Press. Visitado em 27 de Setembro de 2015.

Alfred North Whitehead and Bertrand Russell (1910). Principia mathematica (vol III) (em inglês) Cambridge: University Press. Visitado em 27 de Setembro de 2015.

3.14 Referências - Leitura Recomendada

Números - https://pt.wikipedia.org/wiki/Número

Majungmul; Lee, Ji Won; Trad. Elizabeth Kim. A origem do número. Callis Editora, 2010.

Izabel Galvão. História da Matemática: dos Números a Geometria. Edifieo.

Rosana Madjarof e Carlos Duarte. Pitágoras de Samos Mundo dos Filósofos. Visitado em 27 de fevereiro de 2012. ⟨http://www.mundodosfilosofos.com.br/pitagoras.htm⟩

Iran Abreu Mendes. Número: o Simbólico e o Racional na História. Livraria da Física.

Hércules de Araújo Feitosa; Mauri Cunha do Nascimento; Alexys Bruno Alfonso. Teoria dos Conjuntos - Sobre a Fundamentação Matemática e a Construção de Conjuntos Numéricos. [S.l.]: Ciência Moderna.

Iran Abreu Mendes. Número: o Simbólico e o Racional na História. Livraria da Física.

Elementos de Arithmetica, por João José Luiz Vianna, capítulo II, p.59. Texto disponível no Wikisource.

An Imaginary Tale: The Story of i (the square root of minus one), por Paul J. Nahin, no site Princeton University Press.

Antonio González Carlomán, Didáctica del número natural, Universidad de Oviedo, 1984 ISBN 8-474-68094-8 (em espanhol).

Russell, Bertrand (2007), "1. A série dos números naturais" (em português) (Livro), Introdução à filosofia matemática, Zahar, ISBN 8-571-10970-2.

Georges Ifrah, HISTORIA UNIVERSAL DOS ALGARISMOS - TOMO I a inteligência dos homens contada pelos números e pelo cálculo, NOVA FRONTEIRA ISBN 978-852-090-841-9 Sinopse.

Célia Maria Carolino Pires, Números Naturais e Operações , Editora Melhoramentos, 2013, ISBN 8-506-07233-6.

"Zero", MCS, UK: ST-And, "... uma tábua encontrada em Kish... com uma data estimada em cerca de 700 a.C., utiliza três ganchos para representar um espaço vazio na notação posicional. Outras tábuas datadas da mesma época utilizam um único gancho para representar um espaço vazio.".

CAPÍTULO 4

Os Números Primos

A palavra *primos* vem do latin *primus*, *principal* e *prime* em inglês. Os números primos tem uma longa história. Foi **Pitágoras** (570 a.C) quem primeiro entendeu seu conceito e era interessado nas suas propriedades. **Euclides** (300 a.C) provou que eles são **infinitos** e formulou o **Teorema Fundamental da Aritmética**. Eles são colocados aqui porque exercem um papel importante na Teoria dos Números e tem muito utilidade nas técnicas usadas em determinados algoritmos de criptografia, usados na área de segurança da informação.

4.1 Divisibilidade

Antes de entendermos a definição de um número primo, precisamos saber o que significa um inteiro ser divisível por outro inteiro. Neste caso, existe uma relação de divisibilidade sobre $\mathbb{Z}$.

Definição (**Divisores**)

Sejam a e b dois números inteiros. Diz-se que b é um divisor de a se, e somente se, existe um inteiro c tal que $a = b.c$. Usa-se a notação $b \mid a$ para indicar que b é um divisor de a; neste caso, também se diz que b divide a ou que b é um fator de a ou que a é um múltiplo de b. A relação "b é divisor a, indicada com "é denominada relação de divisiblidade sobre $\mathbb{Z}$. Note que $a \mid 0$ para todo inteiro a e que $0 \mid a$ se, e somente se $a = 0$. Por causa desta última propriedade costuma-se excluir o caso em que o divisor é nulo. Isto é considera-se a restrição da relação da divisibilidade ao subconjuto $\mathbb{Z}^* \times \mathbb{Z}$, onde $\mathbb{Z}^* = \mathbb{Z} - 0$.

Definição (**Máximo Divisor Comum - MDC**)

Se a e b são dois números inteiros então, todo inteiro c tal que $c \mid a$ e $c \mid b$ é denominado divisor comum de a e b.

Definição (**MDC**)

Diz-se que um número inteiro d é um *máximo divisor comum* de dois inteiros a e b se, e somente se, são válidas as seguintes condições: (D1) $d \mid a$ e $d \mid b$, (D2) para todo número inteiro d', se $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

Definição (**Mínimo Múltiplo Comum - MMC**)

Para todo número inteiro a indicamos por $\mathrm{M}(a)$ o conjunto de todos os números inteiros que são múltiplos de a.

4.2 O que são Números Primos

Definição (**O que é um Número Primo**)

Um número inteiro $p > 1$ é um número primo , quando ele tem exatamente dois **divisores**: o número 1 e ele mesmo. Ou seja, um número é primo se ele é somente **divisível** por ele mesmo e pela unidade 1. Isto é, um número é primo, se e somente se, seus únicos **divisores** forem $+1$, -1, $+p$ e $-p$.

Definição (**Primos entre si**)

Diz-se que dois números inteiros a e b são primos entre si , se e somente se, $\mathrm{MDC}(a, b) = 1$.

Teorema (**Teorema Fundamental da Aritmética**)

Aqui está uma menção ao teorema fundamental da aritmética . Todo número inteiro a, com $a \neq 0$ e $a \neq \pm 1$ é igual a um produto de números primos. Além disso, se $a = p_1.p_2.\ldots.p_s = q_1.q_2.\ldots.q_t$ são duas decomposições de a, como produtos de fatores primos, $s = t$ e $p_i = \pm q_i$, para $i = 1, 2, \ldots, s$. Estas decomposições chamam-se **fatoração**.

Corolário 1 (**Inteiros maiores ou igual a 2**)

Todo número inteiro $a \geq 2$ (estritamente maior que 1, portanto, natural) pode ser representado de modo único (a menos da ordem dos fatores) como igual a um produto de números primos *positivos*.

A prova deste corolário é dependente das definições de MDC e MMC.

Consequentemente, podemos ter que qualquer inteiro a, tal que $a \neq 0$, $a \neq \pm 1$, temos que:

$a = p_1^{a_1}.p_2^{a_2}...p_n^{a_n}$,

onde $p_1 < p_2 < ... < p_n$ são primos e cada a_i, para $i \in \mathbb{N}^*$ é um expoente inteiro positivo.

Chamamos cada $p_i^{a_i}$, para $i = 1..n$ de fator do número primo a e o conjunto

$$\{p_i^{a_i} \mid i = 1..n\}$$

são os fatores primos do número a. O que este teorema diz é que qualquer inteiro a, tal que $a \neq 0$, $a \neq \pm 1$, para a pode ser feita uma **decomposição em fatores primos**.

Exemplos:

- $91 = 7 \times 13$
- $2 = 1 \times 2$
- $3600 = 2^4 \times 3^2 \times 5^2$
- $11011 = 7 \times 11^2 \times 13$
- $1368 = 2 \times 3 \times 3 \times 7 \times 11$

Se $\mathbb{P}$ for o conjunto dos números primos, então qualquer inteiro positivo a pode ser expresso como:

$a = \times p \in \mathbb{P} p^{a_p}$, onde $a_p \geq 0$ e para qualquer valor de a, a maioria dos expoentes a_p será 0.

Corolário 2 (Um só fator primo positivo)

Todo número inteiro $a \neq 0$ e $a \neq \pm 1$ admite, pelo menos, um fator primo positivo.

As provas destes teoremas e corolários não são colocadas aqui. Existem vários livros sobre Teoria dos Números, onde pode ser encontrada, como por exemplo em Janos (2009) ou em Monteiro (1969).

4.3 Decomposição em Fatores Primos

Aprendemos a decomposição em fatores primos no ensino médio, mas não sabemos onde o conceito será útil. Mas, na matemática, área da critografia, esta decompisição é muito útil. Todo número natural, maior que 1, pode ser decomposto num produto

de dois ou mais fatores primos.

Decomposição do número 24 num produto $24 = 4x6$, $24 = 2x2x6$ ou $24 = 2x2x2x3 = 2^3x3$. Veja que no produto $2x2x2x3$, todos os fatores são primos. Chamamos de fatoração de 24 a decomposição de 24 num produto de fatores primos. Então a fatoração de 24 é 2^3x3.

De um modo geral, chamamos de **fatoração** de um número natural, maior que 1, a sua **decomposição num produto de fatores primos**.

Regra prática para a fatoração

Existe uma regra prática para fatorar um número natural. Veja, no exemplo, os passos para aplicando a regra:

1. Dividimos o número pelo seu menor divisor primo;

2. a seguir, dividimos o quociente obtido pelo menor divisor primo desse quociente e assim sucessivamente até obter o quociente 1.

A Figura 19 mostra a fatoração do número 630.

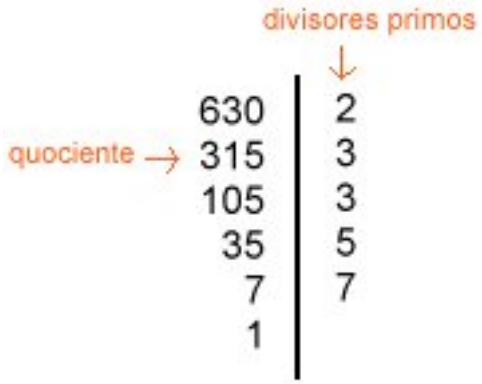


Figura 19 – Exemplo de decomposição em fatores primos.

Fonte: http://www.somatematica.com.br/fundam/decomp.php.

Então $630 = 2x3x3x5x7$ ou $630 = 2x3^2x5x7$.

Num caso mais geral para a sendo inteiro e $a \neq 0$ e $a \neq \pm 1$, é que, por exemplo, temos $30 = 2.3.5$ que é uma decomposição de 30 num produto de fatores primos. A partir desta decomposição podemos ter:

$30 = (-2)(-3)5 = (-2)(3)(-5) = 2(-3)(-5)$, e depois podemos alterar em cada uma destas decomposições a ordem dos fatores.

Tabela 1 – Distribuição Média de Primos até o Inteiro N

N	Q(N)	Q(N)/N (Densidade)	Probabilidade
10	4	0.4	0.4
100	25	0.4	0.4
1 000	168	0.168	1.7
10 000	1 229	0.1229	1.2
100 000	9 592	0.09592	0.9
1 000 000	78 498	0.078498	0.7
10 000 000	664 579	0.0664579	0.6
100 000 000	5 761 455	0.05761455	0.6
1 000 000 000	50 847 534	0.050847534	0.5

Fonte: Michel Janos, Matemática e Natureza, Cap.1, p.24.

4.4 Distribuição dos Números Primos

Teorema (**Infinitos Números Primos**)

Existem infinitos números primos.

A prova deste teorema é devida a Euclides no século III a.C.; a prova, o leitor poderá ver em Janos (2009) ou em Monteiro (1969).

Teorema (**Teorema da distribuição dos números primos**)

Os matemáticos algebristas sempre procuravam buscar as leis que governassem a distribuição dos números primos. Entretanto, quando os matemáticos desistiram de procurar uma fórmula de geração dos números primos (ou que fornecesse a quantidade de primos contida nos primeiros números inteiros N), o passo decisivo foi quando partiram em busca da **distribuição média** de números primos entre os inteiros, como pode ser vista na Tabela 1.

Se chamarmos $Q(N)$ a quantidade de números primos até o valor inteiro N, obtemos a seguinte distribuição média de primos entre o inteiro N:

A coluna $Q(N)/N$ da Tabela 1 pode ser interpretada como a probabilidade que um inteiro selecionado aleatoriamente até o valor N tem de ser primo.

A distribuição dos primos entre os inteiros é extremamente irregular, mas quando verificamos para a densidade dos números primos dada pela razão $Q(N)/N$, a irregularidade parece dar lugar a certa regularidade. Essa regularidade é verificada na Tabela 2 quando verificamos que:

$Q(N)/N) = \frac{1}{lnN}$

Tabela 2 – Visão da Regularidade quando $Q(N)/N = 1/(lnN)$

N	Q(N)/N (1)	1/(ln N) (2)	(1)/(2)
1 000	0.168	0.145	1.159
1 000 000	0.078498	0.072382	1.084
1 000 000 000	0.050847534	0.0482549	1.053
10 000 000 000	0.0455052512	0.04342944	1.047

Fonte: Michel Janos, Matemática e Natureza, Cap.1, p.24.

onde lnN é o logaritmo natural (de base e), como pode ser visto na Tabela ... (seguinte)

O valor da coluna (1)/(2) é: $\frac{Q(N)}{N} = \frac{1}{lnN}$, donde $Q(N) = \frac{N}{lnN}$

Esta conclusão é conhecida como o **Teorema dos Números Primos**.

Em termos da distribuição dos números primos, pode-se considerar quantos números provavelmente serão rejeitados antes que um número primo seja encontrado, usando um teste de números primos. Um resultado da Teoria dos Números, conhecido como Teorema dos Números Primos, afirma que os primos próximos de N são espaçados em média cada lnN inteiros. Assim, na média, teríamos que testar algo na ordem de lnN, antes que um número primo fosse encontrado. Como todos os inteiros pares podem ser imediatamente rejeitados, o valor correto é $0.5 \times lnN$. Por exemplo, se um primo da ordem de grandeza de 2^{200} fosse procurado, então seriam necessários cerca de $0.5ln(2^{200}) = 69$ tentativas para encontrar um número primo. Mas, esse valor é uma média. Em alguns lugares ao longo da linha dos números, os primos são mais próximos, e em outros lugares eles estão mais espaçados. Vejamos o exemplo de Stallings (2008):

Os dois inteiros ímpares consecutivos 1.000.000.000.061 e 1.000.000.000.063 são ambos primos. Eles estão bem próximos. Por outro lado, na sequência:

$$\langle 1001! + 2, 1001! + 3, 1001! + 5, ..., 1001! + 1000, 1001! + 1001 \rangle$$

de 1000 números inteiros **compostos**, os primos estão bem mais espaçados. Um inteiro maior que 1 e que não é primo diz-se **inteiro composto**.

Saber que a densidade dos números primos $Q(N)/N$ pode ser descrita por uma *função logaritmica* foi uma descoberta bastante interessante, porque, intuitivamente, é difícil de se enxergar que a densidade e a função logarítma estejam relacionadas. **Gauss** foi quem fez esta observação. Embora, a prova deste teorema não tivesse sido feita naqueles tempos, só se conseguiu a prova, quase 100 anos mais tarde, por **Jacques Salomon Hadamard** (1865-1963) e **Charles de la Vallée Poussin** (1866-1962), no início do século XX.

4.5 Noções sobre Teoria dos Números

A teoria dos números é o ramo da matemática pura que estuda propriedades dos números em geral, e em particular dos números inteiros, bem como a larga classe de problemas que surge no seu estudo.

Normalmente, o primeiro contato com a teoria dos números é por meio da teoria elementar dos números. Através desta disciplina podem ser introduzidas propriedades bastante interessantes e notáveis dos números inteiros, mas, que ao serem propostas como questões a serem resolvidas, ou teoremas a serem provados, são geralmente de difícil solução ou comprovação. Estas questões estão ligadas basicamente a três tipos de pesquisas, a saber: (a) Estudos específicos sobre as propriedades dos números primos; (b) Estudos envolvendo a pesquisa de procedimentos efetivos eficientes para a aritmética básica; (c) Estudos sobre a resolução de equações diofantinas; (d) Estas questões diretamente ligadas ao estudo do conjunto dos números inteiros e o seu subconjunto: $\mathbb{N}$, o conjunto dos números naturais.

Antes de darmos alguns exemplos de aplicações de números primos, precisamos ver alguns conceitos sobre artimética modular.

4.6 Aritmética Modular - Parte I

Frequentemente, que preferirmos, em certas circunstâncias, ignorar os múltiplos de um dado número quando fazemos cálculos. É o caso dos **dias da semana** ou nas **horas do dia**; no primeiro caso ignoramos múltiplos de 7, no segundo, múltiplos de 24 (ou, muitas vezes, múltiplos de 12). Estes são exemplos de "aritmética modular".

A "aritmética do relógio"é um exemplo de aritmética módulo n, neste caso n = 12. Se forem 7:00 horas e passarem 10:00 horas, então serão 5:00 horas (7 + 10 é igual a 5 módulo 12).

Se passarem 89 horas, serão 0:00 (7 + 89 é igual a 0 módulo 12). Olhamos para o tempo entre os múltiplos de 12. A aritmética modular é a formalização matemática deste tipo de raciocínio.

Quando estamos a utilizar a aritmética usual sobre os números naturais, apenas temos como números: $\{1, 2, 3, 4, 5, ...\}$ Se em vez dos naturais considerarmos os números inteiros passamos a trabalhar com os números $\{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$.

Quais os números que se consideram nesta aritmética? Vejamos o exemplo de $20 \equiv 8(mod 12)$. Neste caso, temos que o número 20 é identificado com o número 8, ou seja, temos que o número 20 e o número 8 são equivalentes na aritmética módulo 12, porque, por definição de congruência, 12 é divisor de $(20 - 8) = 12$. Equivalente a estes dois, temos ainda uma infinidade de outros números: 32, 44, 56, ...

A este conjunto de números $\{8, 20, 32, 44, 56, 68, ...\}$ chamamos classe de equivalência módulo 12 e esta classe vai ser identificada pelo menor deles, ou seja, pelo 8. De um modo análogo, temos ainda mais 11 classes de equivalência nesta aritmética módulo 12, representadas pelos números: 0, 1, 2, 3, 4, 5, 6, 7, 9, 10, 11. E estes vão ser os nossos "números"nesta aritmética.

Generalizando, os "**números**"considerados na **aritmética modular módulo** p são: 0, 1, 2, ..., $p-2$, $p-1$, p. Uma vez que este tipo de aritmética apenas considera um número finito de "números", também se diz que a aritmética modular é uma aritmética finita.

Agora que já temos os nossos números, o passo seguinte é estudar as operações que se podem efetuar com estes números, em particular, a adição e a multiplicação.

Adição Modular - Qual o resultado da adição $(5 + 10)$ na aritmética módulo 12 ?

Na aritmética usual seria igual 15, mas para respondermos corretamente à nossa pergunta temos que saber qual é o resto que 15 tem quando é dividido por 12. Uma vez que este resto é igual a 3, dizemos que:

$5 + 12 = 5 mod 12$ ou $9 + 6 = 3 mod 12$

E se considerássemos agora o módulo 9 em vez de 12? De maneira análoga, mas neste caso a divisão considerada seria por 9 e não por 12. Uma vez que $15 = 1 \times 9 + 6$, dizemos que $5 + 10 = 6 mod 9$.

Multiplicação Modular - Qual será o resultado da multiplicação $(5 \times 10) mod 12$?

Na aritmética usual seria igual a 50, mas para respondermos corretamente à nossa pergunta temos que saber qual é o resto que 50 tem quando é dividido por 12. Uma vez que este resto é igual a 2, dizemos que $5 \times 10 = 2 mod 12$.

E se considerássemos agora, o módulo 9 em vez de 12? Procederíamos de maneira análoga, mas neste caso a divisão considerada seria por 9 e não por 12. Uma vez que $50 = 5 \times 9 + 5$, dizíamos que: $5 \times 10 = 5 mod 9$.

Teorema (**Teorema de Fermat**)

Se p é primo e a é um inteiro positivo não divisível po p, então $(a^{p-1} \equiv 1) mod p$**.**

Uma forma alternativa deste teorema aparece no que segue:

Exponenciação Modular

A exponenciação modular, caso o expoente seja um número primo, é calculada usando-se a forma alternativa do Teorema de Fermat,

Se p é um número primo e a é um inteiro positivo, então $(a^p \equiv a) mod p$.

Exemplos (**Expoentes primos**)

- $a^p = 7^2 = 49 \equiv 7 \bmod 2$, pois $a = 7$ e $p = 2$ é um primo.
- $a^p = 10^5 = 100.000 = 10 mod 5$, pois $a = 10$ e $p = 5$ é um primo.
- $a^p = 11^7 \equiv 11 \bmod 7$, pois $a = 11$ e $p = 7$ é um primo.

Exemplo (**Expoente não-primo**)

Seja $p = 4$, onde p é não-primo. Para encontrar $11^4 (mod 13)$ podemos proceder da seguinte forma:

$11^4 = (11^2)^2 = 121^2 \equiv 121 \bmod 2$

Congruência - Uma das ferramentas mais importantes na Teoria dos Números é a **congruência**.

Congruência é a relação entre dois números inteiros que, divididos por um terceiro, chamado **módulo de congruência**, deixam o mesmo resto. Por exemplo, 20 é congruente a 14 com relação a 6 pois, 20/6=3 restando 2 e 14/6=2 restando 2.

Definição (**Congruência**)

Suponha que a, b e m sejam números inteiros diferentes de zero. Dizemos que **a é congruente a b módulo** m, se m dividir $(a - b)$. Escrevemos isto como: $(a \equiv b) \bmod m$.

Exemplos:

$(20 \equiv 14) \bmod 6$, pois $20 - 14 = 6/6 = 1$, com resto $= 0$.

$(-1 \equiv 9) \bmod 5$, pois $(-1 - 9) = -10/2 = -5$, com resto $= 0$.

$(1100 \equiv 2) \bmod 9$, pois $1100 - 2 = 1098/9 = 122$, com resto $= 0$.

E, na aritmética modular, o quadrado de qualquer número ímpar é 1 módulo 8. Vejamos:

$(3^2 \equiv 1)$ mod 8, pois $9 - 1 = 8/8 = 1$, com resto = 0.

$(5^2 \equiv 1)$ mod 8, pois $25 - 1 = 24/8 = 3$, com resto = 0.

Encontramos congruências em todos os lados. Por exemplo, os relógios trabalham com módulos 12 ou 24 para as horas e módulo 60 para os minutos e segundos. Calendários usam módulo 7 para os dias da semana e módulo 12 para os meses.

Outros exemplos:

(a) $(73 \equiv 4)$ mod 23, pois $73 - 4 = 69/23 = 3$, com resto = 0. (b) $(21 \equiv -9)$ mod 10, pois $21 - (-9) = 21 + 9 = 30/10 = 3$, com resto = 0.

A linguagem da congruência foi desenvolvida por **Karl Friedrich Gauss** no início do século XIX.

4.7 Conceitos Básicos da Congruência

Se os inteiros a e b dão o mesmo resto quando divididos pelo inteiro p (p ¿ 0) então podemos dizer que a e b são côngruos, módulo p e podemos representar: $(a \equiv b)$ mod p.

Uma maneira equivalente de dizer isso é afirmar que a diferença $(a - b)$ ou $(b - a)$ é divisível por p, ou que p é divisor dessa diferença. Veja um exemplo:

$(47 \equiv 43)$ mod 4, logo $(47 - 43)$ é divisível por 4.

A congruência define uma **relação de equivalência**, pois atende às propriedades reflexiva, simétrica e transitiva, ou seja: (a) $(a \equiv a)$ mod p (reflexiva); (b) $(a \equiv b)$ mod p, então $(b \equiv a)$ mod p (simétrica); (c) $(a \equiv b)$ mod p e $(b \equiv c)$ mod p, então $(a \equiv c)$ mod p (transitiva).

Algumas propriedades aritméticas da congruência:

Se $(a \equiv b)$ mod p e $(c \equiv d)$ mod p então: $(a + c \equiv b + d)$ mod p; $(a - c \equiv b - d)$ mod p; $(a.c \equiv b.d)$ mod p.

Todas essas propriedades estão demonstradas em Monteiro (1969). Mas, a visão do conceito de congruência pode ser mais entendido explicado através de exemplos.

4.8 Teoremas de Fermat

Dois teoremas, da Teoria do Números, desempenham papéis importantes em criptografia (mais precisamente em criptografia de chave pública).

Teorema (**Fermat**) - Se p é primo e a é um inteiro positivo não divisível por p (a e p são relativamente primos), então $a^{p-1} \equiv 1$ (mod p). Veja os exemplos na Figura 20.

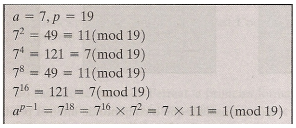


Figura 20 – Exemplos do Teorema de Fermat.

Fonte: Stallings, Criptografia e Segurança de Redes, Teoria dos Números, Cap.8, p.169.

Uma forma alternativa do teorema de Fermat é que:

Se p é primo e a é um inteiro positivo, então $a^p \equiv a(mod p)$.

Esta segunda alternativa não requer que a e p sejam relativamente primos. Veja os exemplos:

$p = 5, a = 3 a^p = 3^5 = 243 \equiv 3(mod 5) = a(mod p)$ $p = 5, a = 10 a^p = 10^5 = 100000 \equiv 10(mod 5) = 0(mod 5) = a(mod p)$

4.9 Função Φ de Euler

Leonhard Paul Euler (1707-1783) foi um matemático e físico suíço de língua alemã, que passou a maior parte de sua vida na Rússia e na Alemanha.

Euler fez importantes descobertas, mais precisamente em cálculo e teoria dos grafos. Também fez muitas contribuições para a matemática moderna no campo da terminologia e notação, em especial, a noção de uma função matemática, usada hoje. **Euler** é considerado um dos mais proeminentes matemáticos do século XVIII. **Euler** foi um dos mais prolíficos matemáticos, calcula-se que toda a sua obra reunida teria entre 60 e 80 volumes. Uma declaração atribuída a **Pierre-Simon Laplace** manifestada sobre **Euler** na sua influência sobre a matemática: "*Leiam Euler, leiam Euler, ele é o mestre de todos nós.*"

Sobre o interesse de **Euler** na teoria dos números, muitos dos primeiros trabalhos de **Euler** foram baseadas nas obras de **Pierre de Fermat**. **Euler** desenvolveu algumas das ideias de **Fermat**, e refutou algumas das suas conjecturas.

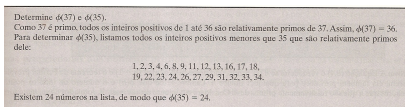
Euler provou o teorema de **Fermat** e inventou também a função Φ *tociente* (n).

Figura 21 – Leonhard Euler - Provou o teorema de Fermat.

Fonte: http://www.arte7cultura.blogspot.com/2013/04/leonhard-euler.html.

Usando as propriedades desta função, ele generalizou o teorema de **Fermat** ao que é hoje conhecido como o teorema de **Euler**. Ele contribuiu de forma significativa para a teoria dos números perfeitos. O conceito é considerado como um teorema fundamental da teoria dos números, e suas ideias alicerçaram o caminho para o trabalho de **Carl Friedrich Gauss** (1777-1855), foi um matemático e físico alemão que contribuiu muito em diversas áreas da ciência, dentre elas a teoria dos números, tendo desenvolvido a artimética modular aqui mostrada.

Função Tociente de Euler - Antes de vermos o Teorema de **Euler**, é preciso mostrar uma quantidade de números importante na Teoria dos Números, chamada de função de **Euler**, denotada por $\Phi(n)$, e que é definida como o número de inteiros positivos menores que n e relativamente primos de n. Para o caso $n = 1$, este não tem significado, portanto define-se $\Phi(1) = 1$. Veja os exemplos de $\Phi(37)$ e $\Phi(35)$ na Figura 22.


Determine $\phi(37)$ e $\phi(35)$.
Como 37 é primo, todos os inteiros positivos de 1 até 36 são relativamente primos de 37. Assim, $\phi(37) = 36$.
Para determinar $\phi(35)$, listamos todos os inteiros positivos menores que 35 que são relativamente primos dele:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18,
19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

Existem 24 números na lista, de modo que $\phi(35) = 24$.

Figura 22 – Exemplos de $\Phi(n)$.

Fonte: Stallings, Criptografia e Segurança de Redes, Teoria dos Números, Cap.8, p.169.

Para o caso de um número primo p, $\Phi(p) = p - 1$. E supondo-se que tenhamos dois números primos p e q, com $p \neq q$, pode ser mostrado que para $n = p.q$,

$\Phi(n) = \Phi(p.q) = \Phi(p).\Phi(q) = (p-1).(q-1)$. A prova da igualdade pode ser encontrada em Stallings (2008), Cap.8, p.170.

Teorema (**Euler**) - No Teorema de **Euler**, para cada a e n relativamente primos, temos: $a^{\phi(n)} \equiv 1(modn)$, onde $\phi(n)$, a função tociente de **Euler**, é o número de inteiros positivos menores que n e, relativamente primos de n.

Como acontece no teorema de **Fermat**, uma expressão alternativa mais geral também útil é: $a^m \equiv 1(modn)$

Da mesma forma que no teorema de **Fermat**, se a e n são relativamente primos, então existe pelo menos um inteiro m que satisfaz esta equação.

Para testar se um número é primo, ver o método de **Miller-Rabin** Stallings (2008), Cap 8, p.171.

4.10 Aplicações dos Números Primos

Até agora, mostramos a teoria dos números primos, como é desde Euclides (300 a.C), com uso somente na matemática pura, sem nenhuma aplicação no mundo concreto.

Para um computador é tarefa fácil descobrir se um número, por exemplo, com uma centena de algarismos é primo. Isto porque, existe algoritmo que pode ser programado no computador. Mas, praticamente impossível descobrir, se esse número pode ser **fatorado** (decomposto em fatores de números primos). Este é um problema computacionalmente difícil (inviável) de ser resolvido.

Podemos exemplicar alguns casos:

Exemplo 1 - Suponha que é solicitado ao leitor multiplicar 18×7. O cálculo de 126 é imediato. Mas, se agora, for dado 126, teremos que fatorá-lo de algumas formas diferentes para descobrir os fatores 18 e 7. Isto mostra que a multiplicação é imediata, mas a fatoração sempre leva mais tempo.

O exemplo mostram que para **fatorar números grandes**, mesmo se utilizando os mais potentes computadores, embora, nao se tenha uma impossibilidade matemática, mas é **computacionalmente inviável**, devido ao tempo de processamento. Os dois exemplos são casos usados que garantem, ainda nos tempos de hoje, a segurança de algoritmos importantes de criptografia.

Exemplo 2 - Muitas das modernas aplicações que estão a ser levadas a efeito no campo da criptografia dependem de algumas das propriedades dos números inteiros e dos números primos. No entanto, as aplicações aritméticas envolvendo as propriedades dos números inteiros estão diretamente relacionadas com a capacidade

de se resolver dois problemas fundamentais:

- O problema do teste para verificar se o número é primo.
- O problema da decomposição em fatores primos.

Estes são problemas aparentemente de simples solução, até que passem a envolver numerais com dezenas e até centenas de dígitos.

4.11 Bibliografia e Fonte de Consulta

Luiz Henrique Jacy Monteiro - Elementos de Álgebra, IMPA, 1969.

ACM (New York) - Association for Computing Machinery. Here´s to You: For Shaping the Future of Computing. Credit: Ron Rivest.

Michel Janos (2009). Matemática e Natureza. Editora da Física.

Teoria dos Números - https://pt.wikipedia.org/wiki/Teoria_dos_números

Euler - ⟨https://pt.wikipedia.org/wiki/Leonhard#CITEREFDunham1999⟩

4.12 Referências - Leitura Recomendada

O. Ore - Invitation to Number Theory. Washington: The Mathematical Association of America, 1967.

W. Leveque - Elementary Theory of Numbers. New York: Dover, 1990.

R. Burn - A Pathway to Number Theory. Cambridge: ambridge University Press, 1997.

R. Kumanduri, C. Romero - Number Theory with Computer Applications. Upper Saddle River: Prentice-Hall, 1998.

K. Rosen - Elementary Number Theory and its applications. Reading: Addison-Wesley, 2000.

CAPÍTULO 5

Congruência e Aritmética Modular - Parte II

UMa ferramenta da aritmética, muito importante na Teoria dos Números é a aritmética modular, que envolve o conceito de **congruência**. A aritmética modular é aqui colocada pela sua utilidade em determinadas áreas da Ciência da Computação, tais como na área de segurança computacional no campo da criptografia ou na área de redes de computadores, no uso em protocolos de comunicação, quando o protocolo necessita numerar sua mensagens enviadas e verificar o número da mensagens recebidas. Existem várias outras aplicações não colocadas neste texto.

5.1 Definindo Congruência e Aritmética Modular

Uma **congruência** é a relação entre dois números que, divididos por um terceiro - chamado *módulo de congruência* - deixam o mesmo resto. Por exemplo, o número 9 é congruente ao número 2, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 2(mod\ 7)$.

Em matemática, aritmética modular (chamada também de aritmética do relógio analógico) é um sistema de aritmética para inteiros, onde os números "voltam pra trás"quando atingem um certo valor, o módulo.

O matemático suiço **Leonhard Euler** (1707-1783) foi o pioneiro na abordagem de congruência por volta de 1750, quando ele explicitamente introduziu a ideia de congruência módulo n, um número natural n.

A *aritmética modular* foi desenvolvida posteriormente por **Carl Friedrich Gauss** em seu livro "*Disquisitiones Arithmeticae*", publicado em 1801, como na Figura 23.

Carl Friedrich Gauss (1777-1855) foi um matemático, astrônomo e físico Alemão que contribuiu muito em diversas áreas da ciência, dentre elas, na matemática, sobre

Figura 23 – Carl Friedrich Gauss - O livro *Disquistiones Artihmaticae* que introduziu a aritmética modular.

Fonte: https://pt.wikipedia.org/wiki/Carl_Friedrich_Gauss

a teoria dos números. Alguns se referem a ele como o *princeps mathematicorum* (o mais notável dos matemáticos) e um grande matemático desde a antiguidade. **Gauss** tinha uma marca influente em muitas áreas da matemática e da ciência e é um dos mais influentes na história da matemática. Ele considerava a matemática como "a rainha das ciências".

Figura 24 – Carl Friedrich Gauss - O criador da aritmética modular.

Fonte: https://en.wikipedia.org/wiki/Carl$_F riedrich_G auss$.

Gauss observou que essa relação tinha um comportamento semelhante à igualdade, e introduziu uma notação específica para este fato e que denominou de **congruência**. Este é um conceito muito importante da teoria dos números, e que está relacionado

com divisibilidade e os restos de uma divisão de números inteiros. Muitas aplicações, no dia-a-dia das pessoas, funcionam exatamente o conceito de congruência. Diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, ISSN, calendários (semanas, meses, anos) e muito usado em criptografia (transformação do que é legível em ilegível e voce-versa) e na numeração das mensagens de um protocolo de comunicação, além de diversos fenômenos periódicos estão diretamente ligados ao tema. É um tema que pode ser trabalhado já no nível do Ensino Fundamental, no contexto do processo de ensino-aprendizagem de matemática (aritmética).

No que segue, vamos mostrar alguns elementos teóricos sobre a aritmética modular e, na segunda parte do trabalho teremos a apresentação de alguns exemplos de aplicação desse importante e interessante tema da área de teoria dos números.

5.2 Exemplos de Congruência

Exemplo 1: (**Aritmética do Relógio Analógico**)

Este é um exemplo clássico do tema, como mostrado em Sa (2008).

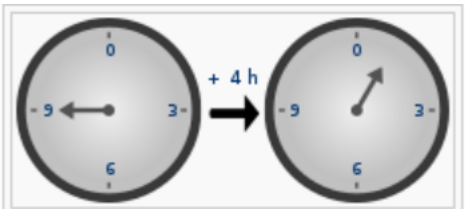


Figura 25 – Congruência Módulo 12 de um relógio analógico - O relógio usa aritmética módulo 12.

Fonte: https://pt.wikipedia.org/wiki/Aritmética_modular.

Num relógio analógico é tratado um caso de congruência, módulo 12. Note que 13 horas é congruente a 1 hora, no módulo 12. Ambos divididos por 12, deixam resto 1. 17 horas é congruente a 5 horas, módulo 12. Tanto 17, como 5, divididos por 12, deixam resto 5... e assim, sucessivamente.

$1 \equiv 13 \equiv 25 \equiv \ldots (mod\ 12)\ 5 \equiv 17 \equiv 29 \equiv \ldots (mod\ 12)$

Assim, as horas marcadas num relógio analógico constituem também um caso clássico de congruência, nesse caso com módulo 12.

Exemplo 2 (**Artmética Modular das Semanas**)

Vejamos uma aplicação interessante sobre o tema, relacionada aos calendários Sa (2008): vamos supor que você saiba em qual dia da semana caiu o dia 1º de janeiro

de um determinado ano. Em 2006, por exemplo, foi um domingo. Imaginemos que você deseja saber quando cairá um outro dia qualquer (vale para qualquer ano). É só montar uma tabela para essa primeira semana, que no caso será:

$Domingo \rightarrow 1$ $Segunda \rightarrow 2$ $Terca \rightarrow 3$ $Quarta \rightarrow 4$
$Quinta \rightarrow 5$ $Sexta \rightarrow 6$ $Sabado \rightarrow 7$

Verificamos aqui que estamos novamente diante de um caso de congruência, módulo 7 nesse caso. Digamos que estivéssemos interessados em descobrir em que dia da semana caiu o dia 5 de julho (e não temos um calendário em mãos, é claro). Primeiro precisamos ver quantos dias existem de 1 de janeiro até 5 de julho. Vejamos:

Janeiro = 31 dias, Fevereiro = 28 dias (2006 não é bissexto), Março = 31 dias, Abril = 30 dias, Maio = 31 dias, Junho = 30 dias, Julho = 5 dias, Total = 186 dias.

Agora, é como se tivéssemos uma fila de 186 dias e estamos desejando saber, na congruência de módulo 7 (7 dias da semana) qual o correspondente ao 186. Acho que você concorda que estamos diante de uma situação bem semelhante à que vimos no caso dos relógios analógicos.

Se dividirmos 186 por 7, teremos o resultado 26 e resto da divisão 4.

Logo, o 186 é congruente ao 4, no módulo 7. Como o dia 4 de janeiro de 2006 foi uma quartafeira, o 186º desse mesmo ano também o será e, é claro, que todas as demais quarta-feiras deste ano serão ocupados por números congruentes ao 4, módulo 7.

Assim, com esses dois exemplos que mostramos, podemos observar que em nosso dia-a-dia existem inúmeras situações onde se faz presente a noção de congruência, módulo k: calendários, relógios analógicos e problemas em geral envolvendo repetições periódicas.

5.3 Conceitos Básicos da Congruência Módulo k

Se os inteiros a e b dão o mesmo resto quando divididos pelo inteiro k, onde $(k > 0)$ então podemos dizer que a e b são côngruos, módulo k e podemos representar: $a \equiv b(mod\ k)$.

Uma maneira equivalente de dizer isso é afirmar que a diferença $(a - b)$ ou $(b - a)$ é divisível por k, ou que k é divisor dessa diferença. Veja um exemplo:

$(47 \equiv 43)$ mod 4, logo $(47 - 43)$ é divisível por 4.

A congruência define uma relação de equivalência, pois atende às propriedades

reflexiva, simétrica e transitiva, ou seja: $(a \equiv a)$ mod k) (reflexiva) $(a \equiv b)$ mod k) então $b \equiv a$ mod k (simétrica) $(a \equiv b)$ mod k) e $(b \equiv c)$ mod k, então $(a \equiv c)$ mod k (transitiva).

Algumas propriedades aritméticas da congruência:

Se $a \equiv b(mod\ k)$ e $c \equiv d(mod\ k)$, então: $a+c \equiv b+d(mod\ k)$ e $a-c \equiv b-d(mod\ k)$ e $a \times c \equiv b \times d(mod\ k)$.

Para qualquer inteiro d, se $d = f(mod\ k)$, então $a \times d \equiv b \times f(mod\ k)$.

Todas essas propriedades estão demonstradas em Monteiro (1969). Mas, a visão do conceito de congruência pode ser mais entendido, explicado através de exemplos.

5.4 Outros Exemplos de Aplicações de Congruência

Mostraremos, no que segue, que na criptografia e em diversos números de documentos de identificação (como no CPF, por exemplo), também está presente a *aritmética modular* e a noção de **congruência**.

Se escrevemos uma palavra em algum idioma, de modo errado, logo percebemos que fizemos uma inversão das letras. Mas, se digitamos um código de identificação de forma errônia, isto ocorrerá com os dígitos de um número, de um código de identificação qualquer, não teríamos como perceber a troca num simples olhar. Para isso e também para minimizar fraudes, foram criados os chamados dígitos de controle ou verificação. Tais dígitos de verificação são normalmente baseados na noção de congruência que mostramos anteriormente.

Exemplo 3 (**Aplicação na Verificação dos dois dígitos de controle de um CPF**)

O número de CPF de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são, como no ISBN e nos códigos de barra, dígitos de controle ou de verificação . A determinação desses dois dígitos de controle é mais um caso de aplicação da noção de congruência.

No caso do CPF, o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos:

Se $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9$ é a seqüência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base $1, 2, 3, 4, 5, 6, 7, 8, 9$ e somar os produtos obtidos.

O dígito que está faltando, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S - a_{10}$ deve ser múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \ (mod\ 11)$. Note que tal número será o próprio resto da divisão por 11 da soma obtida.

Por exemplo, se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos, 235 343 104, o primeiro dígito de controle será obtido da seguinte maneira:

Escrevemos os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9.

2 3 5 3 4 3 1 0 4
1 2 3 4 5 6 7 8 9

Efetuando as multiplicações correspondentes, teremos:

$$(2 \times 1) + (3 \times 2) + (5 \times 3) + (3 \times 4) + (4 \times 5) + (3 \times 6) + (1 \times 7) + (0 \times 8) + (4 \times 9) = 116$$

Dividindo o número 116 por 11, teremos o resultado 10 e resto 6. Dessa forma, o primeiro dígito de controle será o algarismo 6.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que é o que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9.

Vejamos:

2 3 5 3 4 3 1 0 4 6
0 1 2 3 4 5 6 7 8 9

Efetuando as multiplicações, teremos:

(2 x 0) + (3 x 1) + (5 x 2) + (3 x 3) + (4 x 4) + (3 x 5) + (1 x 6) + (0 x 7) + (4 x 8) + (6 x 9) = 145

Dividindo o número 145 por 11, teremos o quociente 13 e o resto 2. Logo, o segundo dígito de controle é o 2. Concluímos então que, no neste exemplo, o CPF completo seria: 235 343 104 62

Se o resto da divisão fosse 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, usaríamos, nesse caso, o dígito zero.

Exemplo 4 (**Aplicação no ISBN**)

Vejamos o exemplo demostrado por Sa (2008) para o código de identificação de livros ISBN. Um dos exemplos mais antigos é o sistema *International Standard Book Number* (ISBN) de catalogação de livros, CD-Roms e publicações em *braile*, que foi criado em 1969. A necessidade que as editoras têm de catalogar os seus livros e informatizar o sistema de encomendas serviu de motivação na geração desse código.

A vantagem é que, por ser um código numérico, ultrapassa as dificuldades geradas pelos diversos idiomas do mundo, bem como a grande diversidade de alfabetos existentes. Dessa forma, poderíamos, por exemplo, identificar através do **ISBN** um livro japonês.

Em tal sistema, as publicações são identificadas através de 10 algarismos, sendo que o último (dígito de controle) é calculado através da aritmética modular envolvendo operações matemáticas com os outros nove dígitos. Esses nove primeiros dígitos são sempre subdivididos em 3 partes, de tamanho variável, separadas por hífen, que transmitem informações sobre o país, editora e sobre o livro em questão.

Por exemplo, a língua inglesa é identificada somente pelo algarismo 0 e a editora **McGraw-Hill** tem um código de 2 algarismos que a identifica, dessa forma, restam ainda 6 algarismos para a identificação de suas publicações, havendo pois a possibilidade de $10^6 = 1\ 000\ 000$ de títulos.

Vejamos como se processa o cálculo do dígito final do **ISBN** (controle).

Representando por $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9$ a seqüência formada pelos 9 primeiros dígitos. Devemos multiplicá-los, nessa ordem, pela base $10, 9, 8, 7, 6, 5, 4, 3, 2$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser o menor valor possível, tal que ao ser acrescentado à soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S + a_{10}$ deve ser múltiplo de 11, ou seja, $S + a_{10} \equiv 0 \pmod{11}$.

Verificando o ISBN

Na contra-capa do livro Temas e Problemas Elementares, da Coleção Professor de Matemática Sa (2008), da Sociedade Brasileira de Matemática, temos o seguinte código do **ISBN**: 85-85818-29-8.

Vejamos o cálculo do dígito de controle que, como estamos observando, é igual a 8. Assim,

8 5 8 5 8 1 8 2 9
10 9 8 7 6 5 4 3 2

Efetuando as multiplicações correspondentes e somando os produtos obtidos, teremos:

$$(8 \times 10) + (5 \times 9) + (8 \times 8) + (5 \times 7) + (8 \times 6) + (1 \times 5) + (8 \times 4) + (2 \times 3) + (9 \times 2) =$$

$80 + 45 + 64 + 35 + 48 + 5 + 32 + 6 + 18 = 333$

Divindo 333 por 11, teremos o quociente 30 e resto 3.

Para obtermos um múltiplo de 11, ao acrescentarmos o décimo algarismo, o menor valor que atende a tal condição será o número 8, pois $11 - 3 = 8$. O que confere o valor apresentado no código dado. Isso significa dizer que $333 + 8 = 341$ é um múltiplo de 11, ou ainda, que $341 \equiv 0 \pmod{11}$.

Uma outra verificação de ISBN

O livro "Matemática Aplicada à Administração", Economia e Contabilidade, da Editora Thompson, tem o seguinte código ISBN 85-221-0399-?. Qual o seu dígito de controle?

Solução:

8 5 2 2 1 0 3 9 9
10 9 8 7 6 5 4 3 2

Efetuando a soma dos produtos correspondentes, teremos: $80 + 45 + 16 + 14 + 6 + 0 + 12 + 27 + 18 = 218$

Dividindo 218 por 11, teremos o quociente 19 e resto da divisão igual a 9.

Dessa forma, o dígito de controle será igual a 2, (11 - 9 = 2).

Podemos observar que os dois livros que usamos como exemplo tem o prefixo 85, que identifica livros publicados no Brasil.

Observações:

- No ISBN, se o dígito for igual a 10 (no caso do resto da divisão por 11 ser igual a 1), é usada a representação do 10 em algarismos romanos, ou seja usa-se um X.

- Em todos os casos que iremos mostrar, que usam aritmética modular, são usadas bases de multiplicação que operadas com os dígitos do número geram um determinado valor S. A esse valor obtido deve ser somado ou subtraído um valor x, de modo a que exista uma congruência ao zero, num módulo que normalmente é 11 ou 10, conforme o caso.

- A partir de janeiro de 2007, os códigos do ISBN estão sendo representados com 13 dígitos. No caso dos livros editados no Brasil há um acréscimo dos dígitos 978 antes do 85.

Exemplo 5 (Aplicação no Código de Barra EAN-13)

Como em Sa (2008), um dos códigos de barras mais usados no mundo todo é o EAN-13, constituído de 13 algarismos, sendo que o último é o dígito de controle. Nesse caso é usada a congruência módulo 10 e os fatores que compõem a base de multiplicação são os dígitos 1 e 3, que vão se repetindo da esquerda para à direita.

Se $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ a_{10}\ a_{11}\ a_{12}$ é a seqüência formada pelos 12 primeiros dígitos de EAN-13, devemos multiplicá-los, nessa ordem, pela base 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3 e somar os produtos obtidos. Vamos representar por S a soma obtida. O dígito que está faltando, que vamos representar por a_{13} deve ser tal que ao ser somado com S, deve gerar um múltiplo de 10, isto é, o número $S + a_{13}$ deve ser múltiplo de 10, ou seja, $S + a_{13} \equiv 0 \pmod{10}$.

Vejamos um exemplo:

Numa embalagem de uma garrafa para bebidas, temos o seguinte código de barras:

8 424906 201767, onde 7 é dígito de controle.

Vamos efetuar os cálculos para a determinação do dígito de controle (que estamos vendo ser o dígito 7).

8 4 2 4 9 0 6 2 0 1 7 6, 1 3 1 3 1 3 1 3 1 3 1 3 (neste caso, esta é a base de multiplicação)

Efetuando os produtos, teremos:

$8 + 12 + 2 + 12 + 9 + 0 + 6 + 6 + 0 + 3 + 7 + 18 = 83$

Dividindo 83 por 10 teremos o quociente 8 e resto 3.

Logo, o dígito de controle será igual a 7, o mesmo que (10 - 3). Note que $83 + 7 = 90$ (múltiplo de 10)

Sabemos também que, no código de barras com 13 algarismos, os três primeiros dígitos do código representam o país de registro do produto (verifique que para produtos filiados no Brasil teremos sempre os dígitos 7, 8 e 9); os quatro dígitos seguintes identificam o fabricante; os próximos cinco dígitos identificam o produto e o último, como já sabemos, é o dígito verificador ou de controle, que se pode calcular através da congruência, módulo 10.

5.5 A Aritmética Modular na Criptografia

Imaginemos dois amigos, **Alice** e **Bob**, que vivem isolados e apenas podem comunicar através do correio. Eles sabem que o carteiro é um tremendo "curioso"e que lê todas as suas cartas. **Alice** tem uma mensagem para **Bob** e não quer que ela seja lida. Que é que pode fazer? Ela pensou em lhe enviar um cofre com a mensagem, fechado a cadeado. Mas como lhe fará chegar a chave? Não pode enviar dentro do cofre, pois assim **Bob** não o poderá abrir. Se enviar a chavem em separado, o carteiro pode fazer uma cópia.

Depois de muito pensar, ela tem uma idéia. Envia-lhe o cofre fechado com um cadeado. Sabe que **Bob** é esperto e acabará por perceber a sua idéia. Com mais uma ida e uma volta do correio, e sem nunca terem trocado chaves, a mensagem chega até **Bob**, que abre o cofre e a lê. Como é que você acha que resolveram o problema? Pense bem no assunto, tente responder a questão. É simples ... depois que você descobrir.

O "truque"usado foi o seguinte: **Bob** colocou um outro cadeado no cofre e ele tinha a chave desse segundo cadeado. Devolve o cofre a **Alice** por correio, desta vez fechado com os dois cadeados. **Alice** remove o seu cadeado, com a chave que possui e reenvia o cofre pelo correio só com o cadeado colocado por **Bob**. É claro que Bob tem apenas que abrir o cofre, com a sua própria chave e ler a mensagem enviada pela sua amada. O carteiro não tem como saber o conteúdo do cofre.

Na criptografia usam-se chaves que, de certa forma, são análogas à estratégia usada pelos dois amigos da história. Esta história relata a velha charada do sigilo nas comunicações e uma de suas brilhantes soluções. Talvez tenha servido de inspiração para os três jovens norte-americanos, **Whitefield Diffie**, **Martin Hellman** e **Ralph Merkle**, ao construirem em 1976 um sistema de criptografia, definiram que o segredo da comunicação é assegurado por duas *chaves* (dois números, um em sigilo e outro público). Neste caso, os comunicantes só precisam trocar entre si (o número público), como aconteceu na história do **Bob** e da **Alice**. Foi esta invenção que inspirou o sistema de **criptografia RSA** (Rovest, Shamir e Addleman), como está na seção de aplicações de números primos no capítulo 4.

Bailey Whitfield Diffie (1944-) é um matemático e criptógrafo estadunidense. Pioneiro em criptografia de chave pública. Formado pelo Instituto de Tecnologia de Massachusetts, ele se interessava muito pela criptografia.

Martin Edward Hellman (1945-) é um criptógrafo Estadunidense, conhecido por sua invenção do protocolo *Diffie-Hellman* de acordo de chave compartilhada, desenvolvido em cooperação com **Whitfield Diffie** e **Ralph Merkle**. **Hellman** publicou sua criação, que acabou por originar a ideia de criptografia de chave pública, com os colaboradores **Whitfield Diffie** e **Ralph Merkle** na Universidade de Stanford em 1976.

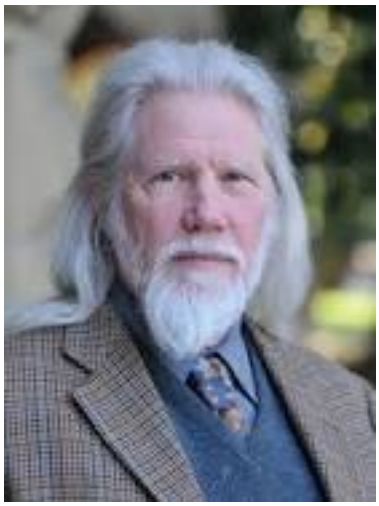


Figura 26 – Whitefield Diffie - Pioneiro em criptografia de chave pública, juntamente com Martin Hellman.

Fonte: http://cisac.fsi.stanford.edu/people/whitefield$_d$*iffie*.

Figura 27 – Martin Hellman - Um dos criadores do método Diffie-Hellman usado para geração e troca de uma chave compartilhada entre duas partes comunicantes.

Fonte: https://pt.wikipedia.org/wiki/Martin_Hellman.

Figura 28 – Ralph Merkle - É um pesquisador estadunidense em criptografia de chave pública e, mais recentemente, pesquisador e palestrante sobre nanotecnologia molecular.

Fonte: https://pt.wikipedia.org/wiki/Ralph_Merkle.

Alice e **Bob** são personagens fictícios, muito citados, em vários livros. São nomes sistematicamente utilizados pelos especialistas de criptografia. É mais interessante do que falar apenas no emissor e receptor, ou apenas em A e B. Costuma se acrescentar a eles uma terceira personagem, representada na nossa história pelo carteiro, que costuma receber o nome de Eva - «Eve», em inglês - e que representa aquela que se põe à escuta - ou seja, aquela que comete "*eavesdrop*".

Até à descoberta de **Diffie**, **Hellman** e **Merkle**, a comunicação de mensagens cifradas exigia uma troca da chave da cifra, como fizemos nas atividades anteriores e como era feito nas chaves de **Júlio César**. Era preciso que **Alice** e **Bob** se encontrassem previamente e combinassem uma chave que apenas eles dois conhecessem. Só isso lhes permitiria, posteriormente, trocar mensagens à distância sem que **Eva**, sempre à escuta, conseguisse percebê-las. Assim funcionaram as mensagens secretas desde os tempos do romano **César** até aos tempos modernos. Assim funcionaram os espiões. A chave poderia ser simples, mas era sempre necessário que **Alice** e **Bob** combinassem tudo antes, e nem sempre isso era possível.

A idéia de **Diffie**, **Hellman** e **Merkle** era revolucionária. Segundo o esquema que propuseram, **Alice** e **Bob** começam por acordar em dois números. E estes podem ser públicos, pois mesmo que **Eva** os consiguisse descobrir, não terá como descobrir a chave do processo de cifragem. Cada um deles escolhe um outro número, que mantém secreto. Feitos alguns cálculos, em ambos lados, baseadas em *aritmética modular*,

ambos chegam a um mesmo resultado: um número que mais ninguém conhece e que será a chave compartilhada entre eles, de codificação das suas mensagens. O processo que inventaram é relativamente simples, embora muito engenhoso, e será mostrado no quadro abaixo. Tudo se passa de forma parecida com a da história dos dois cadeados. As chaves não são trocadas, mas cada um acaba por poder abrir o cofre, sem que o carteiro, o consiga.

O processo inventado por **Diffie**, **Hellman** e **Merkle** marca o nascimento da criptografia com chaves públicas, que funcionam em conjunto com chaves secretas que não precisam ser "trocadas". Baseia-se na *aritmética modular*, que consiste, essencialmente, em trabalhar com os restos da divisão inteira por um número determinado, chamado módulo. Esse processo foi denominado de congruência, módulo k, e foi inventado por **Gauss**, conforme já observamos no início deste capítulo.

Simon Singh, no seu "Livro dos Códigos"em Singh (2001), dá um exemplo que retrata bem o processo matemático da *aritmética modular*, envolvido nessas chaves públicas. **Simon Lehna Singh** (1964-) é um autor britânico. **Singh** é o autor do livro "*O Último Teorema de Fermat*", que narra a história do enigma mais longo da Matemática, o "O Último Teorema de Fermat". Lançado no Brasil pela Editora Record em 1998, o livro "O Último Teorema de Fermat"teve versão para a televisão na série de documentários científicos da BBC "Horizon". É autor também dos livros "Big Bang"e "O Livro dos Códigos".

Figura 29 – Simon Singh - Autor do livro "O Último Teorema de Fermat".

Fonte: https://pt.wikipedia.org/wiki/Simon_Singh.

Neste exemplo, **Alice** e **Bob** precisam se comunicar e combinam nos números que servem: o primeiro de base para uma potenciação e o segundo para o módulo da congruência. Digamos que tenham optado pelos números 5 e 11. Estariam então se referindo ao cálculo de 5^x e da congruência no módulo 11.

(O expoente x seria secreto, à escolha de cada um deles).

Alice escolhe 3 para seu número secreto (expoente da potência) **Alice** calcula

$5_3 = 125$ e, através de congruência módulo 11, gera o número 4, pois 125 dividido por 11 deixa resto 4.

Alice envia o resultado, 4, para Bob.

Bob escolhe 6 para seu número secreto (novamente o expoente da potência). **Bob** calcula $5_6 = 15625$ e, através de congruência módulo 11, gera o número 5, pois 15625 dividido por 11 deixa resto 5.

Bob envia o resultado, 5, para Alice.

Note que, mesmo que esses dois números que eles enviaram um ao outro, fossem interceptados, as pessoas não teriam como saber a chave final do processo.

Alice pega o resultado de Bob, 5, e o seu número secreto, 3, e calcula $5^3 = 125 \equiv 4(mod 11)$. Mas, 125 dividido por 11 deixa resto 4.

Bob pega o resultado de **Alice**, 4, e o seu número secreto, 6, e calcula $4^6 = 4096 = 4$ (mod 11). Mas, 4096 dividido por 11 também deixa resto 4.

Veja que **Alice** e **Bob** encontraram o mesmo número, 4, sem que tivessem informado um ao outro os seus números secretos pessoais. Esse número seria agora usado como chave para a composição das mensagens criptográficas. A congruência, como foi aplicada aqui, funcionou exatamente como a história dos cadeados e do correio, contada por Crato (2001).

Tente fazer com outros números secretos, verifique que você sempre irá obter resultados iguais.

É através da criptografia que, diariamente, através da Internet, uma luta sempre se processa: a de enviar dados e a de tentar captar esses dados (são os famigerados hackers).

É claro que o tema criptografia é muito mais complexo do que mostramos aqui. O que exemplificamos, através de chaves criptográficas simples, foi para mostrar a relação que existe entre esse tema e a aritmética modular. É um assunto bastante interessante, e que pode ser usado no ensino fundamental, relacionado a conceitos importantes da Matemática, como operações inversas, divisibilidade e funções.

5.6 O Problema da Fatoração de Números Primos Grandes

Atualmente, números primos tem tido aplicação na área da Ciência da Computação, em particular na área de segurança computacional, mais precisamente em criptografia (cifragem usada no sigilo das informações). Por exemplo, a aplicação à segurança na

transmissão de dados através da criptografia, a técnica de cifrar e decifrar mensagens que são transmitidas em redes de computadores, em particular, a Internet, ou mesmo, na armazenagem de dados sigilosos em um sistema de computador.

Como aplicação na área da Ciência da Computação, a aritmética modular é utilizada na área de segurança da informação, em várias situações de uso da criptografia, mais particularmente no conhecido desenvolvimento do algoritmo de criptografia de chave pública RSA ou no *Acordo de Chaves de Diffie-Hellman* Stallings (2008).

Uma das formas de transmitir ou armazenar informações de forma sigilosa é usar as técnicas da criptografia. Em criptografia assimétrica no método RSA, duas chaves são necessárias para se ter um algoritmo: uma chave pública PU e uma chave privada PR. Supondo, agora, que a chave pública (cifragem) do transmissor tenha 150 algarismos (um número extremamente grande) e que a chave privada (decifragem) só pode ser obtida a partir da chave pública de cifragem, como obter essa chave privada a partir de dois números primos de 75 algarismos? A chave de decifragem (privada) é o segredo que cada parte tem na comunicação. Então, como se poderia chegar a esse par de números primos (relativamente grandes)? Este é o problema da fatoração de um número num produto de números primos muito grandes, que matematicamente é possível, mas computacionalmente é inviável, pelo tempo de processamento envolvido no processo de fatoração. Este fato matemático sobre a fatoração de números primos grandes é que garante a segurança deste algoritmo.

Este caso, pode ser mostrado no algoritmo de criptografia de chave pública RSA (**Rivest**, **Shamir**, **Adleman** na Figura 30). Eles usaram números primos e o problema da fatoração de números muito grandes, para garantir a inviabilidade computacional quanto ao algoritmo RSA, como mostrado no que segue. A aritmética modular é usada no algoritmo seguinte nas linhas 5, 9 e 11.

Figura 30 – Ron Rivest, Adi Shamir e Len Adleman e o algoritmo RSA

Fonte: (Reprodução) - ACM - Association for Computing Machinery.

Algoritmo RSA (Ron Rivest, Adi Shamir e Len Adleman)- aplicando a função Φ de Euler.

Geração de Chaves RSA

1. Selecione p e q, onde p e q são primos e $p \neq q$
2. Calcule $\mathbf{n} = p.q$
3. Calcule $\Phi(n) = (p-1).(q-1)$

4. Selecione o inteiro e tal que $mdc(\Phi(n), e) = 1;\ 1 < e < \Phi(n)$
5. Calcule d, tal que $d \equiv e^{-1}(mod\Phi(n))$
6. Chave pública $PU = \{e, n\}$
7. Chave privada $PR = \{d, n\}$

Criptografia

8. Texto legível $M < n$
9. Texto cifrado $C = M^e \pmod{n}$

Decriptografia

10. Texto cifrado C
11. Texto legível $M = C^d \pmod{n}$

5.7 Problema do Logaritmo Discreto

O algoritmo mencionado mostrado na seção anteiror é baseado na dificuldade computacional da fatoração de um número primo muito grande, num produto de fatores primos. Para mostrar outra utilidade dos números primos, vejamos uma outra aplicação. Criptosistemas (sistemas de criptografia assimétrica) podem ser baseados em outra forma de dificuldade computacional: o *problema do logaritmo discreto*. Como em Terada (2008), o problema do logaritmo discreto é definido como:

Definição (**Logaritmo Discreto**)

Dados um número primo p e inteiros g, t tais que $0 < g, t < p$, calcular um inteiro s tal que $t = g^s \pmod{p}$.

Usando logaritmo discreto no algoritmo ElGamal geral:

Em criptografia, o algoritmo de **ElGamal** é um criptosistema com o uso de chaves assimétricas (públicas e privadas) criado pelo criptógrafo egípcio **Taher Elgamal** em 1984. A segurança computacional desse algoritmo se baseia na dificuldade de solução que o **problema do logaritmo discreto** apresenta.

Correspondendo a este problema, considerado computacionalmente inviável, pode-se generalizar o Algoritmo de **ElGamal** como podemos ver no que segue, como em Terada (2008):

Existem duas partes comunicantes: *Alice* e *Bob*.

Base de **ElGamal**: *Alice* escolhe inicialmente um inteiro S tal que $1 \leq S \leq | H | -1$. Seja $x \in G$ a ser criptografado por *Bob*. O conjunto chaves é $K = \{(G, A, S, B) : B = A^S\}$. Notemos que G e H são, por hipótese, escolhidos para que S seja dificil de ser calculado, mesmo conhecendo-se A e B (problema do Logaritmo Discreto Geral). Os valores A e B são públicos; S é secreto e conhecido somente por *Alice*. O algoritmo tem duas partes: criptografia e decriptografia.

Algoritmo de Criptografia:

Para um chave pública (A, B) de Alice, Bob efetua as seguintes etapas para $x \in G$:

1. Escolhe um número secreto $k \in \mathbb{Z}_{|H|}$ (este é um NONCE, um valor gerado e comunicado somente uma vez). Se Bob não conhece $| H |$, ele pode escolher $k \in \mathbb{Z}_G$, sem qualquer prejuizo. Recomenda-se usar um k distinto para cada x a ser criptografado.

2. Seja o texto legível $x \in G$. Calcula-se $y = A^k$ e $z = x \circ B^k$. Notemos que $y, z \in G$.

3. O texto ilegível é (y, z), o qual é enviado para *Alice*. Ou seja, $Bob \rightarrow y = A^k$ e $z = x \circ B^k \rightarrow$Alice.
Observe que B^k pode ser considerado como uma chave "volátil", isto é, uma chave que só é usada para criptografar este x, e a criptografia consiste em multiplicar B^k por x $(B^k = A^{Sk})$.

Algoritmo de Decriptografia:

Para *Alice* decriptografar $y, z \in G$ ela terá que efetuar $z \circ (y^S)^{-1}$. Lembre que $y^{-S} = A^{-Sk} = (B^k)^{-1}$.

5.8 Bibliografia e Fonte de Consulta

MONTEIRO, L. H. J. (1969) Elementos de Álgebra. IMPA. Ao Livro Técnico SA, Cap.2, pgs.22-23.

NACHBIN, L. (1971) Introdução à Álgebra. McGraw-Hill. Rio de Janeiro.

Leonhard Euler - ⟨http://www.ams.org/samplings/feature-column/fcarc-eulers-formula⟩

Aritmética Modular - https://pt.wikipedia.org/wiki/Aritmética_modula

Arnaldo Garcia e Yves Lequain. Elementos de Álgebra - Rio de Janeiro, IMPA, 2002. 326 páginas (Projeto Euclides), ISBN 978-85-244-0190-9.

José Plinio de Oliveira Santos - Introdução à Teoria dos Números - Rio de Janeiro, IMPA, 1998. 198 péginas (projeto Euclides), ISBN 978-85-244-0142-8.

Aritmética Modular - ⟨http://www.atractor.pt/mat/alg_controlo/arit_modular/mod_texto.htm⟩

5.9 Referências - Leitura Recomendada

Zeidler, Eberhard. Oxford User's Guide to Mathematics. Oxford, UK: Oxford University Press, 2004. p. 1188. ISBN 0198507631.

Dunnington, G. Waldo. (May, 1927). "The Sesquicentennial of the Birth of Gauss". Scientific Monthly XXIV: 402-414. Retrieved on 29 June 2005. Comprehensive biographical article.

Tent, Margaret. The Prince of Mathematics: Carl Friedrich Gauss. [S.l.]: A K Peters, 2006. ISBN 1568814550.

Simmons, J.. The Giant Book of Scientists: The 100 Greatest Minds of All Time. Sydney: The Book Company, 1996.

Zeidler, Eberhard. Oxford User's Guide to Mathematics. Oxford, UK: Oxford University Press, 2004. p. 1188. ISBN 0198507631.

Bühler, Walter Kaufmann. Gauss: a biographical study. [S.l.]: Springer-Verlag, 1987. 144-145 p. ISBN 0387106626.

CAPÍTULO 6

A Álgebra na Europa

Como já visto no capítulo 2 as origens da álgebra se encontram na antiga Babilônia Struik (1987), cujos matemáticos, da época, desenvolveram um sistema aritmético avançado, que depois a aritmética virou álgebra, com o qual puderam fazer cálculos algébricos. Com esse sistema eles foram capazes de aplicar fórmulas e calcular soluções para incógnitas numa classe de problemas.

6.1 O que Significa a Palavra Álgebra

A palavra "álgebra" não se sujeita a uma etimologia nítida como a palavra "aritmética", que deriva do grego arithmos ("número").

Abu Abd Allah Muhammad ibn Musa al-Khwarizmi (780-850) foi um matemático, astrônomo, astrólogo e geógrafo. O livro intitulado "*Al-jabr Wa'l-mocábala*" Wallis (1693), escrito em Bagdá por volta do ano 825, é um livro histórico com o objetivo de ensinar soluções para os problemas matemáticos cotidianos da época. É um livro histórico de matemática escrito em árabe entre 813 e 833 d.C. pelo matemático e astrônomo muçulmano **al-Khwarizmi**, um erudito pertencente à Casa da Sabedoria de Bagdade, atual capital atual do Iraque. Nesta obra, **al-Khwarizmi** expõe os alicerces da álgebra, sendo o primeiro a estudar sistematicamente a resolução de equações lineares e quadráticas. A palavra "*Al-jabr*" da qual álgebra foi derivada significa "reunião", "conexão" ou "complementação", uma das operações básicas com equações (*al-gabr*) descritas neste livro, quase quatro séculos depois, com o título *Ludus Algebrae et Almucgrabalaeque*. A palavra "*Al-jabr*", foi traduzida para o latim, redundando na palavra *álgebra*, uma variante latina desta palavra árabe. No século XII, traduções de sua obra para o latim, sobre numerais indianos apresentou a notação posicional decimal para o mundo ocidental. Suas contribuições tiveram um grande impacto sobre a linguagem algébrica. O radical da palavra "algarismo" e "algoritmo" vem de *algoritmi*, a forma latina de seu nome "Khwarizmi".

6.2 Diofanto de Alexandria

Diofanto de Alexandria (201 e 214- 284 e 298) foi um matemático grego, considerado como o grande impulsionador da **álgebra**. **Diofanto** desempenhou um papel semelhante ao de Euclides (360 a.C.-295 a.C.) na Geometria. Entre vários livros que escreveu, o mais importante destes é *Arithmetica*, uma obra contendo 130 problemas algébricos, suas soluções numéricas (equações algébricas) e teoria dos números, além de introduzir notação simbólica diferente para o quadrado de uma incógnita, para o cubo e assim sucessivamente. Estudiosos bizantinos, que fugiram de Constantinopla (atual Istambul, capital da Turquia), em meados do século XV (anos 1400), trouxeram o livro para a Europa Ocidental. Provavelmente 170 anos depois, a obra de **Diofanto** era conhecida apenas por alguns, quando, em 1621, foi feita a tradução para o latim. Escreveu também sobre as soluções de inequações: para que uma equação tenha solução, primeiro precisamos saber a qual sistema numérico as soluções pertencem, isto é, se as solução pertencem ao números naturais, inteiros, reais ou outros. Certas equações cujas soluções são números inteiros ou racionais são chamadas de *equações diofantinas*.

Figura 31 – Diofanto: 130 problemas algébricos e suas soluções numéricas.

Fonte: www.somatematica.com.br

6.3 Fibonacci e a Álgebra na Europa

A Álgebra entrou na Europa via **Fibonacci**. **Leonardo Fibonacci** (1170-1250) foi um matemático italiano, tido como o primeiro matemático europeu da Idade Média. É considerado por alguns como o mais talentoso matemático ocidental da Idade Média. Escreveu *Liber Abaci*, sendo a segunda edição, de 1228, a que hoje é conhecida. Esse livro contém uma grande quantidade de assuntos relacionados com a Aritmética e a Álgebra da época, e realizou um papel importante no desenvolvimento matemático na Europa nos séculos seguintes, pois, por esse livro, os europeus vieram a conhecer os algarismos hindus, também denominados arábicos. A teoria contida em *Liber Abaci* é ilustrada com muitos problemas que representam uma grande parte

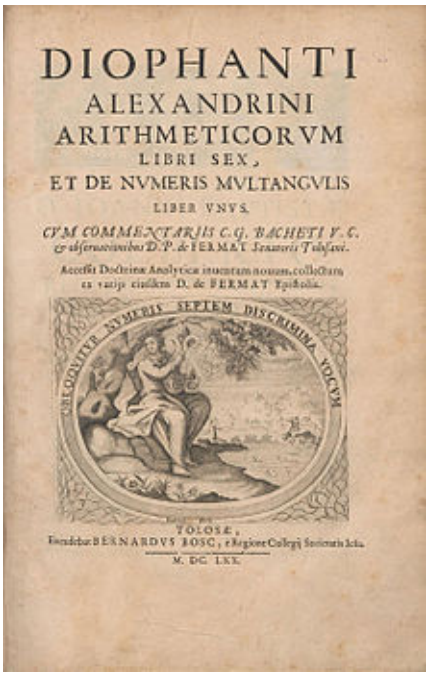


Figura 32 – Traduçao latina (1670) de uma obra de Diofanto.

Fonte: https://pt.wikipedia.org/wiki/Ficheiro:Diophantus-cover-Fermat.jpg

do livro. *Liber Abaci* repercutiu na Europa, acarretando um rápido florescimento da álgebra na Europa, devidos aos seguintes fatores: (a) facilidade de manipular trabalhos numéricos através do sistema de numeração indo-arábico, muito superior aos sistemas (tais como o romano) que requeriam o uso do ábaco; (b) invenção da imprensa com tipos móveis, que acelerou a padronização do simbolismo mediante a melhoria das comunicações, baseada em ampla distribuição; (c) ressurgimento da economia, sustentando a atividade intelectual; (d) e a retomada do comércio e viagens, facilitando o intercâmbio de idéias tanto quanto de bens; (e) cidades comercialmente fortes surgiram primeiro na Itália, e foi lá que o renascimento algébrico na Europa efetivamente teve início.

6.4 François Viète

François Viète (1540-1603) foi um matemático francês que introduziu a primeira notação algébrica sistemática. Ele também esteve envolvido em decifrar códigos e publicou *In Artem Analyticum Isagoge* Viete (1646), que foi o mais antigo trabalho sobre **álgebra simbólica**. Em 1572 publicou o "*Canon Mathematicus*", uma tentativa para servir de introdução à trigonometria. *Canon Mathematicus* abrange trigonometria; ele contém tabelas trigonométricas, também dá a matemática por trás da construção das tabelas. Vinte anos mais tarde publicou "*In artem analyticum isagoge*" que foi o mais antigo trabalho sobre álgebra simbólica. Neste tratado, **Viète** demonstrou o valor dos símbolos introduzindo letras para representar incógnitas. Ele sugeriu o uso de letras como símbolos para quantidades, conhecidas e desconhecidas.

Ele usou para vogais para as incógnitas e consoantes para quantidades conhecidas. A convenção, onde as letras no início do alfabeto representam quantidades conhecidas, enquanto letras perto do final para representar quantidades desconhecidas foi introduzida mais tarde por Descartes em *La Géométrie*. Esta convenção é usada hoje em dia, muitas vezes sem que as pessoas percebam. **Viète** fez muitos melhoramentos na teoria de equações. Ele apresentou métodos para resolver equações de segundo, terceiro e quarto graus.

Figura 33 – Viéte - O primeiro trabalho sobre álgebra simbólica.

Fonte: https://pt.wikipedia.org/wiki/François_Viète.

6.5 René Descartes

René Descartes (1596-1650) foi matemático francês. Historicamente, **René Descartes** deve ter sido o primeiro filósofo a utilizar as técnicas algébricas como meio de exploração científica. Notabilizou-se, sobretudo, por seu trabalho revolucionário na filosofia e na ciência, mas também obteve reconhecimento matemático por sugerir a **fusão da álgebra com a geometria** - fato que gerou a *geometria analítica* e o *sistema de coordenadas* que hoje leva o seu nome (coordenadas cartesianas). Por fim, foi também uma das figuras-chave na Revolução Científica.

O interesse de **Descartes** pela matemática surgiu cedo, no "College de la Fleche", escola do mais alto padrão, dirigida por jesuítas, na qual ingressará aos oito anos de idade. Mas por uma razão muito especial e que já revelava seus pendores filosóficos: a certeza que as demonstrações ou justificativas matemáticas proporcionam. Aos vinte e um anos de idade, depois de freqüentar os ambientes matemáticos em Paris, já graduado em Direito, ingressa voluntariamente na carreira das armas. Durante os quase nove anos que serviu em vários exércitos, não se sabe de nenhuma proeza militar realizada por **Descartes**. Possivelmente, as batalhas que ocupavam suas ideias e seus sonhos travavam-se no campo da ciência e da filosofia.

Figura 34 – Descartes - A junção da Geometria e a Álgebra.

Fonte: http://www.iep.utm.edu/descarte/.

6.6 Os Tempos de Fermat

Pierre de Fermat (1601-1665) foi um matemático e cientista francês. A influência de Pierre de Fermat foi limitada pela falta de interesse na publicação das suas descobertas, conhecidas principalmente pelas cartas a amigos e anotações na sua cópia da *Arithmetica*, de **Diofanto**. Estas cartas passaram a ser publicadas a partir de 1636, por intermédio do padre **Mersenne**, em Paris, que procurou **Fermat** após ouvir falar dele. Nas suas cartas, Fermat descrevia as suas ideias, descobertas e até pequenos ensaios, que eram transmitidos por **Mersene** a outros matemáticos da Europa. **Fermat** gostava de trocar e resolver desafios, como por exemplo, **Mersenne** uma vez escreveu-lhe perguntando se o número - muito grande - 100.895.598.169 era primo ou não. Tais questões geralmente levavam anos a serem resolvidas, mas **Fermat** replicou sem hesitação que o número era produto de 112.303 e 898.423, e que cada um desses fatores era primo.

Fermat também ajudou a criar a **Geometria Analítica** em 1629, e descreveu as suas ideias num trabalho não publicado intitulado "Introdução aos Lugares Geométricos Planos e Sólidos", de 1636, que circulou apenas na forma de manuscrito, e que só foi publicado em 1679, postumamente, junto com sua obra completa. **Fermat**, bastante modesto, era avesso a publicar seus trabalhos. Disso resulta, em parte, o fato de Descartes comumente ser mais lembrado como criador da Geometria Analítica. Neste trabalho **Fermat** introduziu a ideia de eixos perpendiculares e descobriu as equações gerais da reta, circunferência e equações mais simples para parábolas, elipses e hipérboles, e depois demonstrou que toda equação de 1º e 2º grau pode ser reduzida a um desses tipos.

Nada disto está no ensaio de **Descartes**, apesar deste ter tido acesso à "Introdução" de Fermat, vários meses antes de publicar a sua obra intitulada "Geometria", de 1637, como um dos três apêndices do "Discurso do Método", obra considerada o

Figura 35 – Fermat: o precursor da Teoria dos Números.

Fonte: https://en.wikipedia.org.

marco inicial da filosofia moderna. Nela, em resumo, **Descartes** defende o método matemático como modelo para a aquisição de conhecimentos em todos os campos. **Descartes** travou argumentos, com ele, diversas vezes. **Fermat** não conhecia o monumental egoísmo e a disposição de Descartes, mas com paciência demoliu os argumentos de **Descartes** em todas as ocasiões.

O trabalho de **Fermat** também foi centrado sobre as propriedades da tangente de curvas; O método de Fermat, para determinar tangentes, foi desenvolvido pela sua abordagem aos problemas de máximos e mínimos, e foi ocasião de outro atrito com **Descartes**. Quando **Descartes** foi informado do método de Fermat, este atacou a sua genialidade, desafiando Fermat a encontrar a tangente à curva $x^3 + y^3 = 3.a.x.y$ e, loucamente, vaticinou que ele falharia. O próprio **Descartes** foi incapaz de resolver o problema e ficou intensamente irritado quando Fermat o resolveu com facilidade (esta curva chama-se agora folium de **Descartes**).

No caso da geometria analítica, fruto dessa fusão, o mérito não foi de uma só pessoa. Dois franceses, **Pierre de Fermat** (1601-1665) e **René Descartes** (1596-1650), são os responsáveis por esse grande avanço científico: o primeiro movido basicamente por seu gosto pela matemática e o segundo por razões filosóficas. E diga-se de passagem, não trabalharam juntos: a **geometria analítica** é um dos muitos casos, em ciência, de descobertas simultâneas e independentes.

O bem-sucedido **Pierre de Fermat** dedicava muitas de suas melhores horas de lazer à matemática. Na verdade **Fermat** simplesmente não conseguia fugir a sua verdadeira vocação e, apesar de praticar matemática como *hobby*, nenhum de seus

contemporâneos contribuiu tanto para o avanço desta ciência quanto ele. Além da geometria analítica, **Fermat** teve papel fundamental na criação do **Cálculo Diferencial**, do **Cálculo de Probabilidades** e, especialmente, da **Teoria dos Números**.

6.7 Breve História da Álgebra Abstrata

história desta secão está em Milles (1992).

A álgebra, tal como apresentada hoje nos nossos cursos universitários, costuma resultar de difícil compreensão aos nossos estudantes, precisamente por seu caráter abstrato. Normalmente, uma estrutura é definida a partir dos axiomas que a caracterizam e, logo depois, uma sucessão aparentemente interminável de teoremas passa a ser deduzida destes axiomas. Muitas vezes, resulta difícil para o aluno compreender porque a área se desenvolveu na direcão em que ela é apresentada e porque alguns resultados são mais relevantes do que outros.

Nesse sentido, um conhecimento da história do assunto pode tornar claro porque é natural considerar uma determinada estrutura e não outra, um determinado conjunto de axiomas e não outro; porque algumas perguntas são mais relevantes do que outras. Na verdade, a história mostrará que muitas vezes o desenvolvimento de um dado assunto não foi linear nem simples, que os matemáticos levaram muito tempo para compreender a importância de um conceito e, às vezes, até para admití-lo como válido.

A história que pretendemos contar nestas páginas é fascinante em mais de um sentido. Não somente diz como determinadas ideias foram sendo introduzidas gradativamente na matemática, como descreve também o longo processo que levou esta ciência na direção de uma abstração sempre crescente. Também nos mostra que muitas vezes, um determinado conceito foi se impondo por força das circustâncias, como resultado de um acúmulo de descobertas que apontavam na sua direção, mesmo apesar da resistência de um bom número de matemáticos, muitos destes de primeira qualidade.

A história da matemática está intimamente ligada com o desenvolvimento de todas as áreas da cultura humana e muitas vezes são motivações vindas de campos tão diversos como a Física, a Filosofia ou a Arte, que determinam o progresso desta ciência. Algumas destas influências, se bem que não todas, resultarão aparentes nesta nossa história.

6.7.1 O Desenvolvimento da Álgebra

O texto desta seção é originado do trabalho *Breve História da Álgebra Abstrata*, de **César Polcino Milies**, EPUSP.

Durante muito tempo, a palavra Álgebra designava aquela parte da Matemática que se ocupava de estudar as operações entre números e, principalmente, da resolução de equações. Nesse sentido, pode-se dizer que esta ciência é tão antiga quanto a própria história da humanidade, se levamos em conta que esta última se inicia a partir da descoberta da *escrita*. De fato, tanto nas tabuletas de argila da suméria quanto nos papiros egípcios, encontramos problemas matemáticos que lidam com a resolução de equações. No Papiro Rhind, por exemplo, documento egípcio que data aproximadamente do ano 1650 a.C. e no qual o escriba conta que está copiando material que provém do ano 2000 a.C., encontramos problemas sobre distribuição de mercadorias que conduzem a equações relativamente simples. Surpreendentemente, descobrimos também que os antigos babilônios sabiam resolver completamente equações de segundo grau.

No Papiro Rhind, por exemplo, documento egípcio que data aproximadamente do ano 1650 a.C. e no qual o escriba conta que estava copiando material que provém do ano 2000 a.C., encontramos problemas sobre distribuição de mercadorias que conduzem a equaçõeses relativamente simples. Surpreendentemente, descobrimos também que os antigos babilônios sabiam resolver completamente equações de segundo grau.

Desde os seus começos, a álgebra se preocupou sempre com a procura de métodos gerais e rigorosos. Assim por exemplo, **R.J. Gillings** [9, Appendix I] comentando os métodos que os egípcios usavam para lidar com a resolução de equações diz:

Os estudiosos da história e filosofia da ciência do século vinte, ao considerar as contribuições dos antigos Egípcios, se inclinam para atitude moderna de que um argumento ou prova lógica deve ser simbólico para ser considerado rigoroso, e que um ou dois exemplos específicos usando números escolhidos não podem ser considerados cientificamente sólidos. Mas isto não é verdade! Um argumento ou demonstração não simbólico pode ser realmente rigoroso quando dado para um valor particular da variável; as condições para o rigor são que o valor particular da variável seja típico e que uma consequente generalização para qualquer valor seja imediata. Em qualquer dos tópicos mencionados neste livro, onde o tratamento dado pelos escribas seguia estas linhas, ambos os requisitos eram satisfeitos de modo que os argumentos colocados pelos escribas são já rigorosos ... o rigor está implícito no método.

Quando finalmente se desenvolveu uma notação apropriada (empregando letras para reperesentar coeficientes e variáveis de uma equação), foi possível determinar fórmulas gerais de resolução de equações e discutir métodos de trabalho também gerais. Porém, mesmo nestes casos, tratava-se de situações relativamente concretas. As letras representavam sempre algum tipo de números (inteiros, racionais, reais ou complexos) e utilizavam-se as propriedades destes de forma mais ou menos intuitiva. Como veremos adiante, a formalização destes conceitos de modo preciso só aconteceria a partir do século XIX.

Foi precisamente nesse século que alargou-se consideravelmente o conceito de operação. Alguns autores da época não mais se restringem a estudar as operações clássicas entre números, mas dão ao termo um significado bem mais amplo e estudam operações entre elementos, sem se preocupar com a natureza destes, interessando-se apenas com as propriedades que estas operações verificam.

A passagem da álgebra clássica para a assim chamada álgebra abstrata foi um processo sumamente interessante. Representa não somente um progresso quanto aos conteúdos técnico-cietíficos da disciplina como amplia consideravelmente o seu campo de aplicação e, o que é mais importante, implica - num certo sentido - uma mudança na própria concepção do que a matemática é, da compreensão de sua condiçãoo de ciência independente e da evolução dos métodos de trabalho.

Jean Alexandre Eugène Dieudonné (1906-1992) foi um matemático francês. Conhecido por suas pesquisas sobre álgebra abstrata e análise funcional, pelo envolvimento ativo no **Grupo Bourbaki** e no projeto *Éléments de géométrie algébrique* de **Alexander Grothendieck**, e como historiador da matemática, particularmente nos campos da análise funcional e topologia algébrica. **Dieudonné** nasceu e cresceu em Lille, passando um período de sua formação na Inglaterra, onde iniciou a estudar álgebra. Em 1924 foi admitido na **École Normale Supérieure**, onde foi contemporâneo de **André Weil**. Completou os estudos e em seguida doutorou-se em 1931, orientado por **Paul Montel**,[2] período que foi acompanhado por estadias nas universidades de Princeton e Berlim, bem como no Instituto Federal de Tecnologia de Zurique. Em 19321933 foi professor em Bordeaux, em 19331937 em Rennes, em 19371952 em Nancy, sendo professor visitante em Estrasburgo e São Paulo. Em 1952 foi para os Estados Unidos, onde lecionou inicialmente na University of Michigan. De 1953 a 1959 foi professor na Northwestern University. Retornou a Paris em 1959, permanecendo até 1964 no *Institut des Hautes Études Scientifiques*. Desde 1964 foi titular de uma cadeira em Nice.

Em 1934 fundou juntamente com outros matemáticos o Grupo Bourbaki, do qual foi um dos dois membros mais influentes. É de conhecimento corrente que a maior parte dos textos publicados com o pseudônimo **Bourbaki** chegaram a sua forma final pelas mãos de **Dieudonné**. Seu talento para a redação de livros texto e sua visão sintética são expressos também na publicação monumental *Éléments de géometrie algébrique*, escrito juntamente com **Alexander Grothendieck** na década de 1960, a base para a fundamentação da teoria dos Séminaires de géometrie algébrique (SGA) da escola de *Grothendieck*. Em seu *Cours de géometrie algébrique*, publicado em dois volumes, apresenta um esboço sucinto da teoria, apresentando no primeiro volume a história do assunto em questão.

Suas outras áreas de interesse foram teoria dos grupos, grupo de Lie, análise funcional (teoria dos espaços vetoriais topológicos), teoria espectral e topologia (em 1944 introduziu o conceito de *espaço paracompacto*).

Não obstante, é conhecido principalmente por seu *Éléments dAnalyse*, onde expõe em diversos volumes a análise completa até geometria diferencial, grupos de **Lie** e teoria espectral, destinado a profissionais da área. Publicou também livros texto sobre análise e álgebra linear/geometria para iniciantes.

Figura 36 – Jean Dieudonné - O criado do **Grupo Bourbaki** em 1934.

Fonte: Google Images - en.wikipedia.org.

J. Dieudonné dizia que "*... em matemática, os grandes progressos estiveram sempre ligados a progressos na capacidade de elevar-se um pouco mais no campo da abstração" e, na mesma obra,* ***A. Lichnerowicz*** *observou que "... é uma característica da matemática repensar integralmente seus próprios conteúdos e nisso reside, inclusive, uma condição essencial para seu progresso*". A história da álgebra abstrata ilustra perfeitamente estes pontos de vista.

Pode-se dizer que há dois fatores que contribuiram fundamentalmente para o desenvolvimento da álgebra: (a) de um lado, a tendência a aperfeiçoar as notações, de modo a permitir tornar o trabalho com as operações (e equacões) cada vez mais simples, rápido e o mais geral possível e, por outro lado, (b) a necessidade de introduzir novos conjuntos de números, com o consequente esforço para compreender sua natureza e sua adequada formalização.

6.7.2 O Simbolismo Algébrico

Como em Milles (1992), é bem sabido que o uso de uma notação adequada é fundamental para o bom desenvolvimento de uma área da matemática. Porém, a história nos ensina que nem sempre é fácil chegar a uma tal notação. Um bom exemplo vem dos próprios números naturais. A numeração indo-arábica que usamos ainda hoje, começou a ser desenvolvida na Índia e a primeira referência ao princípio posicional aparece pela primeira vez na obra de **Aryabhata** chamada *Aryabatiya*, publicada em 499. A primeira ocorrência de fato se dá no ano 595, onde a data 346 aparece em numeração posicional e o registro mais antigo do uso do número zero se acha numa inscrição indiana de 876 d.C.

A necessidade de uma notação mais sofisticada se manifestou pela primeira vez

em relação à resolução de equações algébricas. Como já observamos, os egípcios resolviam equações de primeiro grau e algumas equações particulares do segundo grau, enquanto que os babilônios conheciam o método para resolver qualquer equação de segundo grau. Também os gregos resolviam este tipo de equações, por métodos geométricos mas, em todos os casos, não havia notações nem fórmulas gerais.

E no século IV d.C., na Aritmética de **Diophanto**, que encontramos pela primeira vez o uso de uma letra para representar a incógnita de uma equação. Como os manuscritos originais de Diofanto não chegaram até nós, não sabemos com toda certeza quais os símbolos que ele usava, mas acredita-se que representava a incógnita pela letra ς, uma variante da letra σ. Esta escolha se deve provavelmente ao fato de que, no sistema grego de numeração, as letras representavam também números conforme sua posição no alfabeto, mas a letra ς não fazia parte do sistema e não correspondia, assim, a nenhum valor numérico particular. Ele usava também nomes para designar as várias potências da incógnita, como quadrado, cubo, quadrado-quadrado (para a quarta potência), quadrado-cubo (para a quinta) e cubo-cubo (para a sexta). O uso de potências superiores a três é notável uma vez que, como os gregos se apoiavam em interpretações geométricas, tais potências não tinham um significado concreto. Porém, de um ponto de vista puramente aritmético, estas potências sim tem significado e esta era a postura adotada por **Diofanto**.

A partir de então, os métodos e notações de **Diofanto** foram se aperfeiçoando lentamente. Mesmo os símbolos hoje tão comuns para representar as operações demoraram a ser introduzidos. Muitos algebristas usavam p e m para representar a adição e a subtração por serem as iniciais das palavras *plus* e *minus*. O símbolo "=" para representar a *igualdade* foi introduzido só em 1557 por **Robert Recorde** e não voltou a aparecer numa obra impressa até 1618. Autores como **Kepler**, **Galileo**, **Torricelli**, **Cavalieri**, **Pascal**, **Napier**, **Briggs** e **Fermat**, entre outros, ainda usavam alguma forma retórica em vez de um símbolo, como as palavras *aequales*, *esgale*, *faciunt*, *gheljck* ou a abreviatura *aeq*. Para uma história detalhada da evolução do simbolismo algébrico, o leitor pode consultar a referência clássica de **F. Cajori** (F. Cajori, *A History of Mathematical Notations*, Dover, New York, 1993).

Robert Recorde(1510-1558) foi um matemático inglês. É bastante conhecido por ter criado o sinal de igualdade, no ano de 1557.

A notação de expoentes é usada por **Nicolas Chuquet** (1445-1500) na sua *Tripary*, onde escreve expressões como 12^3, 10^3 e 120^3 para representar o que hoje escreveríamos como $12x^3$, $10x^3$ e $120x^3$ e também 12^0 e 7^{1m} para $12x^0$ e $7x^{?1}$.

Os primeiros passos para a introdução do conceito de *polinômio* e seu uso para a formulação de problemas de resolução de equações foram dados por **Simon Stevin** (1548-1620). Foi tutor de Maurício de Nassau. Ele foi um defensor do sistema de **Copérnico** e o primeiro a discutir e sugerir o emprego de frações decimais (em oposição ao sistema sexagesimal defendido por outros), na sua obra mais conhecida

Figura 37 – Robert Recorde - O criador do símbolo de igualdade "=" e o primeiro a usar o símbolo "+" em 1557.

Fonte: Google Images - en.wikipedia.org.

Figura 38 – Nicolas Chuquet - O criador da notação de expoentes no século XV.

Fonte: Google Images - en.wikipedia.org.

De Thiende, publicada em *Flamengo* em 1585 e traduzida ao francês, sob o título *La Disme*, no mesmo ano. Alí ele usou símbolos como pequenos círculos envolvendo os dígitos 0, 1, 2, etc. para indicar as posições das unidades, dízimas, centésimas, respectivamente. Assim por exemplo, ele escreve $875,782$ como 875 circ(0) 7 circ(1) 8 cic(2) 2 circ(3) (onde circ() é uma notação criada pelo autor para contornar o problema do Latex de criação do símbolo círculo com o dígito dentro). No restante do livro, ele estuda as operações entre dízimas e justifica as regras de cálculo empregadas. O leitor interessado pode ver uma tradução ao inglês de *De Tiende* em Smith (1929). (D. E. Smith, *A Source Book in Mathematics*, McGraw Hill, New York, 1929, p.20-34).

Figura 39 – Simon Stevin - O introdutor do conceito de polinômio e o emprego de frações decimais no século XVI.

Fonte: Google Images - scienceworld.wolfram.com.

No seu livro seguinte, "L' Arithmetique", publicado em 1585, ele introduz uma notação exponencial semelhante para denotar as várias potências de uma vari´avel. As potências que nós escreveríamos com x, x^2 $x3$ etc. são denotadas por ele como 0, 1, 2, e assim, por exemplo, o polinômio $2x^3 + 4x^2 + 2x + 5$ se escreveria, na sua notao como:2 cic(3) + 4 cic(2) + 2 cic(1) + 5 cic(0).

Ele denomina estas expressões de *multinômios* e mostra como operar com eles. Entre outras coisas, observa que as operações com *multinômios* tem muitas propriedades em comum com as operações entre "*números aritméticos*". Ainda, ele mostra que o algorítmo de **Euclides** pode ser usado para determinar o *máximo divisor comum* de dois *multinõmios*.

E interessante destacar aqui que nos encontramos frente a dois progressos notáveis na direção da abstração. De um lado temos a percepção, cada vez mais clara, de que os métodos de resolução de equações dependem unicamente do grau da equação e não dos valores dos coeficientes numéricos (vale lembrar que autores como **Tartaglia**,

Cardano e outros, que se utilizavam apenas de coeficientes positivos, consideravam como problemas diferentes, por exemplo, as equações da forma $X^3 = a^X + b$ e $X^3 + aX = b$). Mais importante ainda, vemos que **Simon Stevin** trata seus multinômios como novos objetos matemáticos e estuda as operações entre eles.

Mais interessante ainda é o trabalho de **François Viète** (1540-1603). Nascido em Fontenay-le Comte, teve formação de advogado e, nesta condição, serviu ao parlamento de Bretania em Rennes e foi banido de suas atividades, devido à oposição política, entre 1584 e 1589, quando foi chamado por Henri III para ser conselheiro do parlamento, em Tours. Nos anos em que esteve afastado da atividade política, dedicou-se ao estudo da matemática e, em particular, aos trabalhos de **Diophanto**, **Cardano**, **Tartaglia**, **Bombelli** e **Stevin**. Da leitura destes trabalhos ele teve a idéia de utilizar letras para representar quantidades. Isto já tinha sido feito no passado, até por autores como **Euclides** e **Aristóteles**, mas seu uso era pouco frequente.

Sua principal contribuição à Álgebra aparece no seu livro *In Artem Analyticam Isagoge* (Introdução à Arte Analítica) impresso em 1591, onde trata das equações algébricas de um novo ponto de vista. Ele fez importantes progressos na notação e seu verdadeiro mérito esté em ter usado letras não somente para representar a *incógnita*, mas também para representar os coeficientes ou quantidades conhecidas. Ele usava consonantes para representar quantidades conhecidas e reservava as vogais para representar as incógnitas. Deixamos **Viète** descrever a grande descoberta com suas próprias palavras (Viète, *Opera Mathematica* 1646, p.8):

Este trabalho pode ser ajudado por um certo artificio. Magnitudes dadas serão distinguidas das desconhecidas e requeridas por um simbolismo, uniforme e sempre fácil de perceber, como é possível designando as quantidades requeridas pela letra A ou por outras letras vogais A,I,O,V,Y e as dadas pelas letras B,G,D ou outras consonantes.

Assim por exemplo, a equação que nós escrevemos como $bx^2 + cx = d$ era representada por ele na forma:

B in A quadratum plus C plano in A aequalia D solido.

Como **Viète** pensava geometricamente, requeria, para suas equações, um *princípio de homogeneidade*, i.e., todos os termos de uma dada equação deveriam ter a mesma "dimensão"; assim por exemplo, todos os termos de uma equação quadrática, tal como a dada acima, deviam representar volumes. É por causa disso que o coeficiente da variável C é acompanhado do adjetivo plano, pois devia representar uma área. Da mesma forma, D é acompanhado do termo sólido para enfatizar que representa um volume.

Uma restrição à generalidade de sua notação é que ele representava por letras

apenas números positivos e, como muitos dos seus predecessores, não utilizava coeficientes negativos. **Johann van Waveren Hudde** (1628-1704) foi o primeiro a usar, em 1657, letras para representar coeficientes que podiam ser tanto positivos quanto negativos.

Figura 40 – John Hudde - Letras representando coeficientes no século XVII em 1657.

Fonte: Google Images - learn-math.info.

Viète chamava sua álgebra simbólica de *logística speciosa* por oposição à *logística numerosa*, que trata dos números. E importante observar que Viète tinha plena consciência de que seu emprego de letras lhe permitia trabalhar com classes de equações, por oposição ao emprego de números, que permite apenas trabalhar com um exemplo de cada vez. Com isso ele tornou explícita a diferença entre Álgebra e Artimética: para ele, a Álgebra - logística speciosa - era um método para operar com espécies ou formas de coisas e a Aritmética - logística numerosa - lidava apenas com números. Também tentou trabalhar algebricamente, provando, por exemplo, as identidades que os gregos tinham exibido por métodos geométricos. Assim, no seu *Zeteticorum Libri Quinque* - Cinco Livros de Análise - publicado em 1593, ele utiliza o método de "completar quadrados" numa equação de segundo grau e também encontramos ali identidades gerais do tipo: $a^3 + 3a^2b + 3ab^2 + b^3 = (a + b)^3$, que ele escreve na forma:

$$a\ cubus + b\ in\ a\ quad.\ 3 + a\ in\ b\ quad.3 + b\ cubo\ aequalia\ \overline{a + b}\ cubo.$$

Sobre os seus cinco livros de *Análise*, **Viète** não usava o termo álgebra que, por ser de origem árabe, não considerava adequado para a Europa cristã; no seu lugar empregava o termo *Análise* que, devido talvez a sua influência, foi adotado depois como sinônimo de "Algebra Superior".

Dois episódios ilustram muito bem o talento matemático de **Viète** e fama que chegou a desfrutar ainda durante sua vida. Em 1593, o matemático belga **Adriaen**

van Roomen(1561-1615), na versão latinizada do seu nome - propôs "a todos os matemáticos" o problema de resolver uma determinada equação de grau 45, do tipo:

$$x^{45} - 45x^{43} + 945x^{41} - \ldots - 3795x^3 + 45x = K$$

O embaixador dos Países Baixos na corte de França afirmou então que nenhum matemático francês seria capaz de resolver esta equação. O rei, **Henrique IV**, fez **Viète** saber deste desafio e ele notou que a equação proposta resultava de expressar a igualdade $K = sen(45.\vartheta)$ em termos de $x = sen\vartheta$ e conseguiu achar, nessa primeira audiência, uma raiz positiva. No dia seguinte, ele achou todas as 23 raízes positivas da equação. **Van Roomen** ficou tão impressionado que fez uma visita especial a Viète. Este publicou sua solução em 1595, num tratado intitulado *Ad problema, quod omnibus mathematicis totius orbis construendum propusuit Adrianus Pomanus, responsum.*

Outro episódio que ilustra sua extraordinária capacidade é o seguinte. Durante a guerra com a Espanha, ainda a serviço de **Henrique IV**, ele pode decifrar o o código utilizado pelos espanhois a partir de cartas que foram interceptadas e, dali em diante, conhecer o conteúdo de novas cartas escritas nesse código. E os espanhois achavam seu código tão difícil de ser quebrado ...

O uso de letras para representar classes de números e assim tratar das equações de forma mais geral demorou a ser aceito. Um aperfeiçoamento desta notação foi devido a **René Descartes** (1596-1650) que, na sua obra utiliza pela primeira vez a prática, hoje usual, de utilizar as primeiras letras do alfabeto para representar quantidades conhecidas e as últimas, como x,y e z para as incógnitas. E precisamente nessa obra que **Descartes** apresenta as ideias que deram origem à Geometria Analítica, junto com as contribuições de **Pierre de Fermat**. Esse texto não foi apresentado como um livro independente, mas como um apêndice da sua obra, pela que seria mais conhecido, o *Discours de la méthode pour bien conduire sa raison et chercher la vérité dans les sciénces*, em 1637 (neste livro ele descreve o uso da dúvida metódica como forma de tornar a ideias claras e precisas a partir das quais poderia-se chegar a conclusões válidas. Por esta e muitas outras contribuições, ele veio a ser considerado o "pai da filosofia moderna".). A obra foi publicada em francês e não em latim, que era a linguagem científica universal da época. **Franciscus van Schooten** (1615-1660), um matemático holandês, publicou em 1649, em Leyden, uma tradução ao latim que incluia material suplementar e que foi ampliada a dois volumes entre 1654-1661. Foi devido a esta publicação e a ação de **Von Schooten** e seus discípulos que a geometria cartesiana se desenvolveu rapidamente. **Franciscus van Schooten** é conhecido por popularizar a geometria analítica de **René Descartes**.

Tal como **Viète**, **Descartes** utilizava as letras para indicar apenas números positivos, embora não hesitasse em escrever diferenças de coeficientes literais. O uso de letras para representar tanto números positivos quanto negativos aparece pela primeira vez em 1637, numa obra de **John Huddle** (1633-1704) intitulada *De reducrione*

Figura 41 – Van Schooten - Quem popularizou a geometria cartesiana de Descartes.

Fonte: Google Images - learn-math.info.

a equationenum, que também fez parte da edição de **Schooten** da *Geometria de Descartes* entre 1654-1661. O progresso final, em relação ao uso da notaçãoo consistiu em usar uma letra também para representar o grau de uma equação. Nossa notação moderna que utiliza expoentes negativos e fracionários foi introduzida por **Isaac Newton** (1642-1727) numa carta dirigida ao, então, secretário da *Royal Society*, em 13 de junho de 1676, onde diz:

Figura 42 – Isaac Newton - Notação de expontes literais, negativos e fracionários em 1676.

Fonte: Google Images - www.estudopratico.com.br.

Como os algebristas escrevem $a2$, $a3$, $a4$, etc., para aa, aaa, $aaaa$, etc., também eu escrevo $a^{\frac{1}{2}}$, $a^{\frac{2}{3}}$, $a^{\frac{5}{4}}$ para $\sqrt{a}$, $\sqrt[3]{a^2}$, $\sqrt[4]{a^5}$; e escrevo $a^{?1}$, $a^{?2}$, $a^{?3}$, etc., para $\frac{1}{a}$, $\frac{1}{aa}$, $\frac{1}{aaa}$, etc.

Também sua fórmula para o binômio foi anunciada nesta carta, usando letras para representar inclusive expoentes racionais. Antes de **Issac Newton**, já **John Wallis** (1616-1703), um matemático britânico cujos trabalhos sobre o cálculo foram precursores aos de **Isaac Newton**, tinha usado expoentes literais, em 1657, em expressões tais como $AR^m \times AR^n = A^2R^{m+n}$ ao tratar de progressões geométricas.

Figura 43 – John Wallis - Os expoentes literais em equações em 1657, antes mesmo de Newton.

Fonte: Google Images - www.profcardy.com.

O primeiro a usar o símbolo "+" tal como o conhecemos também foi **Robert Recorde** (1510-1558), que em 1557 publicou o primeiro texto de álgebra da Inglaterra, chamado *The Whetstone of Witte*. Ali ele introduz o símbolo dizendo:

"*I will sette as I doe often in woorke vse, a pair of paralleles or Gemowe lines, of one length, thus :=, bicause no .2 thynges, can be moare equalle.*"
(*Usarei, como faço frequentemente no trabalho, um par de linhas paralelas, do mesmo comprimento assim :=, porque duas coisas não podem ser mais iguais*).

Este símbolo não foi incorporado rapidamente. Como vimos, **Viète**, usava ainda, em 1589, a expressão *aequalis* e, mais tarde, o símbolo . **Descartes**, em 1637, usava $\propto$ que provavelmente deriva de æ, usado como abreviatura de *aequalis*. Incidentalmente, vale a pena mencionar que os símbolos + e - hoje usados para denotar adição e subtração, respectivamente, aparecem impressos pela primeira vez num texto de **Johannes Widman**, professor da *Universidade de Leipzig* (1460-1498), foi um matemático alemão, o primeiro a utilizar o sinal "+"e -"na aritmética por meio de seu livro *Aritmética Comercial*, publicado em 1489 em Leipzig, Alemanha.
O sinal + deriva, aparentemente da palavra latina *et*, usada em vários manuscritos para designar a adição e o sinal - da letra *m* que, como vimos, era usada para abreviar *minus*. Eles são usados numa aritmética comercial intitulada *Rechenung auff allen Kauffmanschafft* que publicou em 1489, mas estes sinais já apareciam em notas manuscritas de um seu aluno de 1486 que se conservam na biblioteca de Dresden (Codex Lips 1470). Eles foram aceitos gradativamente e já **Boaventura Cavalieri** (1598-1647), um discípulo de **Galileo**, estudou astronomia, trigonometria esférica e cálculo logarítmico. Bonaventura Cavalieri foi matemático italiano que em 1635 publicou sua obra mais conhecida, *Geometria indivisibilibus continuorum*

Figura 44 – Johannes Widmann - Os sinais "+" e "-" aparecem impressos pela primeira vez num texto em 1489.

Fonte: Google Images - en.wikipedia.org.

nova (*Nova Geometria dos Indivisíveis Contínuos*), em que desenvolveu a ideia de **Kepler** sobre quantidades infinitamente pequenas. Seu método sobre os indivisíveis foi muito criticado na época, pois não apresentava o rigor matemático desejado. **Cavalieri** então, em 1647, publicou a obra *Exercitationes geometricae sex* (*Seis Exercícios Geométricos*), onde usava +, -, =, como se fossem familiares ao leitor, e na qual apresentou de maneira mais clara sua teoria. Mas é considerado um dos precursores do cálculo integral. Tal livro transformou-se em fonte importante para os matemáticos do século XVII.

6.8 História Resumida do Teorema Fundamental da Álgebra

Peter Rothe, no seu livro *Arithmetica Philosophica* publicado em 1608, escreveu que **uma equação polinomial de grau n, com coeficientes reais, podia ter soluções**. **Albert Girard** no seu livro *L'invention nouvelle en l'Algèbre* publicado em 1629, afirmou que **uma equação polinomial de grau n tem soluções, mas não disse que tais soluções eram necessariamente números complexos**. **Thomas Harriot** (1560-1621) foi um matemático algebrista, fundador da escola inglesa de álgebra (1602) e introdutor de vários símbolos e notações empregados em álgebra ainda hoje, como os sinais $>$ (maior que) e $<$ (menor que). **Harriot**, por volta de 1602, havia descoberto que: se a é raiz de um **polinômio**, então $(x - a)$

Figura 45 – Boaventura Cavalieri - Utilizava na época, os sinais "+" e "-", depois de Johannes Widman.

Fonte: Google Images - pt.wikipedia.org.

divide o **polinômio**.

Em 1637 (século XVII), **Descartes** escreve em *La Géométrie*, o que anos antes **Harriot** havia descoberto - se a é raiz de um polinômio, então $(x - a)$ divide o polinômio. **Descartes** afirmou também que para todas as equações de grau n, podemos imaginar n raízes, mas estas podem não corresponder a quantidades nos **números reais**. No início, os números complexos **não eram vistos como números**, mas sim, como um artifício algébrico útil para se resolver equações. **Descartes**, no século XVII (anos 1600), os chamou de *números imaginários*.

Abraham de Moivre e **Leonard Euler**, no século XVIII (anos 1700), começaram a estabelecer uma estrutura algébrica para os números complexos. Em particular, **Euler** denotou a raiz quadrada de -1 ($\sqrt{-1}$) por i. Em matemática, no escopo dos **números complexos**, o **Teorema Fundamental da Álgebra** afirma que qualquer polinómio $p(z)$ com coeficientes complexos de uma variável x e de grau $n \geq 1$ tem alguma **raiz complexa**. Ou em outros termos: "*Um polinômio $p(z)$ de grau n tem sempre n raízes complexas*".

Uma consequência do **Teorema Fundamental da Álgebra** é que **qualquer polinômio com coeficientes reais e grau superior a 0, pode ser escrito como produto de polinômios com coeficientes reais, de primeiro ou segundo grau**. No entanto, em 1702, **Leibniz** afirmou que nenhum polinômio do tipo $x^4 + a^4$ (com a sendo real e não nulo) poderia ser obtido sob aquela forma.

Poucos anos mais tarde, **Nicolaus Bernoulli II** (1695-1726) afirmou o mesmo, relativamente ao polinômio $x^4 - 4x^3 + 2x^2 + 4x + 4$, mas recebeu uma carta de **Euler**

em 1742, na qual lhe foi explicado que o seu polinômio era, de fato, outro.

Jean le Rond d'Alembert (1717-1783) foi um matemático francês. Uma primeira tentativa de demonstrar o teorema foi levada a cabo por **D'Alembert** em 1746, mas a demonstração foi considerada incorrecta.

Outras tentativas foram levadas a cabo por **Euler** (1749), de **Foncenex** (1759), **Lagrange** (1772) e **Laplace** (1795). Estas últimas quatro tentativas recorreram à tese de **Argand**; mais precisamente, a existências de raízes eram dadas como certa e o que faltava provar era que eram da forma $a + b.i$ para números reais a e b. Em terminologia moderna, **Euler**, **Foncenex**, **Lagrange** e **Laplace** estavam a supor a existência de um **corpo algébrico** (uma estrutura algébrica) construindo a **decomposição de polinômios**, ou seja, qualquer polinômio com coeficientes reais e grau superior a 0, pode ser escrito como produto de polinômios com coeficientes reais, de primeiro ou segundo grau.

No fim do século XVIII foram publicadas duas novas demonstrações. Uma delas, algébrica, da autoria de **James Wood**, foi publicada em 1798, mas logo completamente ignorada. A demonstração de **Wood** tinha uma falha de natureza algébrica. A outra demonstração foi publicada por **Gauss** em 1799, que era sobretudo geométrica, mas tinha também uma falha, mas de natureza topológica.

Já no século XIX, uma demonstração rigorosa foi publicada por **Argand** em 1806. **Jean-Robert Argand** (1768-1822) foi um matemático francês, nascido na Suíça. Foi com ele que, pela primeira vez, o **Teorema Fundamental da Álgebra** foi enunciado para **polinômios com coeficientes complexos** e não apenas para **polinómios com coeficientes reais**.

Figura 46 – Argand - O Teorema Fundamental da Álgebra com coeficientes complexos em 1806.

Fonte: www.routledgetextbooks.com.

Gauss demonstrou que o conjunto dos números complexos é algebricamente fechado,

e publicou mais duas demonstrações em 1816 e uma nova versão da primeira demonstração em 1849.

Entretanto, a primeira publicação a conter uma demonstração do teorema foi "*Cours d'analyse de l'École Royale Polytechnique*", em 1821, através de **Augustin-Louis Cauchy** (1789-1857). A demonstração em questão é a de **Argand**, embora este não seja mencionado por **Cauchy**.

Outro detalhe sobre o teorema: nenhuma das demonstrações mencionadas era *construtiva*. **Karl Weierstrass** (1815-1897) foi um matemático alemão, professor na Universidade de Berlim, quem levantou pela primeira vez, em 1891, o problema de encontrar uma *demonstração construtiva* do teorema. Tal demonstração foi obtida por **Hellmuth Kneser** em 1940 e simplificada por **Martin Kneser** em 1981.

Figura 47 – Weierstrass - A demonstração construtiva do Teorema Fundamental da Álgebra.

Fonte: https://en.wikipedia.org/wiki/Karl_Weierstrass.

O trabalho de **Weierstrass** forneceu as bases da **teoria das funções analíticas**, aquelas que são definidas usando-se séries de números reais, e programadas para formarem as bibliotecas de funções embutidas nas linguagens de programação.

6.9 A Insolubilidade da Quíntica

A equação cúbica geral foi resolvida por sendo simplificada em uma cúbica reduzida. A quártica, ao ser reduzida a uma cúbica. Mas, as soluções de cada equação polinomial de grau acima da quártica estavam se tornando cada vez mais complicadas. Parecia que a sólução da quíntica seguiria o mesmo caminho: encontrar a transformação que reduzisse a quíntica para uma quártica e, então, usar a fórmula de **Ferrari**. Talvez por isso mais de dois séculos se tiveram passado.

Por quase 250 anos, após a solução da quártica por **Cardano** e **Ferrari**, matemáticos tentaram resolver o mistério da quíntica. Alguns grandes nomes da matemática naufragaram, incluindo **Leonhard Euler** e **Joseph Louis Lagrange**. Este último ainda publicou um artigo famoso "Reflexão sobre a Resolução das Equações Algébricas".

6.9.1 Paolo Ruffini

Paolo Ruffini (1765-1822) foi o primeiro matemático a sugerir que a quíntica não poderia ser resolvida por meio de radicais, e ofereceu uma prova que a solução algébrica de equações gerais de grau maior que 4 é sempre impossivel. Ruffini se baseou em **Lagrange**. Mas, na prova de Ruffini havia uma lacuna. Em sua tentativa de prova, Ruffini viu uma parcela da verdade: ele percebeu que o caminho para a solução passava por uma análise do que ocorria com as equações quando as raízes fossem permutadas. Neste ponto surgia a ideia do que veio a ser chamado de um *grupo de permutações*, um caso particular do que viria a ser um *grupo*. **Ruffini**, embora não tivesse formalizado a ideia de um *grupo de permutações*, ele provou os resultados iniciais básicos que viria a constituir a *teoria dos grupos*.

6.9.2 Abel

Niels Henrik Abel (1802-1829) era um algebrista norueguês que resolveu atacar o problema de resolver a quíntica. A pricípio achou que havia encontrado uma solução à maneira de Cardano e Ferrari. Depois de perceber que sua prova estava errada, ele chegou à conclusão oposta: era impossível encontrar uma expressão algébrica para as raízes da quintica geral.

Trabalhando na mesma linha de **Ruffini**, mas evitando os erros deste,**Abel** conseguiu provar que quíntica geral não podia ser resolvida pelos radicais. Sua prova trouxe um desfecho a um problema, cuja jornada de solução começara a mais de três milênios antes, no Egito. Abel publicou um ensaio que trazia um esboço de sua prova. **Abel** faleceu aos 27 anos, sem saber que seus escritos haviam causado uma empolgação na comunidade matemática. Deve-se a **Abel** o primeiro estudo sistemático das funções algébricas

Figura 48 – Ruffini - A ideia de grupo de permutações, precursor da Teoria dos Grupos.

Fonte: ⟨https://it.wikipedia.org/wiki/Paolo_Ruffini_(matematico).⟩

Figura 49 – Abel - A quíntica geral não podia ser resolvida pelos radicais.

Fonte: https://en.wikipedia.org/wiki/Niels_Henrik_Abel.

6.9.3 Galois

Évariste Galois (1811-1832), de considerável talento matemático, também foi um personagem importante na tentativa de resolver a quíntica. Embora **Abel** tenha sido o primeiro a demonstrar a insolubilidade da quíntica, **Galois** descobriu uma abordagem muito mais geral para o problema, que estava destinada a se tornar muito importante. **Galois** foi o primeiro a formalizar o conceito matemático de um *grupo algébrico*, que é uma das ideia centrais da Álgebra moderna. A conexão entre **equações polinomiais**, **grupos** e *corpos* é um dos temas fundamentais do ramo da matemática conhecido como *Teoria de Galois*.

Figura 50 – Évariste Galois.

Fonte: www.unicauca.edu.co.

A teoria de **Galois** não somente explica porque não existe solução geral para a quíntica, como também mostra precisamente porque os polinômios de menor grau tem soluções. Qaundo se diz que não existe uma fórmula para polinomiais de grau cinco, significa dizer que a "linguagem"para descrever soluções é composta simplesmente de números inteiros, radicais e expressões algébricas que os envolviam. O que se poderia dizer é que, se existissem fórmulas que de fato extraiam as raizes dos polinômios de grau 5, elas usariam outras expressões que não os radicais. Isto é, a "linguagem"para descrever as raízes seria outra. Até mesmo, sendo necessário a definição de um conjunto de números superior aos números complexos, pois no nível desses, até já existem nas raízes de polinômios de grau 2. O que é interessante aqui é saber que, para entender este assunto completamente, é necessário aprender a teoria de **Galois**. E, para entender a teoria de *Galois*, é necessário em primeiro plano fazer um curso de Álgebra abstrata no curso de graduação.

Neste período, a Álgebra teve modificado o seu caráter ancestral. Em vez de tratar da teoria das equações algébricas (polinomiais), tornou-se a doutrina abstrata dos dias de hoje, com as estruturas algébricas de *anéis* e *corpos*. Mas, uma das origens da Álgebra moderna, no século XIX, foi o desenvolvimento da *teoria dos grupos*, partindo da *teoria de Galois* das equações algébricas e levando a uma teoria abstrata

autônoma, especialmente à *teoria dos grupos finitos*, estabelecendo deste modo um modelo para a transformação da Álgebra como um todo.

Este desenvolvimento da Álgebra pode ser estudado na obra *Lehrbuch der Algebra* (2 vols. 1895-1896) de **Heinrich Martin Weber** (1842-1913), um matemático alemão, professor em Königsberg. Sua área de interesse era álgebra e teoria dos números. É mais conhecido por esta obra. **Weber** teve, em Königsberg, seus alunos famosos, **Hilbert** (ver no capítulo 14) e **Hermann Minkowiski** (1864-1909). Este livro de **Weber** tem capítulos especiais sobre grupos e corpos algébricos.

Figura 51 – Weber - o professor orientador de Hilbert, algebrista do século XIX.

Fonte: ⟨https://pt.wikipedia.org/wiki/Heinrich_Weber.⟩

Quando finalmente se desenvolveu uma notação apropriada (empregando letras para representar coeficientes e variáveis), foi possível determinar fórmulas gerais de resolução de equações e discutir métodos de trabalho também gerais. Porém, mesmo nestes casos, tratava-se de situações relativamente concretas. As letras representavam sempre algum tipo de números (inteiros, racionais, reais ou complexos) e utilizavam-se as propriedades destes de forma mais ou menos intuitiva. Como veremos adiante, a formalização destes conceitos de modo preciso só aconteceria a partir do século XIX. Foi precisamente nesse século que alargou-se consideravelmente o conceito de operação. Alguns autores da época não mais se restringem a estudar as operações clássicas entre números, mas dão ao termo um significado bem mais amplo e estudam operações entre elementos, sem se preocupar com a natureza destes, interessando-se apenas com as propriedades que estas operações verificam.

A passagem da **álgebra clássica** para a assim chamada **álgebra abstrata** foi um processo sumamente interessante. Representa não somente um progresso quanto aos conteúdos técnico-cietíficos da disciplina como amplia consideravelmente o seu campo de aplicação e, o que é mais importante, implica - num certo sentido - uma

mudança na própria concepção do que a matemçatica é, da compreenção de sua condição de ciência independente.

Frege (1848-1925) (ver capítulo 8) e **Peano** (1858-1932) também fizeram o seu trabalho pioneiro neste tema e as suas consequências foram examinadas na obra *Algebraisch Theorie der Körper* (1910), por **Ernst Steinitz** (1871-1928). Nesta última obra , um corpo algébrico (*körper*) é o conceito abstrato principal, num sistema de elementos que tem duas operações, a adição e a multiplicação, satisfazendo a propriedades de tipo associativo, comutativo, e distributivo.

6.10 Os ramos da Álgebra Moderna

Atualmente, em Matemática, Álgebra é o ramo que estuda a manipulação formal de equações, operações matemáticas, polinômios e estruturas algébricas Benatti (2015). O termo álgebra, na verdade, compreende um espectro de diferentes ramos algébricos da matemática, cada um com suas especificidades. As algébras tem sido relavantes para a construção da ciência da computação. A **Álgebra Elementar** que faz parte do currículo no ensino secundário, introduz o conceito de variável representativa de números. Expressões usando estas variáveis são manipuladas usando as regras de operação aplicáveis a números, como a adição. Estes conceitos podem ser usados, por exemplo, na resolução de equações. Na **Álgebra Abstrata** as suas definições exatas conduzem às estruturas tais como os *grupos*, *anéis* e *corpos*. A **Álgebra Linear** se utiliza de alguns conceitos e estruturas fundamentais da matemática como vetores, espaços vetoriais, transformações lineares, sistemas de equações lineares e matrizes, e forma a base matemática da área da computação gráfica. A **Álgebra Computacional**, também conhecida por *computação algébrica* ou *computação simbólica*, serve para a manipulação de fórmulas matemáticas por computadores digitais Davenport, Siret e Tournier (1993), através da computação com símbolos representando objetos matemáticos.

6.11 Bibliografia e Fonte de Consulta

François Viète - https://pt.wikipedia.org/wiki/François_Viete

História do Teorema Fundamental da Álgebra - http://www.prof2000.pt/users/amma/af33/trf1/trigo_p79
84.htm

História do Teorema Fundamental da Álgebra - https://pt.wikipedia.org/wiki/Teorema_fundamental_da_À

James D. Stein - Como a Matemática explica o Mundo, Editora Campus-Elsevier, 2008.

Jim Stein - How Math Explains the World, HarperCollins Publishers, 2008.

E.W. Beth, G. Choquet, J, Dieudonné, C. Gattegno, A. Lichenrowicz e G. Piaget, L'Enseignement des Math´ematiques, Delacheaux & Niestlé, Paris.

N. Bourbaki, Eléments d'histoire des Mathematiques, Hermann, Paris, 1969.

F. Cajori, A History of Mathematical Notations, Dover, New York, 1993.

C. Polcino Milies, A Gênese da Algebra Abstrata, Coleção Tópicos de Matemática Elementar, IMEUSP, São Paulo, 1987.

R.J. Gillings, Mathematics in the times of the Pharaohs, Dover, New York, 1982.

Halberstein, H. and Ingram, R.C., eds. - The Mathematical Papers of Sir William Rowan Hamilton, vol III, Cambridge Univ. Press, London, 1967. p.49-50.

Hankins, T.L. - Algebra as Pure Time: William Rowan Hamilton and the Foundations of Algebra, in Motion and Time, Space and Matter P. Machamer e R. Turnbull, eds., Ohio Univ. Press, Columbus, 1976.

Kline, M. - Mathematical Thought from Ancient to Modern Times, Oxford Univ. Press, New York, 1972.

Ohstrom, P. - W. R. Hamilton's Views of Algebra as the Science of Pure Time, Hist. Math. 12, (1985), 45-55.

Parshall, K. - Joseph H. M. Wedderburn and the Structure Theory of Algebras, Archiv Hist. Exact Sci., 32, (1985), 223-349.

6.12 Referências - Leitura Recomendada

Mathematical Foundations fo Computer Science 2011 - Proceedings of 36th Internation Symposium, MFSC 2011, Warsaw, Poland, August 22-26, Springer.

François Viète - Mathematicians

François Viète - em Handbook to Life in Renaissance Europe - Sandra Sider.

Paolo Ruffini, Teoria generale delle equazioni (⟨http://gutenberg.beic.it/webclient/DeliveryManager?pid=1367335&search_terms=DTL4⟩). 2, Bologna, nella stamperia di STommaso d'Aquino, 1799. URL consultada em 29 de Outubro de 2015.

Luiz Henrique Jacy Monteiro - Iniciação às Estruturas Algébricas, G.E.E.M, São Paulo, Serie Professor N6, 1968.

R. A. Dean - Elements of Abstratct Algebra, Wiley, 1967.

Matthew Hennessy - Algebrac Thory of Processes, The MIT Press, 1988.

I. Herstein - Tópicos de Álgebra, 1964.

Pycior, H., Early Critisism of the Symbolical Approach to Algebra, Hist. Math. 9, (1982), 392-412.

Richards, J. - The Art and Science of British Algebra: a Study of Perception of Mathematical Truth, Hist. Math., 7, (1980), 345 - 365.

Van der Waerden, B.L., A History of Algebra, Springer-Verlag, Berlin, 1985.

C.B. Boyer, História da Matemática, (edição revista por U.C. Merzzbach), Edgar Blucher, São Paulo, 1996.

L.E. Dickson, Algebras and their arithmetics, Univ. Chicago Science Press, Chicago, 1923.

Dubbey, J.M. - Babbage, Peacock and Modern Algebra, Hist. Math., 4, (1977), 295-302.

Fine, B. and Rosenberger, G., The fundamental theorem of algebra, Springer-Verlag, New York, 1997.

CAPÍTULO 7

A Lógica - De Leibniz a Boole

NEste capítulo estaremos falando sobre as contribuições científicas dos lógicos que mais se destacaram no advento da lógica símbolica: **Aristóteles**, **Leibniz**,**George Boole** e **De Morgan**. Depois, a evolução da lógica, como ciência do raciocínio, tem seguimento com **Friedrich Ludwig Gottlob Frege** no século XIX, como será mostrada no capítulo 8.

7.1 O Início da Lógica

Lógica, uma palavra do grego *logos*, tem dois significados principais: discute o uso do *raciocínio humano* e é o estudo do raciocínio válido. No segundo sentido, a lógica é discutida principalmente nas disciplinas de filosofia, matemática e ciência da computação. Para os nossos propósitos enfatizamos o uso da lógica símbolica na ciência da computação.

A Lógica examina de forma genérica as formas que uma argumentação pode tomar, quais dessas formas são válidas e quais são falaciosas. Na matemática, estudam-se as formas válidas de inferência de uma linguagem formal. Na ciência da computação, a lógica é uma ferramenta indispensável. Por fim, a lógica também é estudada na teoria da argumentação Cox J. Robert; Willard (1983).

A Lógica foi estudada em várias civilizações da Antiguidade (3500 a.C.-476 d.C). A Lógica, como disciplina intelectual, foi criada no século IV a.C. por **Aristóteles**. Na Grécia Antiga a lógica foi estabelecida como disciplina por **Aristóteles** que estudava as leis do pensamento. Aristóteles (384 a.C.-322 a.C.) foi um filósofo grego, aluno de **Platão**. Ver Figura 55. Seus escritos abrangem diversos assuntos e juntamente com Platão e Sócrates (professor de Platão), Aristóteles é visto como um dos fundadores da filosofia ocidental. Aristóteles foi o autor do primeiro trabalho sobre Lógica. A Lógica de Aristóteles constitui o exemplo mais sistemático em mais de 2300 anos de história. Sua premissa principal envolve uma teoria de caráter semântico desenvolvida por ele para servir de estrutura para a compreensão da veracidade de proposições.

Foi por meio de sua lLógica que se estabeleceu a primazia da Lógica dedutiva Oliver (1998).

Figura 52 – Em 335 a.C. Aristóteles funda sua própria escola em Atenas, em uma área de exercício público denominada *Liceu*

Fonte: A escola de Aristóteles por Gustav Adolph Spangenberg, 1883-1888, em https://pt.wikipedia.org/wiki/Aristoteles.

Aristóteles sistematizou a Lógica, definindo as formas de inferência que eram válidas e as que não eram - em outras palavras, aquilo que realmente decorre de algo e aquilo que só aparentemente decorre; e deu nomes a todas essas diferentes formas de interferências. A lógica é frequentemente dividida em duas formas do raciocínio de inferência: o raciocínio indutivo e o raciocínio dedutivo. Por 2000 anos, estudar lógica, significou estudar a lógica de Aristóteles.

Um *silogismo* ("conexão de ideias", "raciocínio" composto pelos termos "com" e "cálculo") é um termo filosófico com o qual Aristóteles designou a argumentação lógica perfeita, constituída de três proposições declarativas que se conectam de tal modo que a partir das duas primeiras, chamadas premissas, é possível deduzir uma conclusão. A teoria do *silogismo* foi exposta por Aristóteles. Sua teoria do silogismo constitui o cerne de sua lógica e através dela tenta caracterizar as formas de silogismo e determinar quais deles são válidas e quais não, o que conseguiu com bastante sucesso. Como primeiro passo no desenvolvimento da lógica, a teoria do silogismo foi extremamente importante. A Figura 53 ilustra a ideia de silogismo.

Seus escritos abrangem diversos assuntos, entre outros, como as leis da lógica. Juntamente com Platão e Sócrates (professor de Platão), Aristóteles é visto como um dos fundadores da filosofia ocidental. Em 335 a.C. funda o *Liceu* na cidade de Atenas. O *Liceu* de Aristóteles era uma escola que mantinha cursos regulares, de manhã e à tarde, sobre lógica, física, metafísica, retórica, política e literatura.

A filosogia grega liderada por **Aristóteles** considerava que qualquer argumento

Figura 53 – Os dois cães veritas e falsitas correm atrás da lebre problema, a lógica apressa-se armada com a sua espada *syllogismus*.

Fonte: por Gregor Reisch em Margarita Philosophica, Typus Logic.

lógico (uma proposição) poderia ser reduzido a duas premissas e uma conclusão. Aristóteles criou três princípios que notearam o início da lógica como ciência:

1. Princípio da Identidade: "Uma coisa é igual a si mesmo: A = A."
2. Pricípio do meio excluido: "Uma proposição é verdadeira ou falsa, isto é, "A ou não-A".
3. Princípio da Contradição: "Nenhuma proposição pode ser falsa e verdadeira". "A não pode ser A e não-A".

A lógica de Aristóteles dominou o pensamento científico no mundo ociental por 2000 anos. *Silogismo* é um termo filosófico com o qual Aristóteles designou a argumentação lógica perfeita, constituída de três proposições declarativas que se conectam de tal modo que a partir das duas primeiras, chamadas *premissas*, é possível deduzir uma *conclusão*. Os silogismos seguem algumas regras como:

- Todo silogismo (argumento) contém somente 3 *termos*: maior, médio e menor.
- Os termos da conclusão não podem ter extensão maior que os termos das premissas.
- O termo médio não pode entrar na conclusão.
- O termo médio deve ser universal ao menos uma vez.
- De duas premissas negativas, nada se conclui.
- De duas premissas afirmativas, não pode haver conclusão negativa.

- A conclusão segue sempre a premissa mais fraca.
- De duas premissas particulares, nada se conclui.

Silogismo regular é o argumento típico dedutivo, composto de 3 proposições - *Premissa Maior* (P), *Premissa Menor* (p) e *Conclusão* (c) - onde 3 *termos*, Maior (T), Médio(M) e Menor (t), são compostos 2 a 2. Num silogismo, as premissas são *um* ou *dois* juízos que precedem a conclusão e, dos quais ela decorre como consequente necessário dos antecedentes, dos quais se infere a consequência. Nas premissas, o *termo maior* (formará o predicado da conclusão) e o *termo menor* (formará o sujeito da conclusão) são comparados com o *termo médio*, e assim temos a premissa maior e a premissa menor, segundo a extensão dos seus termos. Como exemplificado na Figura 54.

Figura 54 – Um exemplo clássico de silogismo.

Fonte: http://www.colegioweb.com.br/curiosidades/como-funciona-o-silogismo-aristotelico.html.

Outro exemplo é: “Todo político é mentiroso”. (1ª premissa, a declaratória) “Luiz é político”. (2ª premissa, a indicativa). Logo, “Luiz é mentiroso”. (conclusão)

Mais de 2300 anos depois de sua morte, Aristóteles continua sendo uma das pessoas mais influentes. Ele contribuiu para quase todos os campos do conhecimento humano e foi o fundador de muitas áreas novas. Entre inúmeras outras conquistas, Aristóteles foi o fundador da lógica formal. Lógica formal é o estudo da inferência com conteúdo puramente formal. Uma inferência possui um conteúdo puramente formal se ele pode ser expresso como um caso particular de uma regra totalmente abstrata, isto é, uma regra que não é sobre uma qualquer coisa em particular. As obras de Aristóteles contêm o primeiro estudo formal da lógica.

O nascimento da chamada lógica moderna, através do trabalho de **Gottlob Frege** no século XIX (1879) e **Bertrand Russell** no século XX (Principia Mathematica em 1910-1913, Introdução à Filosofia da Matemática em 1919), trouxeram a tona sérias limitações da lógica aristotélica. Mas, a lógica formal moderna segue e amplia o trabalho de Aristóteles Mckeon (2001).

Lógica simbólica é o estudo das abstrações simbólicas que capturam as características formais da inferência lógica Hamilton (1980). A lógica simbólica é frequentemente dividida em dois ramos que constituem as lógicas clássicas. **lógica proposicional** (iniciada por **Leibniz**, desenvolvida por **Boole, De Morgan**) que sistematizou o conceito de verdades absolutas, e a **lógica de predicados** (proposta por **Gottlob Frege**), chamadas de Lógicas clássicas, sendo que a Lógica Proposicional deu surgimento a Álgebra Booleana e formou a base do projeto de hardware dos computadores digitais. E a Lógica dos Predicados, estendida a partir da Lógica proposicional, introduziu o conceito das verdades relativas, é até hoje, utilizada na Matemática e na programação de computadores.

A Lógica aristotélica havia se tornado amplamente aceita em ciências e matemática. **Leibniz** propôs sistematizar a lógica de Aristóteles, que manteve-se em ampla utilização no Ocidente até o início do século XIX. O sistema lógico de Aristóteles foi responsável pela introdução do silogismo hipotético, da lógica indutiva Berman (1983) e a lógica modal temporal Knuuttila (1981) Fisher, M. e Gabbay (2005), estas últimas complementares das lógicas clássicas. Pela lógica temporal, há situações em que os atributos de " verdadeiro" e "falso" não bastam, e é preciso determinar se algo é "*Verdadeiro no período de tempo T*" ou "*Falso após o evento E*". Para isso, é utilizado um sistema lógico específico que inclui novos operadores para tratar dessas situações Fisher, M. e Gabbay (2005). Mais tarde no século XX, **Zohar Manna** e **Pnueli** provaram a lógica temporal no sentido da especificação e verificação de propriedades de sistemas de computação.

Figura 55 – Platão e Aristóteles - Na Escola de Atenas,

Fonte: por Rafael Sanzio, na Stanza della Segnatura, nos Museus Vaticanos. Fonte: https://pt.wikipedia.org/wiki/Aristoteles.

7.2 Leibniz - O sentido matemático da Lógica Aristotélica

Mas, foi **Gottfried Wilhelm Leibniz** (1646-1716) quem primeiro tentou dar a lógica aristotélica um sentido matemático. **Leibniz** acreditava que para resolver todos os problemas da cooperação humana deveria existir uma *linguagem universal* e uma *álgebra do raciocínio* ("calculus raciocinator").

Leibniz desenvolveu uma **técnica pela qual todo raciocínio poderia ser reduzido a um cálculo matemático**. **Leibniz** imaginava, uma técnica servindo como um tipo de **linguagem universal**, cujos símbolos e vocabulário eram direcionados ao raciocínio de uma maneira que erros, exceto aqueles que de fato existissem, eram simplesmente o resultado da aplicação incorreta das regras. A linguagem deveria ser ideográfica, cada símbolo representando um conceito bem definido Janos (2009).

Figura 56 – Leibniz - A linguagem universal e o cálculo do raciocínio.

Fonte: iep.utm.edu.

Embora, a lógica de **Aristóteles** tenha dominado o pensamento científico no mundo ocidental por 2000 anos, Mas, foi a idéia de uma "linguagem universal"cultivada por **Gottfried Wilhelm Leibniz** (1646-1716), quem desenvolveu um método de raciocínio lógico, que iniciava o advento da lógica moderna.

Como curiosidade, o uso de "*função*"como um termo matemático foi iniciado por Leibniz, em uma carta de 1694, para designar uma quantidade relacionada a uma curva, tal como a sua inclinação em um ponto específico Arp e Caplan (2013b).

Leibniz - o precursor da lógica simbólica

Depois dos desenvolvimentos da matemática nos séculos XVI e XVII, a idéia da introdução do *simbolismo* já vinha sendo amadurecida. A lógica moderna começou ainda no século XVII com **Leibniz**. Para contornar a ambiguidade dos termos e

dos processos conclusivos da linguagem ordinária, **Leibniz** viu surgir a idéia central de sua nova lógica precisamente como projeto de criação de uma lógica simbólica e de caráter completamente calculístico, análogos aos procedimentos matemáticos. Ou seja, se estava construindo um *simbolismo* cada vez mais manipulável e seguro, capaz de funcionar de uma maneira, por assim dizer, mecânica e automática, sujeito a operações que, no fundo, não eram mais do que regras para manipulação de símbolos.

Seus estudos influenciaram, 200 anos mais tarde, vários ramos da lógica matemática moderna e outras áreas relacionadas, como por exemplo a *Cibernética*.

"*Norbert Wiener dizia que se fosse escolher na História da Ciência um patrono para a Cibernética, elegeria Leibniz*").

Leibniz deu-se conta de tudo isto e concebeu, também para a dedução lógica. Ele fez a desvinculação do conteúdo semântico das proposições, isto é, considerando regras cuja aplicação pudesse prescindir da consideração do conteúdo semântico das expressões. Isto veio aliviar o processo de inferência, do esforço de manter presente o significado. Deste modo coube a **Leibniz** a descoberta da verdadeira natureza do "cálculo"em geral, além de aproveitar pela primeira vez a oportunidade de reduzir as regras da dedução lógica a meras regras de cálculo. **Leibniz** influenciou seus contemporâneos e sucessores através de seu ambicioso programa para a Lógica. Este programa visava criar uma linguagem universal baseada em um alfabeto do pensamento, chamada *characteristica universalis* e uma espécie de cálculo universal para o raciocínio.

Na visão de **Leibniz** a linguagem universal deveria ser como a álgebra: uma coleção de símbolos básicos que padronizassem noções simples. Noções mais complexas teriam seu significado através de construções apropriadas envolvendo os símbolos básicos, que iriam assim refletir a estrutura das noções complexas. Numerais, palavras que indica os seres em termos numéricos, isto é, que atribui quantidade aos seres ou os situa em determinada sequência, seriam usados para representar noções *não analíticas* (não sujeitas a análise), os quais poderiam tornar possíveis que as verdades de qualquer ciência pudessem ser "calculadas"por operações aritméticas, desde que formuladas na referida linguagem universal ((22, volume XI)) .

Essa idéia de **Leibniz** sustentava-se em dois conceitos intimamente relacionados: o de um **simbolismo universal** e o de um **cálculo de raciocínio** (isto é, um método quase mecânico de raciocínio). Isto para a história da computação tem um particular interesse, pois esse *calculus ratiocinator* de **Leibniz** continha o embrião da máquina de raciocinar buscada, três séculos depois, por *Alan Turing* e depois pelos pesquisadores dentro do campo da Inteligência Artificial. **Leibniz** percebeu, bem antes, de **George Boole**, *Charles Babbage* e *Alan Turing*, a possibilidade da mecanização do cálculo aritmético.

O próprio **Leibniz** e seu contemporâneo **Blaise Pascal** procuraram construir máquinas de calcular. O leitor encontrará sobre máquinas de calcular no capítulo sobre Calculadoras Mecânicas, a Pré-História dos Computadores, no volume II. Nota-se portanto, que o mesmo impulso intelectual que o levou ao desenvolvimento da lógica matemática, o conduziu à busca da mecanização dos processos de raciocínio.

Ressalte-se aqui atenção sobre a idéia de uma *linguagem universal*. Como já foi dito, ele captou muito bem as inúmeras ambigüidades a que estão submetidas as linguagens de comunicação ordinárias e as vantagens que apresentam os símbolos da aritmética e da álgebra. Ao querer dar à lógica uma linguagem livre de ambigüidades e ao procurar associar a cada idéia um símbolo e, obter a solução de todos os problemas mediante a combinação destes símbolos,**Leibniz** acabou provocando um novo desenvolvimento da própria lógica.

A idéia de uma linguagem universal ("*characteristica universallis*") e do "*calculus ratiocinator*", foi a contribuição de **Leibniz** ao desenvolvimento da lógica. Esta contribuição aparece sob dois aspectos: ele aplicou com sucesso métodos matemáticos para a interpretação dos silogismos aristotélicos, e apontou aquelas partes da álgebra que estão abertas a uma interpretação não aritmética. Pela primeira vez se expôs, de uma maneira clara o princípio do procedimento formal. **Leibniz** tornou-se, assim, o grande precursor da lógica matemática simbólica, com origem na segunda metade do século XVII.

Na realidade, o trabalho de **Leibniz** ficou substancialmente reduzido a alguns fragmentos, parciais, muito interessantes e capazes de nos dar uma idéia de como concebia sua obra. Nem sequer seus seguidores diretos levaram para a frente a construção do cálculo lógico, mais além de um nível muito rudimentar. Provavelmente, a *characteritica universallis* tenha afastado **Leibniz** de objetivos de construir o primeiro cálculo lógico autêntico. Em uma linguagem universal deveria ser possível falar sobre temas, além do conjunto de números. Teria-se que poder falar, argumentos lógicos, sobre os fatos da vida cotidiana. Mas, não seria conveniente trabalhar com uma infinidade de símbolos referentes a cada um dos temas. A ideia de **Leibniz**: *um mesmo conjunto de símbolos serviria para falar de todos os temas* através de proposições.

Nos tempos de hoje, uma **proposição** é uma declaração que poderia somente ser julgada, de forma absoluta, como *verdadeira* (V) ou *falsa* (F), mas nunca como verdadeira e falsa simultaneamente. Existem declarações que não são proposições, mas que são chamadas de **sentenças**. E quais são as **declarações** que não são proposições? Uma declaração *aberta* não é considerada proposição, pois não é possível julgá-la como verdadeira nem como falsa. Pois ela depende dos valores assumidos por variáveis contidas nela. Neste caso, diz-se que no caso de sentenças temos verdades relativas. Como exemplo, (a) considere a **proposição**: "Leibniz propôs uma linguagem universal". Neste caso, pode-se dizer que a declaração é verdadeira. (b) Considere a **sentença**: "*Ele* propôs uma linguagem universal". Nesta segunda declaração é

impossível dizer se ela é verdadeira ou falsa sem saber quem é a variável "*Ele*" (qual o valor de "Ele").

O *calculo ratiocinator* seria um cálculo proposicional descrevendo uma técnica, que utilizando operadores lógicos "**e**", "**ou**", "**não**", possibilitaria as proposições lógicas para denotar qualquer argumento lógico possível. Uma **proposição** descreve e comunica um ou mais fatos, devendo ser **verdadeira** ou **falsa**. Uma proposição seria denotada por "*p*" e lê-se "*p é tal que*". Uma proposição é **válida** quando seu valor é **verdadeiro**. Uma proposição seria composta de **subproposições** unidas pelos operadores lógicos "**e**", "**ou**", "**não**", "implicação", "equivalência" e mais as "tautologias", "princípio da contradição" (este princípio de **Aristóteles** estabelece que, a negação de uma proposição falsa é verdadeira) e o "princípio do silogismo" (uma forma de argumentação que deduz uma conclusão válida a partir de duas premissas).
O **Cálculo Proposicional** é um *sistema dedutivo* que usa a *linguagem da lógica simbólica* para representar um conjunto de inferências válidas (deduções), isto é, preservando a veracidade (verdade), a partir de expressões com "**e**", "**ou**", "**não**", "**implicação**", "**equivalência**". O que interessa são apenas as **inferências válidas**, do ponto de vista da lógica em si Janos (2009), ou seja, dentro do escopo da sintaxe da linguagem da lógica, abstraindo-se o significado (semântica) da proposição (também chamada de sentença). O leitor pode aprender mais sobre esses conceitos, em Janos (2009),Manna (1985) ou Filho (2002).

7.3 A Lógica Proposicional

A Lógica Proposicional, também chamada Lógica Sentencial é a linguagem lógica que formaliza a estrutura lógica mais elementar do discurso matemático, definindo precisamente o significado dos conectivos lógicos "nao" ($\neg$), "e" ($\wedge$), "ou" ($\vee$), "se-entao" (condicional, $\rightarrow$), e o "se-e-somente-se" (bicondicional, $\leftrightarrow$). A definição da Lógica Sentencial desdobra-se na especificação do que seja uma linguagem proposicional e na descrição de uma abstração adequada para os princípios lógicos que governam os conectivos.

Primeiro, introduzimos os símbolos básicos e mostramos como eles são combinados para formar as setenças abstratas da Lógica Proposicional. Apresentamos regras sintáticas com as quais combinações de símbolos são tomadas ser sentenças na linguagem. Também consideramos o que estas sentenças significam.

7.3.1 A Linguagem

Definição (**Proposições**)

As sentenças da lógica proposicional são feitas dos seguintes símbolos, chamados proposições:

Tabela 3 – Regras semânticas para os conectivos lógicos

Notação Informal	Notação Convencional
and	$\wedge$
or	$\vee$
not	ou $\neg$
if-then	$\supset$ *ou* $\rightarrow$
if-and-only-if	$\equiv$ *ou* $\leftrightarrow$

Fonte: The Logical Basic for Computer Programming, Volume I, Manna e Waldinger.

Os símbolos proposicionais (não-lógicos): P, Q, R, S, P_1, Q_1, R_1, S_1, P_2, Q_2, R_2, S_2.

Os símbolos: *truth* e *false*, usados em proposições.

Os símbolos lógicos:

- Pontuação: (,)
- Conectivos: "nao" ($\neg$), "e" ($\wedge$), "ou" ($\vee$), "se-entao" (condicional, $\rightarrow$), e o "se-e-somente-se" (bicondicional, $\leftrightarrow$)

Os símbolos de veracidade e falsidade: *truth* e *false*, que podem aparecer nas expressões da Lógica.

Definição (**Sentenças**)

Usaremos as letras $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$, e $\mathcal{H}$, podendo ser escritas com subscritos, para representar as *sentenças*. Contudo, estes símbolos não são parte da linguagem da Lógica Proposicional, mas somente em nossa "metalinguagem" informal, a linguagem na qual falamos usando a Lógica Proposicional.

Definição (**Sentenças**)

As sentenças da Lógica Proposicional são construídas a partir das proposições, por aplicação dos conectivos proposicionais:

Em cada caso, as sentenças $\mathcal{F}$, $\mathcal{G}$, e $\mathcal{H}$, usadas para se construir sentenças mais complexas, pelas regras acima, serão chamadas suas componentes. Assim, os componentes de if $\mathcal{F}$ then $\mathcal{G}$, são $\mathcal{F}$ e $\mathcal{G}$.

Toda sentença intermediária que usamos para construir uma sentença $\mathcal{E}$, incluindo a própria $\mathcal{E}$, é uma subsentença de $\mathcal{E}$. Assim, as subsentenças de $\mathcal{E}$ é a própria $\mathcal{E}$, as componentes de $\mathcal{E}$, e as subsentenças destas componentes.. As subsentenças de $\mathcal{E}$, outras diferentes do que a própria $\mathcal{E}$ são as subsentenças próprias de $\mathcal{E}$.

Exemplo - Uma sentença $\mathcal{E}$: $((\ (P \vee Q)) \equiv ((\ P) \wedge (\ Q)))$

- As proposições P e Q sentenças.
- $(P \wedge Q)$, $\neg P$, e $\neg Q$ são sentenças.
- $(\ (P \vee Q)$ e $((\neg P) \wedge (\neg Q))$ são sentenças.
- E a expressão $\mathcal{E}$: $((\neg(P \vee Q)) \equiv ((\neg P) \wedge (\neg Q)))$ é uma sentença.

Cada das 8 sentenças (incluindo $\mathcal{E}$) é uma subsentença de $\mathcal{E}$; cada das 7 sentenças (excluindo $\mathcal{E}$) é uma subsentença própria de $\mathcal{E}$.

7.3.2 O Significado de uma Sentença

Até o momento temos apresentado a sintaxe (ou forma) das sentenças, sem atribuir qualquer significado (semântica) a essas. Agora é mostrado como atribuir um valor de veracidade (**true**) ou falsidade (**false**) para uma sentença da Lógica Proposicional. Nós devemos distinguir os símbolos *true* e *false* os quais podem ocorrer dentro de uma sentença, os quais são sempre italizados, dos valores semânticos **true** e **false**, os quais são os possiveis significados de uma sentença, que são escritos em fontes não italizadas.

É significativo falarmos sobre se os valores semânticos de uma sentença (**true** ou **false**), se nós sabemos os valores semânticos dos próprios símbolos P e Q. Esta informação é provida, pelo que se chama de *interpretação*.

Definindo mais precisamente a noção de *interpretação*.

Definição (**Interpretação**)

Uma interpretação $\mathcal{I}$ é uma atribuição de uma valor-semântico (true ou false), para cada conjunto de símbolos proposicionais; a interpretação *vazia* atribui um valor semântico a nenhum símbolo. Para cada sentença $\mathcal{F}$, uma interpretação $\mathcal{I}$ é dita ser uma interpretação para $\mathcal{F}$, se $\mathcal{I}$ atribui um valor semântico, **true** ou **falso**, para cada dos símbolos proposicionais de $\mathcal{F}$.

Definição (**Regras Semânticas**)

- Regra *proposição*: O valor semântico de cada símbolo proposicional, P, Q, R, S, numa expressão lógica $\mathcal{E}$ é o mesmo como o valor semântico atribuido a $\mathcal{E}$ por $\mathcal{I}$.
- Regra *true*: A sentença *true* (... é verdade ...) é **true** sob $\mathcal{I}$.
- Regra *false*: A sentença *false* (... é falso ...) é **false** sob $\mathcal{I}$.

De outra forma, estas regras podem também ser expressas por *tabelas-verdade* (criadas por **Emil Post**) e sumarizadas para os conectivos lógicos como:

Tabela 4 – Regras semânticas para o conectivo lógico *not*

$\mathcal{F}$	$not\mathcal{G}$
true	true
true	false

Fonte: The Logical Basic for Computer Programming, Volume I, Manna e Waldinger.

Tabela 5 – Regras semânticas para os conectivos lógicos

$\mathcal{F}$	$\mathcal{G}$	$\mathcal{F} \wedge \mathcal{G}$	$\mathcal{F} \vee \mathcal{G}$	$\mathcal{F} \rightarrow \mathcal{G}$	$\mathcal{F} \equiv \mathcal{G}$
true	true	true	true	true	true
true	false	false	true	false	false
false	true	false	true	true	false
false	false	false	false	true	true

Fonte: The Logical Basic for Computer Programming, Volume I, Manna e Waldinger.

Tabela 6 – Regra semântica para *if-then-else*

$\mathcal{F}$	$\mathcal{G}$	$\mathcal{H}$	if $\mathcal{F}$ then $\mathcal{G}$ else $\mathcal{H}$
true	true	true	true
true	true	false	true
true	false	true	false
true	false	false	false
false	true	true	true
false	true	false	false
false	false	true	true
false	false	false	false

Fonte: The Logical Basic for Computer Programming, Volume I, Manna e Waldinger.

7.3.3 Definições Importantes

Definição (**válida**, **satisfatível**, **contraditória**, **implicação**, **equivalente**, **consistente**)

Uma sentença $\mathcal{F}$ é **válida**, se ela **verdadeira** sob toda interpretação para $\mathcal{F}$.

Uma sentença $\mathcal{F}$ é **satisfatível**, se ela **verdadeira** para alguma interpretação para $\mathcal{F}$.

Uma sentença $\mathcal{F}$ é **contraditória** (ou insatisfatível), se ela **falsa** sob toda interpretação para $\mathcal{F}$.

Uma sentença $\mathcal{F}$ **implica** uma sentença $\mathcal{G}$, se para toda interpretação $\mathcal{I}$ para $\mathcal{F}$ e $\mathcal{G}$, se $\mathcal{F}$ for verdadeira sob $\mathcal{I}$, então $\mathcal{G}$ é também verdadeira sob $\mathcal{I}$.

Duas sentenças $\mathcal{F}$ e $\mathcal{G}$ são **equivalentes**, se toda interpretação sob $\mathcal{F}$ e $\mathcal{G}$, então $\mathcal{F}$ tem o mesmo valor-semântico como $\mathcal{G}$.

Um conjunto de sentenças $\mathcal{F}_1$, $\mathcal{F}_2$, ... é **consistente**, se existe alguma interpretação $\mathcal{I}$, para $\mathcal{F}_1$, $\mathcal{F}_2$, ..., sob a qual cada $\mathcal{F}_i$ é verdadeira.

7.3.4 Esquemas de Sentenças Válidas

Até temos apresentado sentenças particulares da Lógica Proposicional e introduzido métodos para estabelecer sua validade. Podemos estabelecer a validade de um esquema de setenças.

Suponha o esquema tal que $\mathcal{F}$ or (not $\mathcal{F}$). Instanciando $\mathcal{F}$ como:

(Existem macacos em Jupiter) or (not(Existe macacos em Jupiter))

A veracidade desta sentença pode ser determinada a partir de sua estrutura, sem sabermos se seus constituintes são verdadeiros ou falsos.

Da mesma forma:

(Chuí tem pouco mais de 5 mil habitantes) or (not(Chuí tem pouco mais de 5 mil habitantes))

é verdadeira sem se consultar a prefeitura de Chuí. De fato, ambas as sentenças são instâncias da sentença abstrata

$$\mathcal{F} \vee (\neg \mathcal{F})$$

a qual implica que as sentenças:

- $P \vee (\neg P)$,
- $Q \vee (\neg Q)$,
- $((P \wedge Q) \vee (\neg(P \wedge Q)))$

e mais uma classe infinita de outras sentenças que se encaixam neste esquema, sejam todas válidas.

7.3.5 O método da Tabela-Verdade

As duas seções anteriores definiram a sintaxe e a semântica da linguagem da Lógica Proposicional e formalizaram ainda, do ponto de vista semântico, o conceito de implicação lógica. Esta seção descreve um método sistemático para decidir implicação lógica chamado de tabela-verdade.

O método baseia-se na observação de que, se $\mathcal{F}$ é um conjunto finito de proposições e Q é uma proposição, há um número finito de símbolos proposicionais ocorrendo em Q e nas proposições em $\mathcal{F}$. Logo, há um número finito de atribuições de valores-verdade

Tabela 7 – Implicação Lógica ou Consequência Lógica

A	B	C	$A \Rightarrow (B \Rightarrow C)$	$(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$
true	true	true	**true**	**true**
true	true	false	false	false
true	false	true	**true**	**true**
true	false	false	**true**	**true**
false	true	true	**true**	**true**
false	true	false	**true**	**true**
false	false	true	**true**	**true**
false	false	false	**true**	**true**

Fonte: The Logical Basic for Computer Programming, Volume I, Manna e Waldinger.

(valores semânticos) distintos para esses símbolos. Assim, para se decidir se $\mathcal{F}$ é uma implicação lógica para Q, ou Q é consequência lógica de $\mathcal{F}$, basta enumerar todas essas atribuições e, para cada delas que satisfizer a todas as proposições em $\mathcal{F}$, testar se ela também satisfaz Q. Se esta condição for sempre observada, então podemos afirmar que Q é consequência lógica de $\mathcal{F}$. Note que, se a interpretação $\mathcal{I}$ não satisfaz a alguma proposição em $\mathcal{F}$, o valor que a interpretação atribui a Q não importará, pela forma em que a *implicação lógica* foi definida. Indicamos implicação lógica da forma: $\mathcal{F} \Rightarrow Q$.

Este método naturalmente pode ser usado também para decidir se uma sentença é satisfatível, ou se duas sentenças são equivalentes.

Exemplos (**Implicação lógica**)

(a) Seja $\mathcal{F}$: $A \Rightarrow (B \Rightarrow C)$ e seja $\mathcal{G}$: $(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$.

A pergunta é $\mathcal{F} \Rightarrow \mathcal{G}$? A resposta pode ser vista na Tabela 7. Cada linha da tabela corresponde a atribuição de valores-semânticos, para os simbolos proposicionais A, B e C. Como para toda interpretação $\mathcal{I}$, se $\mathcal{F}$ é verdadeira, $\mathcal{G}$ também é verdadeira, então dizemos que $\mathcal{F}$ implica logicamente $\mathcal{G}$ e denotamos também por $\mathcal{F} \vDash \mathcal{G}$. E onde $\mathcal{F} \vdash Q$ para denotar que Q é um teorema, isto é, Q é uma dedução de $\mathcal{F}$.

Pode ser provado que se uma sentença $\mathcal{F}$ for um conjunto finito de proposições, digamos $\mathcal{F} = (P_1, P_2, \ldots, P_n)$, então $\mathcal{F} \vDash R$, se e somente se, $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow R$ é uma tautologia.

Além disso, se $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_n)$, então $\mathcal{F}$ e $\mathcal{Q}$ são tautologicamente equivalentes, se e somente se, $(Q_1 \wedge Q_2 \wedge \ldots \wedge Q_n) \leftrightarrow R$ é uma tautologia.

A tautologia mais trivial, já nos referimos. É a chamada **Lei do Terceiro Excluído**: "uma sentença ou é verdadeira ou é falsa". Formalmente, $\mathcal{F} \vee (\neg\mathcal{F}) = (\neg\mathcal{F}) \vee \mathcal{F}$.

Tabela 8 – Implicação Lógica ou Consequência Lógica

$\mathcal{F}$	$\mathcal{Q}$	Nome da Lei
$A * (B * C)$	$(A * B) * C$	associatividade
$A * B$	$B * A$	comutatividade
$A \wedge (B \vee C)$	$(A \wedge B) \vee (A \wedge C)$	distributividade
$A \vee (B \wedge C)$	$(A \vee B) \wedge (A \vee C)$	distributividade
$A \rightarrow (B \rightarrow C)$	$(A \rightarrow B) \rightarrow (A \rightarrow C)$	distributividade
$\neg(A \wedge B)$	$\neg A \vee \neg B$	De Morgan
$\neg(A \vee B)$	$\neg A \wedge \neg B$	De Morgan
$\neg\neg A$	A	
A $\rightarrow B$	$\neg A \vee B$	
$\neg(A \rightarrow B)$	$A \wedge \neg B$	
$\neg(A \leftrightarrow B)$	$(A \wedge \neg B) \vee (\neg A \wedge B)$	

Fonte: Programação em Lógica, Marco A. Casanova.

Há uma série de outras leis úteis da Lógica Proposicional (Sentencial) que podem ser apresentadas ou como tautologias da forma $\mathcal{F} \leftrightarrow \mathcal{G}$ ou como pares de sentenças $\mathcal{F}$, $\mathcal{G}$ que são tautologicamente equivalentes.

A tabela 8 apresenta algumas destas leis que podem ser usadas para expressar as sentenças da Lógica.

7.3.6 A Álgebra das Proposições

Toda Lógica é uma linguagem. Com uma linguagem, nós podemos expressar as proposições e as sentenças da Lógica. O que **George Boole** descobriu (ver no decorrer deste capítulo) é que com o conjunto de símbolos para proposições pode-se construir uma Álgebra. Neste caso, a Álgebra é dada pelo conjunto dos símbolos proposicionais, mais os conectivos lógicos.

A tabela 8 apresenta algumas leis desta Álgebra, com as quais podemos provar propriedades expressas pela Lógica. Com o Método da Tabela-Verdade podemos verificar várias propriedades envolvendo os conectivos lógicos e as proposições desta Lógica (Capítulo 7 em Filho (2002)), tratando as implicações e equivalências pelo **Método da Tabela-Verdade**.

Um outro método de prova desta Lógica é o **Método Dedutivo**. As implicações e equivalências podem ser provadas por este método mais eficiente. No emprego do Método Dedutivo desempeham papel importante as equivalências relativas à Álgebra das Proposições, que subsistem quando as proposições que nelas figuram são substituídas pelas sentenças compostas de proposições tautológias e contraditórias. Assim, com a visão de um **Método Dedutivo** mais a linguagem da Lógica, temos o que denominamos, neste caso, o **Cálculo** da Lógica. Neste caso, o Cálculo da Lógica

Proposicional é baseado numa Álgebra, a Álgebra das Proposições.

Algo muito interesse e inerente à esta Lógica Proposicional, é que esta Lógica trata de **verdades absolutas**: ou seja, uma proposição é verdadeira ou falsa. Uma sentença é verdadeira ou falsa. Este conceito ficará mais claro quando se estuda a Lógica dos Predicados, que será apresentada no capitulo 8.

7.4 De Morgan

Augustus De Morgan (1806-1871) foi um matemático e lógico indiano, mas britânico de vivência, professor de matemática na então recém-criada universidade, em Londres, cargo que ocupou até 1866. Foi o primeiro presidente da *London Mathematical Society*, fundada em 1866.

Figura 57 – A preparação do caminho para o nascimento da lógica simbólica.

Fonte: http://pt.wikipedia.org/wiki/Augustus_De_Morgan.

Como professor, um de seus primeiros trabalhos, *Elementos de Aritmética*, de 1831, distingue-se pelo tratamento filosófico das ideias de número e magnitude. Além disso, contribuiu para o simbolismo matemático propondo o uso do traço inclinado para a impressão das frações. Sua maior contribuição para o conhecimento foi como reformador da lógica. **Augustus De Morgan**. As realizações mais importantes de **De Morgan** foram o lançamento das bases, a preparação do caminho para o nascimento da lógica simbólica.

De Morgan apercebeu-se que Boole tinha aberto um novo e importante patamar. Sobre o trabalho de **Boole**, **De Morgan** formulou as *Leis de De Morgan* usadas na Lógica Proprosicional. Efetivamente, o renascimento dos estudos de lógica que começaram na primeira metade do século XIX deveu-se quase que inteiramente aos trabalhos de **George Boole**.

Surgiu a moderna concepção de álgebra, que levou à compreensão da álgebra como álgebra, ou seja, como o desenvolvimento abstrato das conseqüências de um grupo de postulados sem necessariamente a interpretação ou aplicação de números. Sem esta compreensão de que a álgebra em si mesma nada mais é do que um sistema abstrato, ela poderia ainda encontrar-se inserida no contexto aritmético do século XVIII, incapaz de avançar para as variantes propostas por **Hamilton** (1805-1865).

Por iniciativa própria, **Boole** separou os símbolos das operações matemáticas das coisas sobre as quais elas operavam, buscando compreendê-las. Seu trabalho nesta direção é extremamente interessante, porém obscurecido pelo seu principal interesse - a criação de um simples e manejável sistema simbólico.

7.5 George Boole: da Lógica à Álgebra

O trabalho da *linguagem universal* e a álgebra do raciocínio chamada "*calculus raciocinator*" foi uma inovação de **Leibniz** que seu sucessor, **George Boole** (1815-1864) um matemático inglês do século XIX, estendeu **transformando lógica em álgebra**. Daí, o termo "álgebra booleana" é uma homenagem a **George Boole**.

Boole foi o primeiro a definí-la como parte de um sistema de lógica em meados do século XIX. Mais especificamente, a **álgebra booleana** foi uma tentativa de utilizar técnicas algébricas para lidar com as regras de inferência do cálculo proposicional. Boole introduziu o sistema algébrico, inicialmente, em uma publicação simplificada, o *The Mathematical Analysis of Logic*, publicado em 1838, em resposta a uma controvérsia que existia entre **Augustus De Morgan** e **William Hamilton**, e mais tarde como um livro mais substancial, *The Laws of Thought*, publicado em 1854.

A Álgebra Booleana surgiu por volta de 1860, em artigos escritos por **William Jevons** e **Charles Sanders Peirce**. A primeira apresentação sistemática de Álgebra Booleana ocorreu em 1890. O primeiro tratamento extensivo de Álgebra Booleana foi em 1898, com *Universal Algebra* de **Whitehead** Lobur (2006). O que **Boole** viu foi que as regras de inferência do "*calculus raciocinator*" de Leibniz, já formavam uma **álgebra proposicional**, ou seja, um conjunto de proposições, munido dos operadores "**e**", "**ou**", "**não**", "**implicação**", "**equivalência**", e mais os elementos distinguidos da álgebra "**true**" e "**false**".

Nesta álgebra, aparecem as leis de **De Morgan**, completando a **álgebra proposicional**. A Álgebra de Boole é uma álgebra abstrata, e sua estrutura algébrica captam as propriedades essenciais dos operadores lógicos e de conjuntos, ou ainda oferece um estrutura para se lidar com "afirmações" Scheinerman (2003).

Formalmente, uma Álgebra Booleana é uma 6-*upla* $(L, \wedge, \vee, \neq, \mathbf{false}, \mathbf{true})$consistindo de um conjunto munido de duas operações binárias (também denotado por $\vee$ (ge-

ralmente chamado de "ou"), $\wedge$ (geralmente chamado de "e"), uma operação unária (também denotada por $\neq$ (também geralmente chamado de "não"), e duas constantes (também denotada por "**false**", geralmente chamado de "zero" ou de "falso") e outra constante (também denotada por "**true**" (geralmente chamado de "um" ou de "verdadeiro"), e satisfazendo as seguintes **propriedades**, para quaisquer p, q e r pertencentes a L: (a) Associativas, (b) Comutativas, (c) Absortivas, (d) Distributivas, (e) Elementos Neutros.

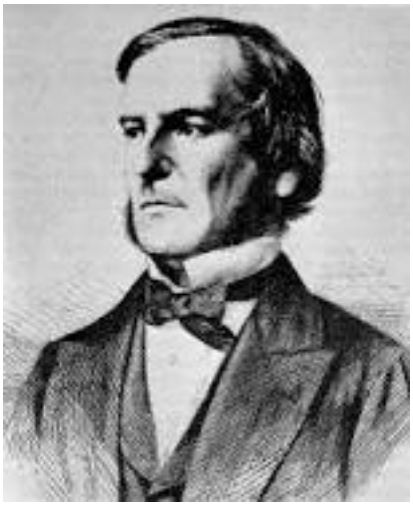


Figura 58 – George Boole: a transformação da lógica em álgebra.

Fonte: livrespensadores.net.

Na matemática e na ciência da computação, as álgebras booleanas são estruturas algébricas que "capturam a essência" das operações lógicas E, OU e NÃO, bem como das operações da teoria de conjuntos como união, produto cartesiano e complemento de um conjunto. Ela também é o fundamento da matemática computacional, que associa as constantes true e false aos números binários 0 e 1, respectivamente. A álgebra booleana acabou por ter sua aplicação na eletrônica. Foram pela primeira vez aplicadas, alguns anos depois, aos interruptores (relés) e depois transformados em bits, no século XX, por **Claude Shannon**.

Os operadores da Álgebra Booleana podem ser representados de várias formas. É frequente serem simplesmente escritos como E, OU ou NÃO (são mais comuns os seus equivalentes em inglês: AND, OR e NOT). Na descrição de circuitos também podem ser utilizados NAND (NOT AND), NOR (NOT OR) e XOR (OR exclusivo). Os matemáticos usam com frequência + para OU e . para E (visto que sob alguns aspectos estas operações são análogas à adição e multiplicação noutras estruturas algébricas) e representam NÃO com uma linha traçada sobre a expressão que está a ser negada. Aqui podemos usar outra notação comum, com $\wedge$ para E, $\vee$ para OU, e $\neg$ para o operador NÃO.

O *calculus raciocinator* de que **Boole** transformou em uma álgebra, formou, mais

tarde, no século XX, a base para a construção dos circuitos lógicos criados por **Shannon**, na segunda metada da década de 40, e que hoje formam a lógica dos circuitos eletrônicos do computador dos dias de hoje.

7.6 Bibliografia e Fonte de Consulta

Leibniz - http://amatematicaalema.blogspot.com.br/2011/02/leibniz-o-precursor-da-logica.html

George Boole - https://pt.wikipedia.org/wiki/George_Boole

De Morgan - https://pt.wikipedia.org/wiki/Augustus_De_Morgan

Edgar de Alencar Filho - Introdução à Lógica Matemática, Nobel, 2002.

Marco A. Casanova et. al. - Programação em Lógica, V Escola de Computação, SBC, 1986.

Zahar Manna e Richard Waldinger - The Logic Basis for Computer Programming, Addison-Wesley, 1985.

7.7 Referências e Leitura Recomendada

Leibniz - ⟨http://www.di.ufpb.br/raimundo/Revolucao_dos_Computadores/Histpage17.htm⟩

Enderton, Herbert. A mathematical introduction to logic. Second ed. Boston, MA: Academic Press, 1972, 2001. ISBN 978-0-12-238452-3.

Kleene, Stephan C. - Introduction to Metamathematics, Horth-Holland Publishing Company, Amsterdan.

Shoenfield, J. R. - Mathematical Logic, Addison-Wesley Publishing Company, Reading, Massachusetts, 1967.

CAPÍTULO 8

Século XIX - Frege e o Cálculo dos Predicados

Apresenta-se neste capítulo, as lógicas surgidas no século XIX, a partir de **Frege**, aplicadas à Ciência da Computação. A lógica, como ciência, tem por objeto o estudo dos métodos e princípios que permitem distinguir raciocínios válidos de outros não válidos.

8.1 O Cálculo de Frege

Ao contrário de **Aristóteles**, e mesmo de **George Boole**, que procuravam identificar as formas válidas de argumento (eles pensavam na **línguagem** da lógica), a preocupação básica de **Friedrich Ludwig Gottlob Frege** (1848-1925) era a sistematização do raciocínio matemático, ou dito de outra maneira, encontrar uma caracterização precisa do que deveria ser uma "demonstração matemática". O que **Frege** pensava era num **cálculo**, um sistema dedutivo, ao invés da linguagem da Lógica, por onde se pudesse fazer provas. Na Lógica Proposicional apresentada no capitulo anterior, ela foi iniciada por **Leibniz** através de fragmentos pensado visando uma linguagem o mais abrangente possivel que falasse de tudo.

George Boole contribuiu para transformar essa lógica numa álgebra, mas o método dedutivo desta Lógica Proposicional que temos hoje, deve-se a **Emil Post**. A partir das várias propridades algébricas mostradas no capitulo anterior, chegou-se ao Método Dedutivo constituido de várias regras de inferência construídas a partir da definição do que vem a ser um *argumento*, a *validade de um argumento* e os *critérios de avaliar a validade de um argumento* e os *argumentos válidos fundamentais*. Esses argumentos básicos são usados para fazer inferência, os passos de uma dedução ou demonstração. Com este Método Dedutivo temos o cálculo proposicional.

Frege havia notado que os matemáticos da época freqüentemente cometiam erros em suas demonstrações, supondo assim que certos teoremas estavam demonstrados,

quando na verdade não estavam. Para corrigir isso, **Frege** procurou formalizar as regras de demonstração, iniciando com regras elementares, bem simples, sobre cuja aplicação não houvesse dúvidas (os axiomas).

Figura 59 – O nascimento da lógica moderna e o cálculo dos predicados.

Fonte: https://pt.wikipedia.org/wiki/Gottlob_Frege.

O resultado que revolucionou a Lógica, foi a criação do **Cálculo de Predicados**, um sistema de representação simbólica (por volta de 1879) para representar formalmente a estrutura dos enunciados lógicos e suas relações, e a contribuição para a invenção da Lógica de Predicados Axiomática (o conhecido **Cálculo dos Predicados**).

8.2 A Lógica e o Cálculo dos Predicados

No estudo estudo sobre a Lógica Proposicional, nós temos determinado que uma sentença tal como:

Os macacos em Jupiter são vermelhos **ou** Os macacos em Jupiter não são vermelhos.

é verdadeira sem a necessidade de uma investigação na biologia de Jupiter. A sentença é uma instância da sentença válida da Lógica Proposicional P or (not P), tomado-se P ser a proposição "Os macacos em Jupiter são vermelhos".

Entretanto, existem sentenças que nós podemos dizer que é verdadeira pela sua forma, mas que não são instâncias de nehuma sentença válida na Lógica Proposicional. Por exemplo:

Existem pedras vermelhas em Jupiter **ou Todas** as pedras em Jupiter não são vermelhas.

Existe um número perfeito ímpar **ou Todos** os números perfeitos não são ímpares.

são verdaeiras sem termos que lançar uma aeronave espacial ou mesmo sabermos a definição de um número perfeito.

A linguagem da Lógica Proposicional é grosseira e primitiva para poder expressar o conceito de um objeto, uma propriedade de um objeto (tal como sendo uma pedra ou um número perfeito), ou a relação entre diversos objetos de um Universo de Discurso.

A linguagem da Lógica dos Predicados estende a linguagem da Logica Porposicional por habilitarmos a falar sobre objetos e o relacionamento entre eles. Agora, as sentenças acima podem, ambas, ser consideradas como instâncias da sentença abstrata $\mathcal{F}$ (que não é da Lógica Proposicional), tal que:

$\mathcal{F}$: (**para algum** x)[p(x) **e** q(x)] **ou** (**para todo** x)[se p(x) então **não** q(x)]

Para a sentença das "pedras", tomamos p(x) ser "x é uma pedra sobre Jupiter" e q(x) ser "x é vermelha". Sob esta interpretação, o significado intuitivo da sentença $\mathcal{F}$ torna-se:

$\mathcal{F}$: (**para algum** x)[x é uma pedra sobre Jupiter **e** x é vermelha] **ou** (**para todo** x)[se x é uma pedra sobre Jupiter então **não** x é vermelha]

Para a sentença dos "números", tomamos p(x) ser "x é um número perfeito" e q(x) ser "x é ímpar". Sob esta interpretação, o significado intuitivo da sentença $\mathcal{F}$ torna-se:

$\mathcal{F}$: (**para algum** x)[x é um número perfeito **e** x é ímpar] **ou** (**para todo** x)[se x é um número perfeito então **não** x é ímpar]

Ambas as sentenças são interpretadas como verdadeiras. De fato, **qualquer instância da sentença abstrata $\mathcal{F}$, é verdadeira sem considerarmos o significado atribuido a p(x) e q(x)**.

Por outro lado, nem toda instância da sentença abstrata $\mathcal{G}$, tal que:

$\mathcal{G}$: (**para todo** x)[p(x)] **ou** (**para todo** x)[não p(x)]

é verdadeira. Por exemplo, se tomarmos p(x) ser "x é um macaco Rhesus", o significado intuitivo da sentença $\mathcal{G}$ torna-se:

$\mathcal{G}$: (**para todo** x)[x é um macaco Rhesus **ou** (**para todo** x)[**não** (x é um macaco Rhesus)].

Isto é: "**Todos** os macacos são Rhesus" **ou** "**todos** os macacos **não** são Rhesus".

Visto que não verdade que todos sejam macacos Rhesus, mas também não é verdade que todos sejam macacos Rhesus (de fato, existe algum macaco Rhesus), a sentença inteira é contraditória e portanto é falsa. Note que na sentença abstrata $\mathcal{G}$, a existência do elemento variável x, muda completamente, em relação a sentença abstrata da mesma forma como na Lógica Proposicional. A introdução de uma variável ou de variáveis, numa sentença abstrata desta Lógica, traz o conceito de lógica de primeira ordem, pois agora, quantifica-se (existe, para todo) variáveis nesta Lógica.

8.2.1 Verdades absolutas × Verdades Relativas

Ao contrário da Lógica Proposicional de **Leibniz**, **Boole**, **De Morgan**, que lida com **verdades absolutas**, sem poder expressar variáveis, no **Cálculo dos Predicados** lidamos com **verdades relativas**, podendo-se expressar variáveis através da distinção da afirmação (um predicado) de seus argumentos. Entende-se que a afirmação pode ser verdadeira ou falsa, de acordo com os valores atribuidos às variáveis as quais a afirmação é aplicada, dentro do universo de discurso da Lógica dos Predicados.

A **Lógica de Predicados** é uma lógica simbólica de sistema formal como lógica de primeira ordem. Na lógica de primeira ordem, dois quantificadores comuns são: os quantificadores existencial $\exists$ ("existe um") e universal $\forall$ ("para todo"). As variáveis poderiam ser elementos no domínio do discurso, ou talvez as relações ou funções durante este universo. No uso informal, o termo "lógica de predicados" ocasionalmente se refere a lógica de primeira ordem. Alguns autores consideram que o cálculo de predicados seja a forma axiomática da lógica de predicados (seu sistema dedutivo), e a lógica de predicados é a liguagem deste cálculo, com sua sintaxe e sua semântica para as expressões válidas logicamente Manna (1985), Hamilton (1978) Stolyar (1970). O Cálculo dos Predicados, por ser *consistente* (tudo que é provado é verdadeiro) e *completo* (tudo que é verdadeiro pode ser provado), tem sido muito relevante para a ciência da computação. Várias ferramentas de prova automática de teoremas (lógica computacional) existem no sentido de provar a correção da especificação ou implementação de programas de computador.

No **Cálculo dos Predicados** lidamos com verdades relativas ou variáveis, através da distinção da afirmação (um predicado) de seus argumentos. Entende-se que a afirmação pode ser verdadeira ou falsa, de acordo com os valores atribuidos às variáveis as quais a afirmação é aplicada, dentro do universo de discurso da Lógica dos Predicados. Neste caso, *predicados*indexpredicados são proposições (também chamadas sentenças).

8.2.2 Fatos Históricos sobre a Linguagem de Primeira Ordem

A Lógica de Primeira Ordem originou-se no "*Begriffsschrift*" publicado por **Frege** em 1879. Posteriormente, por volta de 1930, três matemáticos **Godel**, **Herbrand**

e **Skolem** obtiveram resutados importantes sobre o problema de caracterizar adequadamente os princípios lógicos de primeira ordem, partindo de resultados de *Löwewnhein* e de **Skolem**, anteriores a 1920, **Gödel** em sua tese de doutorado "*Über die Vollständigkeit des Logikkalküls*", defendida em 06 de Fevereiro de 1930 (Hilbert era o orientador), provou a existência de um **sistema axiomático consistente e completo** para a Lógica de Primeira Ordem. **Herbrand**, também na sua tese de doutorado "*Recherches sur la Théorie de la Démonstration*", completada em abril de 1929 e defendida em 11 de junho de 1930, obteve uma solução para o *problema da caracterização dos princípios lógicos* de primeira ordem que se tornou fundamental para a mecanização da Lógica de Primeira Ordem (ver em Casanova, Giorno e Casanova (1986)). Estes princípios é que tornaram possivel a implentação da Lógica de Primeira Ordem com na linguagem de programação Prolog Casanova, Giorno e Casanova (1986). Finalmente, **Skolem**, em uma série de trabalhos publicados em torno de 1930, ofereceu uma outra soulução para o problema da caracterização de certa forma semelhante aos resultados de **Herbrand**.

Um segundo grupo de resultados importantes refere-se aos chamados *problemas de decisão* para a Lógica de Primeira Ordem. Por exemplo, o *problema da validade* consiste em determinar se existe, ou não, um algoritmo que recebe como entrada qualquer fórmula de primeira ordem, e produz como saída um "*sim*", se a fórmula e sempre válida, e um "*não*" em caso contrário. **Church** em "*An Unsolvable Problem with Elementary Number Theory*" (1936), e independentemente **Turing**, no trabalho "*On Computable Numbers with an Application to the Entscheidungsproblem*" (1936), provaram que tal algoritmo não pode existir, estabelecendo assim, a indecidibildade do problema da validade. Este resultado teve inúmeras ramificações imediatas para outros problemas de decisão em primeira ordem, que são abordados no Cap.2 em Casanova, Giorno e Casanova (1986). No contexto da programação em Lógica como está em Casanova, Giorno e Casanova (1986), este resultado é evidentemente muito importante porque impóe uma limitação séria no que se poderia atingir em Programação em Lógica de Primeira Ordem.

Mas, um benefício trazido pela Lógica de Primeira Ordem foi, em virtude de ser provada consistente e completa, serve muito bem à construção de Teorias de Primeira Ordem. Exemplos desta teorias são dados no último capítulo sobre Os Sistemas Formais da Computação em **??**.

A Lógica de Primeira Ordem como será descrita aqui é um sistema formal apropriado à definição de teorias do universo de discurso da Matemática.

8.2.3 A Linguagem de Primeira Ordem

Definição (Um Alfabeto $\mathcal{A}$)

- Símbolos Lógicos:
  - Pontuação: (,)

  - Conectivos: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
  - Quantificadores: $\exists$ (existencial), $\forall$ (universal)
  - Variáveis: um conjunto nãp-vazio, enumerável de símbolos distintos dos demais
  - Igualdade: $=$ (opcional)

- Símbolos Não-Lógicos
  - Um conjunto, possivelmente vazio, de constantes.
  - Para cada $n > 0$, um conjunto, possivelmente vazio, de símbolos funcionais n-ários, distintos dos demais.
  - Para cada $n > 0$ um conjunto, possivelmente vazio, de símbolos predicativos n-ários, distintos dos demais.

Definição (**Termos**)

Um conjunto de termos de primeira ordem sobre o alfabeto $\mathcal{A}$, é o menor conjunto satisfazendo as seguintes condições:

- Toda variável em $\mathcal{A}$ é um termo.
- Toda constante em $\mathcal{A}$ é um termo.
- Se $t_1, t_2, \ldots, t_n$ são termos e f e um símbolo funcional n-ário de $\mathcal{A}$, então, $f(t_1, t_2, \ldots, t_n)$ também é um termo sobre $\mathcal{A}$.
- Se $\mathcal{F}$ é uma sentença (constituída de proposições) e s e t são termos, então a condicional **se** $\mathcal{F}$ **então** s **else** t é um termo.

Definição (**Proposições**)

Intuitivamente, as constantes e variáveis denotam objetos no universo de discurso As proposições da Lógica de Primeira Ordem são voltados para representar relações entre objetos do universo do discurso. Proposições são cosntruídas de acordo com as seguintes regras:

- Os símbolos *true* (*verdade*) e *false* (*falso*) são proposições.
- Se $t_1, t_2, \ldots, t_n$ são termos, onde $n \geq 1$ e p e um símbolo predicativo n-ário de $\mathcal{A}$, então, $p(t_1, t_2, \ldots, t_n)$ é uma proposição.

Definição (**Sentenças - Fórmulas Bem-Formadas**)

O conjunto de fórmulas sobre $\mathcal{A}$ é o menor conjunto satisfazendo as seguintes considerações:

- Se $t_1, t_2, \ldots, t_n$ são termos e p um símbolo predicativo n=ário, então $p(t_1, t_2, \ldots, t_n)$ é uma fórmula sobre o alfabeto $\mathcal{A}$.
- Se t_1 e t_2 são termos e "=" é um símbolo de $\mathcal{A}$, então $(t_1 = t_2)$ é uma fórmula sobre $\mathcal{A}$.
- Se P e Q são fórmulas (proposições) sobre $\mathcal{A}$, então $\neg P$, $(P \wedge Q)$, $(P \vee Q)$, $(P \rightarrow Q)$ e $(P \leftrightarrow Q)$, também são fórmulas (sentenças) sobre $\mathcal{A}$.
- Se P é uma fórmula sobre $\mathcal{A}$ e x é uma variável de $\mathcal{A}$, então $\forall\, x(P)$ e $\exists\, x(P)$ também são fórmulas sobre $\mathcal{A}$.

Fórmulas bem-formadas são as **sentenças** da Lógica de Primeira Ordem. Da mesma forma que na Lógica Proposicional, **sentenças são formadas por proprosições**. E as **proposições** são as chamadas fórmulas-atômicas (indivisíveis).

Pelas regras de formação das fórmulas, as variáveis podem ocorrer em uma fórmula, associadas a um quantificador ou não. Esta observação origina uma série de definições auxiliares como seguem:

8.2.4 O Significado de uma Sentença

Em definir validade para Lógica Proposicional, nós primeiro definimos a noção de veracidade/falsidade de uma sentença sob uma interpretação, que atribui valores **true** ou **false** (valores-semânticos) aos símbolos proposicionais da sentença. Agora, nó estendemos esta noção para a Lógica dos Predicados de forma análoga. Como as *sentenças* envolvem *termos*, uma *interpretação* deve incluir um *domínio*, **um conjunto de objetos que provê um significado para os termos**. A noção precisa de uma interpretação será agora definida. Uma **interpretação para uma sentença deve atribuir um significado a cada um dos simbolos livres da sentença**. Atribuiremos valores do domínio para constantes e as variáveis livres, funções (sobre o dominio) aos símbolos funcionais e relações (sobre o domínio) aos símbolos predicativos. A associação de um valor para a *expressão* é determinado a partir dos valores de seus componentes, por aplicar as *regras semânticas* definidas para a Lógica dos Predicados. O leitor pode estudar estes detalhes em Manna (1985).

8.2.5 Modelos e Consequência Lógica

Usamos aqui a definição dada em Loeckx e Sieber (1987).

Seja W um conjunto de fórmulas, tal que $W \subseteq WFF_B$, onde WFF_B é o conjunto de fórmulas bem-formadas da Lógica dos Predicados de base B. $B = (F, P)$, onde F é conjunto de símbolos funcionais e P é o conjunto de símbolos predicativos da Lógica dos Predicados. Uma interpretação $\phi = (D, I)$ é chamada um *modelo* de W, se toda fórmula $w \in W$ é *válida* ($\models_\phi w$) sob essa interpretação ϕ. Uma fórmula $w \in WFF_B$ é chamada uma consequência lógica de W - denotado por $W \models_\phi w$, se

w é válida ($\models_\phi w$) para todo modelo ϕ de W.

O método usual de demonstração de uma não-contradição, consiste em contruir um *modelo*, como definido acima, ou seja oferecer uma *interpretação* semântica, para o sistema considerado. Porque se uma *teoria* admite um *modelo*, então ela é não-contraditória. **Gödel** provou a recíproca desta propriedade: "todo sistema axiomático de primeira ordem, não contraditório, possui um *modelo*".

8.3 Caracterizando as Lógicas Clássicas, Hoje

Hoje, a Lógica é o estudo filosófico do *raciocínio válido*. Utilizada em atividades mais intelectuais, a lógica é usada principalmente nas disciplinas de filosofia, matemática e na área da **ciência da computação**. Ela examina de forma genérica as formas que a argumentação pode tomar, quais dessas formas são **válidas** e quais são **não-válidas** (falaciosas). Na matemática, estuda-se as formas válidas de inferência através de uma linguagem formal. Na computação, ajudou a construir os computadores digitais que temos hoje, como mostrado no Capítulo 8 do Volume 2 da presente série.

Esta parte da decomposição funcional da estrutura interna das frases (substituindo a dicotomia sujeito-predicado, herdada da tradição lógica aristotélica, pela oposição matemática função-argumento) e da introdução do conceito de quantificação (implícito na lógica clássica), tornando assim possível a sua manipulação em regras de dedução formal. Os enunciados "*para todo x* - $\forall x$", "*existe x* - $\exists x$"que denotam operações de quantificação sobre variáveis, têm a sua origem no seu trabalho, como o exemplo: "Todos os humanos são mortais"se torna "Todos os X são tais que, se x é um humano então x é mortal".

Mas, a lógica simbólica, surgido com **Leibniz** no século XVII, foi negligenciada por muitos anos depois de sua invenção. Entretanto, com o trabalho pioneiro de **George Boole**, sua grande criação tem sido melhorada. Até 1910 ainda existiam eminentes matemáticos desdenhando-a sob a curiosidade filosófica, sem qualquer significância matemática. O trabalho de **Whitehead** e **Russel** em *Principia Mathematica* (1910-1913) foi o primeiro a convencer um grupo de matemáticos que a lógica simbólica devia receber uma séria atenção.

A *Lógica Simbólica* é uma ferramenta matemática para o estudo dos métodos, estruturas e validade das deduções e provas matemáticas. Entretanto, a dificuldade desta abordagem ficou clara quando **Bertrand Arthur William Russell** (1872-1970) e **Alfred North Whitehead** (1861-1947) publicaram seu trabalho monumental denominado *Principia Mathematica*, o livro em três volumes, publicados entre 1910 e 1913, onde dezenas de páginas e símbolos foram necessários somente para provar que $1 + 1 = 2$. **Russell**, foi um dos mais influentes matemáticos, filósofos e lógicos que viveram no século XX.

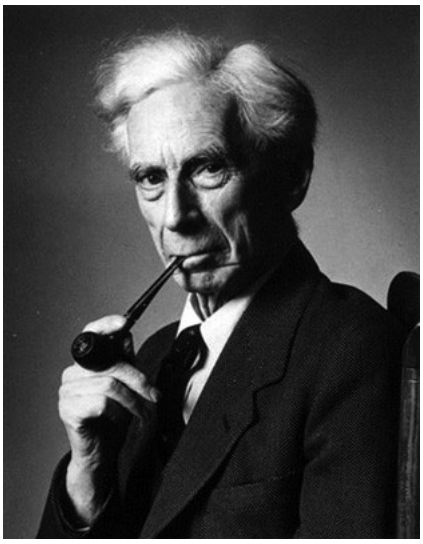


Figura 60 – Russell - matemático, filósofo e lógico do século XX.

Fonte: openlibrary.org.

8.3.1 Lógica dos Predicados e a Inteligência Artificial

A Lógica dos Predicados é uma lógica bem apropriada para a área da Inteligência Artificial (IA), a inteligência vista de forma similar à humana, exibida por software, como desenvolvida por **John McCarthy** (1927-2012), um cientista da computação estadunidense, conhecido pelos estudos no campo da IA, e por ser o criador da primeira linguagem de programação funcional, chamada LISP (List Processing), recebeu o Prêmio Turing de 1972 e a Medalha Nacional de Ciências dos Estados Unidos de 1991 McCarthy (1963a).

Figura 61 – John McCarthy - O Cálculo dos Predicados e a IA.

Fonte: Google Images - www.independent.co.uk.

Além, das Lógicas Proposicional e de Predicados, existem as Lógicas Temporais descorrentes destas, que podem ser aplicadas para especificar e verificar propriedades de sistemas de computação, mas especificamente, os sistemas concorrentes ou distribuídos.

8.3.2 Ferramentas atuais em Lógica de Primeira Ordem

Existem algumas ferramentas baseadas em lógica de primeira ordem, para se provar a correção de **protocolos criptográficos**:

- *Timed Cryptographic Protocol Logic* Kramer (2006) (http://eprint.iacr.org/).
- Um outro provador de teoremas é AVISPA - *Automated Validation of Internet Security Protocols and Applications* (http://www.avispa-project.org/).
- Uma outra ferramenta é a que está em Han Zhiyong Zhou (2009).
- Outra lógica é a que é apresentada em *Time-Dependent Cryptographic Protocol Logic and Its Formal Semantics*Lei Jun Liu (2011), onde uma lógica modal predicativa é proposta.
- SPASS - *An Automated Theorem Prover for First-Order Logic with Equality* (http://www.spass-prover.org/)
- PROVERIF - *Cryptographic protocol verifier in the formal model* (http://prosecco.gforge.inria.fr/personal/bblanche/proverif/)

8.4 Ordens nas Lógicas Clássicas

Aqui cabe a explicação do que vem a ser a *ordem* sobre uma lógica clássica.

- **Lógica Proposicional de ordem 0**: Também conhecida por Lógica Sentencial, é a lógica mais básica, que descreve apenas **verdades-absolutas**.
- **Lógica de Primeira Ordem**: é uma extensão de lógica proposicional, onde se pode expressar **verdades-relativas**, onde se pode quantificar variáveis através dos quantificadores $\exists$ (existe) e $\forall$ (para todo). Usa a idéia de universo de discurso ou domínio de discurso (normalmente chamado apenas de "domínio"). O domínio é um conjunto sobre os quais se pode quantificar. A lógica de primeira ordem inclui apenas **variáveis e quantificadores sobre elementos individuais do domínio**. Por exemplo, na sentença de primeira ordem $(\forall\, x \mid x \neq x + 1)$, a variável x é usada para representar um indivíduo arbitrário, no domínio da lógica de primeira ordem.

- **Lógica de Segunda Ordem**: na lógica matemática, a lógica de segunda ordem é uma extensão da lógica de primeira ordem, pela adição de variáveis e quantificadores sobre **conjuntos** de indivíduos. Por exemplo a sentença $(\forall S \wedge \forall x)(x \in S \vee x \notin S)$ diz que, para todo o grupo S de indivíduos e todo indivíduo x, ou x pertence a S, ou x não pertence a S (este é o princípio da bivalência). Uma sentença na lógica de segunda ordem, assim como na lógica de primeira ordem, é uma fórmula bem formada sem variáveis livres (de nenhum tipo).

- **Lógica de Alta-Ordem** (High Order Logic): na matemática e na lógica, uma lógica de ordem superior é uma forma de lógica de predicados que se distingue da lógica de primeira ordem por permitir a presença de quantificadores sobre predicados e funções. Por exemplo, numa lógica de alta-ordem, um quantificador existencial sobre um símbolo de função poderia ser interpretado como um modificador "Existe uma função f". Este sistema formal se distingue em que suas fórmulas contém variáveis que podem ser quantificadas, e por possuir uma semântica mais forte. Lógicas desse tipo, com sua semântica padrão, são mais expressivas, que a de primeira ordem.

8.4.1 Lógica de Segunda Ordem

Da lógica de segunda ordem e seus resultados metalógicos: suas propriedades na *teoria dos modelos* são "menos bem-comportadas"do que as da lógica de primeira ordem em relação a certas aplicações.

Segue como corolário do **Teorema da Incompletude de Gödel**, que não há sistema dedutivo (isto é, não há uma "demonstrabilidade") para fórmulas de segunda ordem que satisfaça simultaneamente esses três atributos desejados:4

(**Correção**) Toda sentença demonstrável de segunda ordem é universalmente válida, isto é, verdadeira em todos domínios sob a semântica padrão.

(**Completude**) Toda fórmula de segunda ordem universalmente válida, sob a semântica padrão, é demonstrável.

(**Efetividade**) Existe um algoritmo que possa verificar e decidir corretamente se uma dada sequência de símbolos é uma demonstração válida ou não.

Este corolário é expresso dizendo-se que a lógica de segunda ordem não admite uma teoria de demonstração completa. Neste aspecto a lógica de segunda ordem com semânticas padrão difere da lógica de primeira ordem, e esta é uma das razões pelas quais os lógicos muitas vezes evitam usar lógica de segunda ordem.

Como foi mencionado acima, **Henkin** demonstrou que o sistema dedutivo padrão para o lógica de primeira ordem é correto, completo, e efetivo para a lógica de

segunda ordem com semântica de **Henkin**, e o sistema dedutivo com princípios de compreensão e de escolha são corretos, completos e efetivos para as semânticas de **Henkin** que usa apenas **modelos** que satisfazem esses princípios.

8.4.2 Lógica de Alta Ordem

Lógica de **primeira ordem** quantifica apenas as variáveis (∃, ∀); lógica de segunda ordem, além disso, também quantifica sobre conjuntos; lógica de terceira ordem também quantifica sobre conjuntos de conjuntos, e assim por diante.

Por exemplo, a frase $\forall\, P$, de segunda ordem, tal que:

$$(0 \in P \wedge \forall\, i.I \in P \rightarrow i + 1 \in P) \rightarrow (\forall\, n.N \in P)$$

expressa o princípio da indução matemática.

Em matemática e lógica, uma **lógica de ordem superior** é uma forma de lógica de predicados que se distingue da lógica de primeira ordem pela aplicação de quantificadores adicionais e uma semântica mais rigorosa. Lógicas de ordem superior tem semântica mais expressiva, mas suas propriedades modelo-teórico (da Teoria dos Modelos, que estuda estruturas matemáticas, do ponto de vista da lógica, na qual ("algebra universal + logic = teoria dos modelos") são menos bem-comportadas do que os de lógica de primeira ordem.

Lógica de ordem superior é a união de primeira, segunda, terceira ... ordem lógica; ou seja, ele admite quantificação sobre conjuntos arbitrariamente profundamente aninhados.

Aplicando esta lógica, existe o sistema provador de teoremas, denominado *Isabelle* Nipkow Lawrence C. Paulson (2014), utilizado para provar hardware e software, e que na área de segurança computacional pode provar a correção de protocolos criptográficos.

Atualmente há duas semânticas possíveis para HOL. Na semântica padrão ou completa, quantificados e objetos do tipo superior variam sobre todos os objetos possíveis tipo. Por exemplo, um quantificador sobre um conjunto de indivíduos varia ao longo de todo o conjunto das partes do conjunto de indivíduos. Assim, na semântica padrão, uma vez que o conjunto de indivíduos é especificado, temos o suficiente para indicar todos os quantificadores.

HOL com semântica padrão é mais expressiva do que a lógica de primeira ordem por, exemplo, admitir axiomatizações categóricas dos números naturais e dos números reais, que são possíveis com a lógica de primeira ordem. No entanto, sabemos através dos resultados de Gödel, que HOL com semântica padrão não admite um

efetivo e completo cálculo como prova eficaz.

8.5 Lógica Dedutiva e Indutiva

A lógica diferencia duas classes fundamentais de argumentos: os *dedutivos* e os *indutivos*. Os *argumentos dedutivos* são aqueles em que as premissas fornecem um fundamento definitivo da conclusão, enquanto nos indutivos as premissas proporcionam somente alguma fundamentação da conclusão, mas não uma fundamentação conclusiva.

Um *raciocínio indutivo* é um tipo de raciocínio que partindo de premissas particulares obtém uma conclusão universal. Uma outra maneira de expressar essa diferença é dizer que numa dedução é impossível que as premissas sejam verdadeiras e a conclusão falsa, mas no raciocínio indutivo no sentido forte isso é possível, embora seja pouco provável. Num raciocínio dedutivo a informação da conclusão já está contida nas premissas, de modo que se toda a informação das premissas é verdadeira, a informação da conclusão também deverá ser verdadeira. No raciocínio indutivo a conclusão contém alguma informação que não está contida nas premissas, ficando em aberto a possibilidade de que essa informação a mais cause a falsidade da conclusão apesar das premissas verdadeiras Copi Cohen (1990).

8.6 Bibliografia e Fonte de Consulta

Zohar Manna e Richard Waldinger - The Logical Basis for Computer Programming, Volume I: Deductive Reasoning, Addison Wesley, 1985.

Zohar Manna e Richard Waldinger - The Logical Basis for Computer Programming, Volume II: Deductive Systems, Addison Wesley, 1990.

Lógica de Ordem Superior - https://pt.wikipedia.org/wiki/Lógica_de_orden_superior

Programação em Lógica - Marco A. Casanova, Fernando A. C. Giorno, Antonio L. Furtado, V Escola de Computação, Belo Horizonte, 1986.

Lógica Indutiva e Probabilidades - Newton da Costa, Ed. Hucitec, 2008.

Introdução à Lógica Matematica - Edgar de Alencar Filho, 2002.

Fitting, Melvin (2002). Types, Tableaus, and Gödel's God. Springer Science & Business Media. p. 139. ISBN 978-1-4020-0604-3. Godel's argument is modal and at least second-order, since in his definition of God there is an explicit quantification over properties. [...] [AG96] showed that one could view a part of the argument not as second-order, but as third-order.

Encyclopedia of Artificial Intelligence: Second Edition, “Logic, Higher-order”, by Dale Miller, February 1991.

HEIJENOORT, Jean van. From Frege to Gödel: a source book in mathematical logic, 1879?1931 (em inglês). Cambridge, Massachusetts: Harvard University Press, 1967.

MORTARI, Cezar A. Introdução à Lógica. São Paulo: Editora UNESP, 2001.

8.7 Referências - Leitura Recomendada

Zohar Manna - The Mathematical Theory of Computation, McGraw Hill, 1974, reimpressão Dover, 2003.

Manna & Pnueli - The Temporal Logic of Reactive and Concurrent Systems: Specification, (Springer-Verlag, 1991).

Manna & Pnueli - The Temporal Logic of Reactive and Concurrent Systems: Safety, (Springer-Verlag, 1995).

Manna & Pnueli - The Temporal Logic of Reactive and Concurrent Systems: Progress, (não publicado; os três primeiros capítulos estão disponíveis em Manna/Pnueli: The Temporal Verification of Reactive Systems: Progress).

Grupo de Sistemas Inteligentes, *Lógica Borrosa y Aplicaciones. Aplicación en Robótica*, ⟨http://www.puntolog.com/actual/articulos/uni_santiago6.htm⟩, Universidad de Santiago de Compostela.

Jean Yves Béziau, Walter Carnielli e Dov Gabbay, eds.. *Handbook of Paraconsistency*. London: King’s College, 2007. ISBN 978-1-904987-73-4

Priest, Graham e Tanaka, Koji (1996, 2009). *Paraconsistent Logic Stanford Encyclopedia of Philosophy*. Visitado em June 17, 2010. (First published Tue Sep 24, 1996; substantive revision Fri Mar 20, 2009)

Oliveira, Wilnice, T. R., *Utilizando Integrais Fuzzy em Tomada de Decisão Multicritérios*, dissertação de mestrado, PPGCC-UFSC, 2003.

Logic for philosophy, Theodore Sider

John P. Burgess. Philosophical logic. [S.l.]: Princeton University Press, 2009. vii-viii p. ISBN 978-0-691-13789-6

Susan Haack. Deviant logic: some philosophical issues. [S.l.]: CUP Archive, 1974. p. 4. ISBN 978-0-521-20500-9

Susan Haack. Philosophy of logics. [S.l.]: Cambridge University Press, 1978. 204 p. ISBN 978-0-521-29329-7

L. T. F. Gamut. Logic, language, and meaning, Volume 1: Introduction to Logic. [S.l.]: University of Chicago Press, 1991. 156-157 p. ISBN 978-0-226-28085-1

Seiki Akama. Logic, language, and computation. [S.l.]: Springer, 1997. p. 3. ISBN 978-0-7923-4376-9

Robert Hanna. Rationality and logic. [S.l.]: MIT Press, 2006. 40-41 p. ISBN 978-0-262-08349-2

John P. Burgess. Philosophical logic. [S.l.]: Princeton University Press, 2009. 1-2 p. ISBN 978-0-691-13789-6 Interpolation and definability: modal and intuitionistic logics. [S.l.]: Clarendon Press, 2005. p. 61. ISBN 978-0-19-851174-8

D. Pigozzi. In: M. Hazewinkel. Encyclopaedia of mathematics: Supplement. Volume III. [S.l.]: Springer, 2001. p. 2-13. ISBN 1-4020-0198-3.

Hazewinkel, Michiel, ed. (2001), "Abstract algebraic logic", Encyclopedia of Mathematics, Springer, ISBN 978-1-55608-010-4.

Stewart Shapiro, 2001, "Classical Logic II: Higher Order Logic,"in Lou Goble, ed., The Blackwell Guide to Philosophical Logic. Blackwell, ISBN 0-631-20693-0

Benzmuller, Christoph; Miller, Dale (2014). "Automation of Higher-Order Logic". In Gabbay, Dov M.; Siekmann, Jörg H.; Woods, John. Handbook of the History of Logic, Volume 9: Computational Logic. Elsevier. ISBN 978-0-08-093067-1.

ALCOFORADO, P.; DUARTE, A.; WYLLIE, G. Os Primeiros Escritos Lógicos de Gottlob Frege. São Paulo: IBFC Ramon Llull, 2012.

COSTA JÚNIOR, Fernando V. Minicurso de Lógica Matemática: Uma introdução à Lógica Matemática e uma aplicação do método da Dedução Natural a sistemas axiomáticos formais. Disponível em: ¡https://logicaematematica.wordpress.com/2014/02/04/minicurso-de-logica-matematica/¿. Acesso em: 04 Fev. 2014.

CAPÍTULO 9

Teoria dos Conjuntos

A primeira teoria matemática que tratou de conjuntos foi desenvolvida por **Cantor** - **Georg Ferdinand Ludwig Philipp Cantor** (1845-1918). A partir do final do século XIX a *teoria dos onjuntos* tornou-se uma poderosa ferramenta matemática para aplicações em muitos campos da matemática, mas sobretudo, aqui será usada como base para os capitulos seguintes, que focalizam a origem matemática da ciência da computação. O matemático **Georg Cantor** começou as suas pesquisas estudando séries trigonométricas, mas logo foi direcionado por elas a elucidar o *conceito de conjunto*. Dessa maneira ele deu origem à teoria de conjuntos, desenvolvendo a primeira teoria matemática dos números infinitos. *Conjuntos* representam uma forma simples de se modelar o mundo em que vivemos.

No século XIX, a chamada escola de Berlin participava o matemático alemão**Leopold Kronecker** (1823-1891). Ele estudou em Berlim e obteve o grau de doutor em 1845 com uma tese sobre Teoria dos Números. As suas principais contribuições para a matemática foram no campo da álgebra e continuidade de funções. A esta escola pertenceram matemáticos eminentes, especialistas em álgebra e na teoria dos números algébricos. A esses nomes podemos associar **Richard Dedekind** e seu aluno notável, *Georg Cantor*. **Richard Dedekind**, em constante contato com **Cantor**, utilizava os desenvolvimentos da teoria de conjuntos na sua elucidação do conceito de *continuidade* e na sua definição dos números reais. Como expressado por **Hilbert** com referência a **Dedekind**:

> "O matemático viu-se forçado a ser um filósofo, para poder seguir sendo matemático."

O ensinamentos de **Kronecker** sobre o infinito estavam em constante flagrante com as teorias de **Dedekind** e especialmente de **Cantor**. **Richard Dedekind**, durante 31 anos professor na *Technishe Hochschule de Brunswick*, construiu uma teoria rigorosa dos números irracionais. **Karl Wilhelm Theodor Weierstrass** (1815-1897), mais conhecido como **Karl Weierstrass**, foi um matemático alemão, professor

Figura 62 – Leopold Kronecker - Algebrista do século XIX, orientador acadêmico de Georg Cantor.

Fonte: https://pt.wikipedia.org/wiki/Leopold_Kronecker.

na Universidade de Berlim. **Cantor** e **Weierstrass** deram definições aritméticas de números irracionais um tanto diferentes da teoria de **Dedekind**, mas baseados em considerações semelhantes.

Figura 63 – Karl Weierstrass - Contemporâneo de Cantor em Berlin.

Fonte: https://pt.wikipedia.org/wiki/Karl_Weierstrass.

Aos olhos de **Kronecker**, entretanto, o maior herege, que se opunha às opiniões determinadas por certos grupos, era **Cantor**. **Cantor** era conhecido não só pela sua teoria dos irracionais, mas também pela sua *teoria dos conjuntos*. Com essa teoria, **Cantor** criou um campo inteiramente novo da pesquisa matemática, que era capaz de satisfazer as exigências mais sutis do rigor, uma vez que suas premissas fossem aceitas.

As publicações de **Cantor** começaram em 1870 e continuaram durante muitos anos. Em 1883 publicou *Grundlagen einer allgemeinen Mannigfaltigkeitslehre*, onde desenvolver uma teoria dos números cardinais transfinitos (como contar conjuntos infinitos) baseada num tratamento matematico sistemático do infinito. Atribui o menor cardinal transfinito $\aleph N$ ao conjunto enumerável. dando ao *continuum* um número transfinito mais elevado e, deste modo, conseguiu, tornou-se possível criar uma aritmética dos números transfinitos análoga à aritmética ordinária. No sentido de ordenar conjuntos infinitos, **Cantor** também definiu números ordinais transfinitos, expressando a maneira pela qual conjuntos infinitos pudessem estar ordenados (existisse uma relação de ordem sobre os conjuntos infinitos.

O principal opositor de **Cantor** era **Kronecker**, que representava uma tendência totalmente oposta no mesmo processo de aritmetização das matemáticas, diante das controvérsias das correntes filosóficas da matemática do século XIX. **Kronecker** era da corrente *intuicionista*, enquanto **Cantor**, da corrente *formalista*. Mas, **Cantor** ganhou larga aceitação quando a sua teoria para a fundamentação da teoria das funções reais e em topologia (espaços topológicos) se tornaram cada vez mais óbvia, especialmente depois de **Lebesgue**, que em 1901, enriqueceu a teoria dos conjuntos com a sua *teoria da medida*. Continuavam a haver dificuldades lógicas na teiroa dos números transfinitos e apareceram paradoxos, como, por exemplo, os de **Bertrand Russel**. Isto mais uma vez conduziu a diferentes escolas de pensamento sobre os fundamentos da matemático. A controvérsia do século XX entre formalistas e intuicionistas era, assim, uma continuação a um novo nível da controvérsia entre **Cantor** e **Kronecker**, que teria outros protagonistas. O leitor pode continuar entendendo o que aconteceu no início do século XX, no capítulos 14 e 15.

Cantor foi um matemático russo. Em 1856 sua família mudou-se para a Alemanha, continuando aí os seus estudos. Doutorou-se na Universidade de Berlim em 1867, tendo como professores **Ernst Kummer**, **Karl Weierstrass** e **Leopold Kronecker**. Em 1872 foi docente na Universidade de Halle-Wittenberg, na cidade alemã Halle an der Saale, ficando conhecido por ter elaborado toda a conceituação da **teoria dos conjuntos**.

Henri Léon Lebesgue(1875-1941) foi um matemático francês. Estudou de 1894 a 1897 na Escola Normal Superior de Paris e foi professor no Lycée Henri-Poincaré de Nancy. Lá ele descobriu a *integral* que leva seu nome. O autor, quando estudante de graduação no Instituto de Matemática da UFRJ (1971-1974), cursou um disciplina sobre a *integral de Lebesgue*. Lembra o autor que nesta disciplina foram demonstrados 12 lemas para se poder demonstrar o primeiro teorema.

Figura 64 – Cantor - as primeiras ideias da teoria dos conjuntos

Fonte: https://pt.wikipedia.org/wiki/Georg_Cantor.

Figura 65 – Henry Lebesgue - A teoria da medida que enriquecei a teoria de conjuntos de Cantor.

Fonte: https://pt.wikipedia.org/wiki/Henri_Lebesgue.

Os conceitos da **teoria dos conjuntos** são simples, mas requerem a abstração e a maturidade da linguagem de um sistema formal algébrico: a álgebra abstrata dos conjuntos. A teoria lida com as propriedades de coleções de elementos bem definidas chamadas de **conjuntos**. Os conjuntos são, então, compostos de elementos. E os elementos podem ser de qualquer natureza. Assim, servem como uma forma de se modelar o mundo que vivemos. De forma geral, podemos pensar esse mundo, como conjuntos de coisas de natureza quaisquer.

Posteriormente, no capítulo sobre a Visão Abstrata de Dados, falaremos de uma outra maneira de se modelar o mundo computacional que vivemos: os **objetos**. Mas, de qualquer forma, quando lá chegarmos, encontraremos os conjuntos de dados que são atributos de uma classe de objetos, os conjuntos de objetos de uma determinada classe, o conjunto de operações de uma classe. Enfim, encontraremos os conjuntos.

Vamos nos referir neste capítulo, as noções da **teoria dos conjuntos**, criada do ponto de vista intuitivo, por **Cantor**: a *teoria ingênua dos conjuntos*. Dados aos paradoxos encontrados pelo próprio **Cantor** e outros, como por exemplo, o que parece o paradoxo mais importante, o paradoxo de **Russel**, a teoria dos conjuntos passou por modificações propostas por outros matemáticos, no que tange a formulação de axiomas que sustentassem a teoria de *Cantor*.

Assim, em 1908, **Ernst Zermelo** (1871-1953) propôs a primeira *teoria axiomática dos conjuntos*, a chamada *teoria dos conjuntos de* **Zermelo**. Em 1922, um outro matemático, **Adolf Abraham Halevi Fraenkel** (1891-1965), melhorou o sistema axiomático criado por **Ernst Zermelo**. Ele propôs um dos muitos sistemas axiomáticos que foram propostos no início do século XX para promover uma teoria dos conjuntos sem paradoxos. Na matemática, a teoria dos conjuntos de **Zermelo-Fraenkel**, nomeada em homenagem a eles, é a *forma padrão da teoria axiomática dos conjuntos*, sendo o fundamento matemático mais comum, que conhecemos hoje. Entretanto, pelo nível a que se propõe este livro, adotaremos um ponto de vista informal, para mostrar vários exemplos na área da ciência da computação, e ilustrar o entendimento da matemática, usando esta ciência.

O primeiro trabalho de **Fraenkel** foi nos números p-ádicos de Kurt Hensel e na *Teoria dos Anéis*, uma estrutura algébrica definida entre os grupos e corpos algébricos, não abordada neste volume, mas que tem importância no estudo dos polinômios. Ele é conhecido por seu trabalho em teoria axiomática dos conjuntos, publicando seu primeiro grande trabalho no tema ("Einleitung in die Mengenlehre"), em 1919. Em 1922 e 1925 ele publicou dois artigos em que procurava melhorar o sistema axiomático de Zermelo; o resultado são os *axiomas de Zermelo-Fraenkel*. **Fraenkel** trabalhou na Teoria dos conjuntos e nos Fundamentos da matemática. **Fraenkel** também estava interessado na história da matemática, escrevendo em 1920 e 1930 sobre os trabalhos algébricos de **Gauss**, e ele publicou uma biografia de **Cantor**.

Figura 66 – Ernst Zermelo: a formalização da teoria dos conjuntos de Cantor

Fonte: www.learn-math.info.

Figura 67 – Adolf Fraenkel: a formalização da teoria dos conjuntos de Cantor

Fonte: https://pt.wikipedia.org/wiki/Adolf_Abraham_Halevi_Fraenkel.

Ao mesmo tempo e de forma independente, o matemático norueguês **Thoralf Albert Skolem** (1887-1963) fazia o mesmo. **Skolem** conhecido principalmente por seu trabalho em lógica matemática e teoria dos conjuntos. O resultado, um *sistema de dez axiomas*, chamados de *axiomas de Zermelo-Fraenkel*, é o mais utilizado atualmente para fundamentar a teoria dos conjuntos.

Figura 68 – Skolem - O pioneiro na construção de modelos *não-standard* de aritmética e teoria dos conjuntos.

Fonte: https://pt.wikipedia.org/wiki/Thoralf_Skolem.

Skolem publicou aproximadamente 180 artigos sobre equações diofantinas, teoria dos grupos, teoria dos reticulados, e principalmente sobre, lógica matemática e teoria dos conjuntos. **Skolem** publicou uma demonstração em 1927, mas **Emmy Noether** independentemente o redescobriu alguns anos depois. **Skolem** foi um dos primeiros a escrever sobre *reticulados*. Em matemática, especialmente na *teoria da ordem* e em álgebra, um *reticulado* é uma estrutura $L = (L, R)$ tal que L é parcialmente ordenado por R e para cada dois elementos a, b de L, existe o supremo (menor limite superior) e o ínfimo (maior limite inferior) de $\{a, b\}$. **Skolem** foi um pioneiro da *Teoria dos Modelos*. Na matemática, *Teoria de Modelos* é o estudo da representação de conceitos matemáticos em termos de teoria de conjuntos, ou o estudo de modelos que apoiam sistemas matemáticos. É assumido que existem alguns objetos matemáticos pré-existentes, e investiga-se o que pode ser concluído de tal coleção de objetos, algumas operações e/ou relações entre estes objetos, e alguns axiomas. Em 1920, ele simplificou enormemente a demonstração de um teorema de **Leopold Löwenheim**, demonstrado em 1915, resultando no teorema de Löwenheim-Skolem, o qual afirma que se uma teoria tem um *modelo*, então ela tem um *modelo enumerável*. *Skolem* (1922) refinou os axiomas de **Zermelo** para a teoria dos conjuntos, mas utilizando a

lógica de primeira ordem. O axioma resultante é parte, agora, dos axiomas padrão da teoria dos conjuntos. Em 1933 e posteriormente, **Skolem** foi pioneiro na construção de modelos *não-standard* de aritmética e teoria dos conjuntos.

A completude da lógica de primeira ordem é um corolário fácil, de resultados demonstrados por Skolem no início dos anos 20 e discutidos em Skolem (1928), mas ele não chegou a perceber este fato, talvez devido ao fato de os matemáticos e lógicos não estarem conscientes da completude como um problema matemático fundamental até a primeira edição de 1928 do Principles of Theoretical Logic de Hilbert e Ackermann quando a completude foi claramente enunciada. Em todo caso, Kurt Gödel primeiro provou esta completude em 1930.

Skolem desconfiou da ideia de infinito absoluto e foi um dos fundadores do *finitismo* na matemática. **Skolem** (1923) mostrou sua aritmética primitiva recursiva, uma contribuição muito precoce para a *teoria das funções computáveis*, como meio de evitar os então chamados paradoxos do infinito. Então, ele desenvolveu a aritmética dos números naturais primeiramente definindo os elementos por recursão primitiva, e então montando outro sistema para demonstrar propriedades dos elementos definidos pelo primeiro sistema. Esses dois sistemas o possibilitavam definir números primos e estabelecer uma parcela considerável da teoria dos números. Se o primeiro desses sistemas puder ser considerado como uma linguagem de programação para definir elementos, e o segundo como lógica de programação para demonstrar propriedades desses elementos, **Skolem** pode ser visto como um pioneiro não-intencional da *ciência da computação teórica*.

Como veremos no capítulo **??**, em 1929, **Presburger** provou que a aritmética de Peano sem multiplicação era consistente, completa (estes conceitos o leitor pode ver no capítulo 15) e *decidível* (ver no capítulo 12). No ano seguinte, **Skolem** provou que o mesmo era verdade para a aritmética de Peano sem a soma, um sistema denominado de aritmética de **Skolem** em sua homenagem. O famoso resultado de **Gödel** em 1931 (ver em 15) é que a própria aritmética de Peano (com ambas adição e multiplicação) era *incompleta* e consequentemente *indecidível*.

9.1 A solução da angústia de Cantor

A solução da angústia de Cantor, a *hipótese do continuum*, era a hipótese de que, depois do primeiro infinito, a próxima quantidade infinita seria a quantidade de pontos de um *continuum*, ou seja, a quantidade dos pontos da reta real ($\mathbb{R}$). Cerca de 60 anos se passaram, após a descoberta de **Cantor** desse problema fundamental, até que aparecesse uma solução. Ela foi encontrada por um outro matemático genial, dessa vez da Universidade de Chicago, chamado **Paul Joseph Cohen** (1934-2007), nascido em Long Branch, New Jersey, Estados Unidos. **Cohen** doutorou-se em matemática em 1958, na Universidade de Chicago. É mais conhecido pela sua prova da independência entre a *hipótese do continuum* e o *axioma da escolha* da teoria de

conjuntos de **ZermeloFraenkel**.

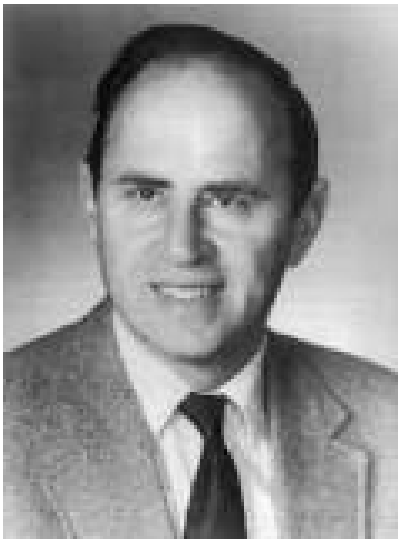


Figura 69 – Paul Joseph Cohen: a solução sobre a Hipótese do Continuum de Cantor.

Fonte: curvebank.calstatela.edu.

Na época de **Cohen** já havia suficiente maturidade matemática na *teoria dos conjuntos* para que alguém percebesse (provavelmente só **Cohen** percebeu na época) que a noção de *conjunto* era muito vaga (a teoria dos conjuntos nasceu ingênua) para que a *hipótese do continuum* pudesse ser demonstrada como verdadeira ou falsa.

Cohen provou que a *hipótese do continuum* não podia ser demonstrada com os outros axiomas da teoria, assim como sua negação também não poderia. Como consequência, acabamos podendo impor, ou não, a *hipótese do continuum* como um axioma independente dos demais, obtendo assim pelo menos duas matemáticas diferentes e contraditórias.

Por causa do trabalho de **Cohen**, surgiram a possibilidade da existência de pelo menos duas matemáticas diferentes. Uma matemática já era determinada por um *sistema lógico subjacente* e por uma *teoria de conjuntos*. Logo, como já se sabia antes de **Cohen**, existem infinitas matemáticas porque existem infinitas lógicas. Qualquer mudança em algum axioma do sistema lógico subjacente, ou em algum axioma de uma teoria de conjuntos, pode produzir uma matemática totalmente diferente. Mesmo que seja só uma simples mudança, em apenas um axioma - por exemplo, como aconteceu com a matemática baseada na *Fuzzy Logic* (lógica difusa), uma matemática que tantas aplicações industriais, tecnológicas e científicas tem tido nos seus anos de existência.

Mas, o trabalho de **Cohen** mostrou que a *hipótese do continuum*, que **Cantor** tentou desesperadamente demonstrar é, surpreendentemente, um *axioma da teoria dos conjuntos* que pode ser afirmado ou negado, produzindo matemáticas diferentes

em cada caso. O curioso é que, aparentemente, só a matemática clássica - aquela que afirma a *hipótese do continuum* - tem interessado à maioria dos físicos e veio a interessar aos matemáticos que conduziram à ciência da computação.

Cohen falou sobre seu trabalho sobre a independência do *axioma da escolha* e da *hipótese do continuum* dos axiomas de **Zermelo-Fraenkel** em uma palestra de título "*Independence results in set theory*", apresentada no simpósio internacional sobre a "*teoria dos modelos*"em Berkeley, em julho de 1963. Sua prova apareceu em dois artigos "*The Independence of the Continuum Hypothesis*"(1963) e "The Independence of the Continuum Hypothesis II"(1964). **Andrzej Mostowski**, revisando o primeiro deles, escreveu:

- Estes resultados apresentam as soluções longamente aguardadas, dos mais destacados problemas em aberto da teoria dos conjuntos axiomática e deve ser considerado como o mais importante avanço no estudo da teoria dos conjuntos axiomática, desde a publicação de ***Gödel*** *(capítulo 15) em 1940, da monografia "The Consistency of the Continuum Hypothesis"(1940). ... Para este revisor parece mais do que provável que a influência da descoberta de* ***Cohen*** *será, pelo menos, tão profunda em* ***metamatemática****, como na filosofia geral da matemática (e talvez não somente de matemática).*

Em 1966, **Cohen** publicou a monografia sobre *Teoria dos Conjuntos e a Hipótese do Continuum*, baseada em um curso que ele deu em Harvard na primavera de 1965. **Azriel Lévy**, quem ouviu pela primeira vez os resultados de **Cohen** na conferência sobre a teoria dos modelos em Berkeley, escreveu:

- Esta monografia é principalmente uma exposição dos resultados célebres do autor, ou seja, a independência da hipótese do contínuo e o axioma da escolha. Além disso, também apresenta os principais resultados clássicos em lógica e teoria dos conjuntos. ... Este livro apresenta uma abordagem nova e intuitiva e dá alguns vislumbres do processo mental que levou o autor a suas descobertas. O leitor encontrará neste livro apenas a quantidade certa de observações filosóficas para uma monografia matemática.

John Charles Fields (1863-1932) foi um matemático canadense que fundou a *Medalha Fields*, destinada a agraciar matemáticos por conquistas excepcionais. No mesmo ano, **Cohen** foi premiado com uma medalha *Fields*, considerada o prêmio Nobel da Matemática, pelo seu trabalho fundamental sobre os fundamentos da teoria dos conjuntos.

No inicio do século XX, em 1900, o matemático **David Hilbert** (leia no capitulo 14), formulou uma lista de 23 problemas como desafio para os matemáticos do século XX e a apresentou no *Congresso Internacional de Matemática de Paris*. O primeiro problema era a independência da *hipótese do continuum* em relação aos

outros axiomas das teorias de conjuntos. **Cohen** teve a distinção de resolver, 63 anos depois, o Problema 1 de **Hilbert** (ver em 14).

9.2 Conceitos Primitivos

Voltando à teoria dos conjuntos básica, as seguintes noções serão consideradas como *conceitos primitivos*: conjunto, elemento, relação de pertinência, relação de igualdade, igualdade de conjuntos e par ordenado.

Definição: (**Conjunto**) - Um conjunto é uma coleção de elementos, sem considerar repetição desses elementos dentro do conjunto. Se *repetição* de elementos é envolvida, o conceito é mais amplo e é denominado *bag*, em alusão a uma *bolsa*, que pode conter vários elementos repetidos dentro dela.

Definição: (**Elemento**) - Um elemento é um membro de um conjunto.

Definição: (**Relação de Pertinência**) - Sem um elemento x faz parte de um conjunto X, usa-se a notação $x \in X$, que deve ser lida como "x é elemento do conjunto X"ou "x pertence a X". A negação de $x \in X$ é representada por $x \notin X$, onde se lê "x não pertence a X.

Definição: (**Relação de Igualdade**) - Se dois elementos a e b representam o mesmo elemento, escrevemos $a = b$ e dizemos "a é igual a b e o símbolo denominado *sinal de igualdade*. A negação de $a = b$ será indicada por $a \neq b$ e que significa "a é diferente de b", ou seja, os símbolos a e b não representam o mesmo elemento.

Definição: (**Igualdade de Conjuntos**) - Consideraremos que dois conjuntos A e B sáo iguais se, e somente se, todo elemento de A pertence a B e todo elemento de B pertence a A. Abreviadamente, $A = B$.

Definição: (**Subconjunto**) - Sejam A e B dois conjuntos. Diz-se que A é subconjunto de B se, e somente se, todo elemento de A é também elemento de B. Usa-se a notação $A \subset B$ para indicar que A é subconjunto de B, A é uma parte de B, que A está contido em B ou que B contém A, isto é $B \supset A$. O símbolo $\subset$ é denominado *sinal de inclusão*.

Uma vez, introduzido o *sinal de inclusão* $\subset$, a noção de igualdade entre conjuntos pode ser posta como $A = B$ se, e somente se, $A \subset B$ e $B \subset A$.

Definição (**Complementar**)

Seja A uma parte de um conjunto E e seja, por hipótese que, um conjunto A', tal que $A' \subset E$, formado por todos os elementos x tais que $x \notin A$: $A' = \{x \in E \mid x \notin A\}$. O conjunto A' é denominado complementar de A em E e é indicado por $C_U A$.

Definição (**Conjunto Vazio**)

Da definição imediatamente anterior, podemos concluir que se $A = E$, teremos que $A' = \{x \in E \mid x \notin E\}$, ou seja, A' é um conjunto que não tem elementos. Isto é, A' é um *conjunto vazio*. Também podemos dizer que uma das partes de um conjunto E é o próprio conjunto E, definido como o complementar de E em E, o qual é indicado por ϕ. Esta definição mostra que o conjunto ϕ não possui nenhum elemento, e é indicado para simbolizar o *conjunto vazio*.

Também, se $A = E$, tem-se que $A' = \phi = \{x \in E \mid x \notin E\}, \forall\, E$. E pela hipótese na definição anterior, que $\phi \subset E, \forall\, E$. Esta última propriedade caracteriza o conjunto vazio, pois, se um conjunto A é tal que $A \subset E, \forall\, E$, tem-se, em particular que, $A \subset \phi$ e como $\phi \subset A$, teremos $A = \phi$, o que significa que existe um único conjunto vazio e que ele está contido em qualquer outro conjunto.

Para explicar o *conjunto vazio* em computação, o leitor pode imaginar uma tabela de banco de dados que foi criada e que, inicialmente, está *vazio*, sem ainda nenhum registro de dados.

Definição (**Conjunto Unitário**)

Seja E um conjunto náo vazio e seja a um elemento de E. O subconjunto de $\{x \in E \mid x = a\}$ é indicado por $\{a\}$ e é denominado *conjunto unitário* determinado pelo elemento a. Note que $\{a\} \subset E$ para qualquer que seja a de E.

Para explicar um *conjunto unitário* em computação, o leitor pode imaginar uma tabela de banco de dados que foi criado e que, inicialmente, tem armazenado apenas *um* registro de dados.

Definição (**Conjunto das Partes de um Conjunto**)

Para todo conjunto E admite-se que exista um outro conjunto, denotado por $P(E)$, cujos elementos são as partes de E. Em outras plavras, dizer que um conjunto $X \subset E$, é dizer que $X \in P(E)$. Dizemos que $P(E)$ é o *conjunto das partes* de E.

Se $E = \phi$, então, $P(E)$ é um *conjunto unitário* cujo único elemento é o *conjunto vazio*, isto é, $P(\phi) = \{\phi\}$.

Note que se $X = E$, temos $E \subset E$, ou seja $E \in P(E)$. Logo, todo conjunto também pode ser considerado como elemento de um outro conjunto.

Para explicar um *conjunto das partes* em computação, o leitor pode imaginar uma tabela de banco de dados que foi criado e que pode-se ter as visões desse banco (tabela) tendo armazenado registros que podem ser vistos desde o *vazio*, o *unitário* (quando só existe 1), podendo ser visto também as suas partes, constituídas de

subconjuntos contendo conjuntos de registros, até o último subconjunto, a visão final de toda a tabela, vista em termos de subconjuntos.

9.3 Operações com conjuntos

Para explicar as operações da álgebra dos conjuntos, é suposto que todos os conjuntos considerados são partes de um universo de conjuntos U, chamdo *conjunto-universo*.

Definição (**Interseção de Conjuntos**)

Sejam dois conjuntos A e B que são partes de U. A interseção B, denotada por $A \bigcap B$ é definida como $A \bigcap B = \{x \in U \mid x \in A \; e \; x \in B\}$.

Definição (**Conjuntos Disjuntos**)

Sejam dois conjuntos A e B que são partes de U. Se A interseção $B = \phi$, dizemos que A e B são *conjuntos disjuntos*, ou seja, não tem elementos em comum.

Definição (**União de Conjuntos**)

Sejam dois conjuntos A e B que são partes de U. $A \cup B$, denotada por $A \cup B$ é definida como $A \cup B = \{x \in U \mid x \in A \; ou \; x \in B\}$.

Definição (**Diferença entre Conjuntos**)

Sejam dois conjuntos A e B que são partes de U. O subconjunto $A - B = \{x \in U \mid x \in A \; ou \; x \notin B\}$ é denominado diferença entre A e B.

9.4 Visualização das Operações entre Conjuntos

As definições de *complemento*, *interseção*, *união* e *diferença* entre conjuntos, podem ser visualizadas nas Figuras 1a, 1b, 1c e 1d, pelos diagramas de **Venn**. **John Venn** (1834-1923) foi um matemático inglês. A partir de 1862, foi professor na Universidade de Cambridge, estudou e ensinou lógica e teoria das probabilidades.

Teorema (**Propriedades das Operações sobre conjuntos**)

Quaisquer que sejam as partes A, B e C de U, tem-se:

1. $A \cap A = A$ e $A \cup A = A$
2. $A \cap B = B \cap A$ e $A \cup B = B \cup A$ (propriedades comutativas)
3. $A \cup \Phi = A$ e $A \cap U = A$
4. $(A \cap B) \cap C = A \cap (B \cap C)$ e $(A \cup B) \cup C = A \cup (B \cup C)$ (propriedades associativas)

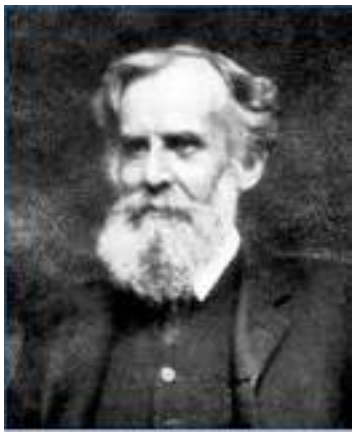


Figura 70 – Diagramas de Venn para as operações sobre conjuntos.

Fonte: https://pt.wikipedia.org/wiki/John_Venn.

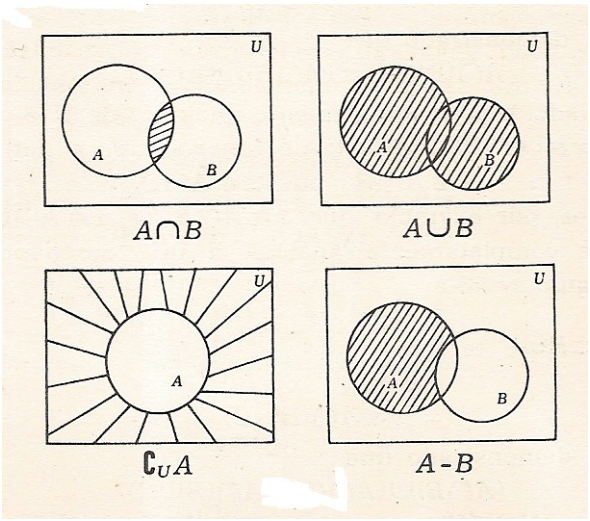


Figura 71 – Diagramas de Venn - Complemento, interseção, união e diferença entre conjuntos.

Fonte: Elementos de Álgebra, Jacy Monteiro, Monteiro (1969).

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (propriedades distributivas)

Aqui, um primeiro exemplo de uma álgebra, o que vem a ser a álgebra dos conjuntos. As noções de conjuntos finitos e infinitos, alguns axiomas desta teoria e a noção de subconjunto e as operações básicas sobre conjuntos, são mostrados como estão em Monteiro (1969).

9.5 Bag Theory - Multiconjuntos

Bag theory, também chamada de teoria dos multiconjuntos é uma generalização do conceito de *conjunto*. Num conjunto não existem elementos repetidos. Mas, a

repetição é consentida numa *bag* (num multiconjunto). Uma bag, corresponde ao caso de um bolsa que pode conter elementos iguais que são repetidos. Para especificar sistemas de computação, existe o método formal da linguagem Z Spivey (1988), Spivey (1989), que se utiliza da teoria dos conjuntos Monteiro (1969), da lógica dos predicados Loeckx e Sieber (1987), das funções do λ-Cálculo Michaelson (1989). Estendendo a linguage Z, existe a linguagem de especificão OBJECT Z Duke e Rose (2000), a qual reúne a linguagem Z, mais as estruturas de classe (um tipo abstrato de dados baseado em estados) com o comportamento dos esquemas da linguagem Z e mais lógica temporal.

9.6 Bibliografia e Fonte de Consulta

Biografia de Paul Joseph Cohen - http://www-history.mcs.st-andrews.ac.uk/Biographies/Cohen.html

A Solução da Angústia de Cantor - ⟨http://www.somatematica.com.br/coluna/08062001.php⟩

Luiz Henrique Jacy Monteiro - Elementos de Álgebra, IMPA, 1969.

John Venn - ⟨https://pt.wikipedia.org/wiki/John_Venn⟩

Zermelo - ⟨https://pt.wikipedia.org/wiki/Ernst_Zermelo⟩

Adolf Fraenkel - ⟨https://pt.wikipedia.org/wiki/Adolf_Abraham_Halevi_Fraenkel⟩

Georg Cantor - ⟨https://pt.wikipedia.org/wiki/Georg_Cantor⟩

Henri Lebesgue - ⟨https://pt.wikipedia.org/wiki/Henri_Lebesgue⟩

Thoralf Skolem - ⟨https://pt.wikipedia.org/wiki/Thoralf_Skolem⟩

Karl Weierstrass - ⟨https://pt.wikipedia.org/wiki/Karl_Weierstrass⟩

Leopold Kronecker - ⟨https://pt.wikipedia.org/wiki/Leopold_Kronecker⟩

9.7 Referências - Leitura Recomendada

Paul R. Halmos - Teoria Ingênua dos Conjuntos, Ed. Polígono, 1960.

Seymour Lipschutz - Teoria dos Conjuntos, Coleção Schaum, Ao Livro Técnico, 1968.

Benedito Castrucci - Elementos da Teoria dos Conjuntos, Livraria Nobel, 1969.

Edgard de Alencar Filho - Teoria Elementar dos Conjuntos, Livraria Nobel, 1980.

Corry, Leo. David Hilbert and the Axiomatization of Physics (1898-1918): from Grundlagen der Geometrie to Grundlagen der Physik. Dordrecht: Kluwer, 2004., p. 379.

Beiträge zur Begründung der transfiniten Mengenlehre, por Georg Cantor (em alemão).

CAPÍTULO 10

Relações e Funções

Este capítulo trata sobre relações e funções. Particulamente úteis na ciência da computação, as formas de relações de equivalência e de relações de ordem, aparecem em algumas situações relavantes da construção da ciência da computação, enquanto as funções deram origem a toda uma discussão inicial com relação as suas avaliações que redundaram na teoria da computabilidade e no surgimento das linguagens funcionais.

Introduzir, agora, a noção de produto cartesiano, é importante porque uma peça chave em um sistema de computação pode ser um banco de dados relacional, construido a partir de tabelas, e uma tabela explora o conceito de *relação*, que é um subconjunto de um produto cartesiano. Em termos do que existe matematicamente sobre relações, as propriedades mais importantes das **relações de equivalência** são usadas no paradigma da programação orientada a objetos, e as **relações de ordem** ordenam eventos em um sistema de computação, ordem dos eventos é fundamental. Finalizando o capítulo, consideraremos o conceito fundamental de aplicação e função.

10.1 Conceitos Básicos

Definição (**Pares Ordenados**)

Consideramos a noção de par ordenado como um conceito primitivo. A cada elemento a e a cada elemento b está associado um terceiro elemento indicado por (a, b), denominado par ordenado, de modo que se tenha $(a, b) = (c, d)$ se, e somente se, $a = c$ e $b = d$. Dizemos ainda que a é o primeiro elemento do par e b é o segundo elemento do par ordenado (a, b).

Para evitar confusões, fazemos algumas observações:

$\{a, b\} = \{b, a\}$, mas $(a, b) \neq (b, a)$.

No caso em que $a = b$, temos $\{a, b\} = \{a\}$, mas $(a, b) \neq (b, a)$. O que significa que deve-se fazer distinção entre o conujnto $\{a, b\}$ e o para ordenado (a, b).

Definição (**Produto Cartesiano**)

O conceito de produto cartesiano é a base para o conceito de relação, que por sua vez, deu origem, na década dos anos 70, aos bancos de dados relacionais.

Sejam dois conjuntos A e B diferentes do *conjunto vazio*. Chama-se *produto cartesiano*, denotado por $A \times B$, o conjunto de todos os pares ordenados (a, b), onde $a \in A$ e $b \in B$.

Assim, $A\ X\ B = \{(a, b) \mid a \in Aeb \in B\}$.

Se $A = \Phi$ ou $B = \Phi$, tem-se que $A \times B = \Phi$.

Generalizando, podemos ter um *produto cartesiano* de mais de dois conjuntos, tal como $A\ X\ B\ X\ ...\ X\ Y\ X\ Z$. Neste caso, dizemos que temos a construção de um *tupla* de n elementos.

Exemplo (Computação - **Produto Cartesiano**)

Seja um conjunto de pessoas e que um cadastro dessas pessoas tenha que ser feito por uma empresa que mantém uma carteira de clientes. Considere então os conjuntos denotados por NOME, ENDEREÇO, IDADE, INTERESSE, INSTITUICAO. Então, neste caso, define-se o produto cartesiano destes conjuntos, indicado por $(NOME \times ENDEREÇO \times IDADE \times INTERESSE \times INSTITUICAO)$, o conjunto formado por todos as quíntuplas (tuplas de 5 componentes) ordenadas por elementos destes conjuntos. Produto Cartesino são muito úteis para a construção de tabelas que armazenam dados numa base de dados computacional. Relações são subconjuntos de produtos cartesianos, e portanto, também muito importantes na construção de bancos de dados chamados relacionais.

10.2 Conceituando Relações

Definição (**Relação**)

Sejam E e F dois conjuntos e seja $E\ X\ F$ o *produto cartesiano* de E por F. Todo subconjunto R de $E\ X\ F$ é denominado *relação* de E em F. Se R é uma relação de E em E, neste caso, dizemos que R é um subconjunto de $E\ X\ E$, e R é uma *relação sobre* E.

Se R é uma relação entre E e F, usaremos a notação $a\ R\ b$, onde $a \in E$ e $b \in F$, lendo-se "a está na relação R com o elemento b, porque $(a, b) \in R$.

10.2.1 Relações de Equivalência

Descobrir relações de equivalência é fundamental para os matemáticos entenderem certas classes de objetos. Como exemplos, temos a congruência dos inteiros ("descoberta"por Gauss), que é ferramenta básica para entendermos certos teoremas em Teoria dos Números. Esta seção mostra a característica ou condição de coisas equivalentes. **Equivalente** é um adjetivo, oriundo do francês "équivalent", que expressa algo que possui igual valor, ou que tem o mesmo sentido. A palavra equivalente, quando usada para descrever alguma coisa, implica que essa coisa pode substituir outra tendo igual virtude, significado, ou atributo. Neste sentido pode-se pensar no conceito de **classe**, como um conjunto de coisas diferentes que podem substituir ou representar outras, porque essas coisas são equivalentes. Exemplos, numa classe de professores de matemática do ensino fundamental, um professor pode substituir ou representar outro. Note que os professores, como pessoas, são diferentes, mas, podem exercer a mesma tarefa, ou seja de ensinar a matemática fundamental.

Assim, na matemática ou lógica, é a característica das coisas diferentes, mas que possuem um mesmo valor, mesmo significado. Na Lógica, por exemplo, a correspondência entre duas proposições (sentenças) diferentes que possuem o mesmo valor-verdade, ou seja, se uma é verdadeira, a outra também será. Do ponto de vista da ciência da computação, o termo classe é um termo técnico, aplicado em linguagens orientadas a objetos, para descrever conjuntos de estruturas de dados caracterizados por propriedades comuns, chamadas de atributos. Portanto, seja em matemática, lógica ou ciência da computação, coisas diferentes estão reunidas num conjunto de coisas, mas que existe uma relação entre elas, chamada na álgebra de relação de equivalência.

Definição: (**Relação de Equivalência**)

Diz-se que uma relação R sobre um conjunto E é uma relação de equivalência se, e somente se, são válidas as seguintes condições:

- E1 - $\forall\, x \in E$, tem-se $x\ R\ x$, *propriedade reflexiva.*
- E2 - $\forall\, x, y \in E$, se $x\ R\ y$ então $y\ R\ x$, *propriedade simétrica.*
- E3 - $\forall\, x, y, z \in E$, se $x\ R\ y$ e $y\ R\ z$ então $x\ R\ z$, *propriedade transitiva.*

10.2.2 Relação de Equivalência e Partição de Conjunto

Seja E um conjunto não vazio e seja A uma parte não vazia de $\mathbf{P}(E)$. Diz-se que A é uma partição do conjunto E (ou seja, $A \in \mathbf{P}(E)$ se, e somente se, as seguintes condições são verificadas:

a) $X \neq \Phi$, para todo X em A; b) quaisquer que sejam X e Y em A, se $X \neq Y$, então $X \cap Y = \Phi$; c) para $X \in A$, $\bigcup X = E$.

De a) pode-se ver que $\Phi \notin A$ e a condição b) mostra que as partes em A são disjuntas duas a duas.

Existe, na álgebra, dois teoremas importantes sobre **partições de conjuntos** e **relações de equivalência**, que estabelece a conexão entre os conceitos de relação de equivalência e de partição.

Teoremas (**Relação de Equivalência e Partições**)

Toda partição P sobre um conjunto E, determina uma relação de equivalência sobre E.

Toda relação de equivalência sobre um conjunto E, determina uma partição sobre o conjunto E.

As demonstrações destes teoremas podem ser vistas em Nachbin (1971).

10.2.3 Relação de Ordem

De uma maneira geral, a palavra **ordem** diz respeito a disposição das coisas de acordo com uma categoria, ou seja, o lugar que lhes convém. Colocar em ordem é o ato ou efeito de organizar as coisas em posições pré-estabelecidas. Se coisas estão numa categoria, em posições pre-estabelecidas, causadas por algum fato, tais coisas estão relacionadas de algum modo característico, numa relação de causa e efeito. A matemática, através da álgebra, define essa relação, chamando-a de *relação de ordem*. Vejamos nas Figuras 73, 74 e 75, um exemplo da relação de ordem pensada por **Lamport** (ver na Figura 72) para ordenar eventos em um sistemas distribuido. Para contornar o problema do tempo físico em sistemas de computação distribuido, **Lamport** criou um modelo lógico, em que definiu uma relação de ordem sobre eventos se comunicando num sistema distribuido.

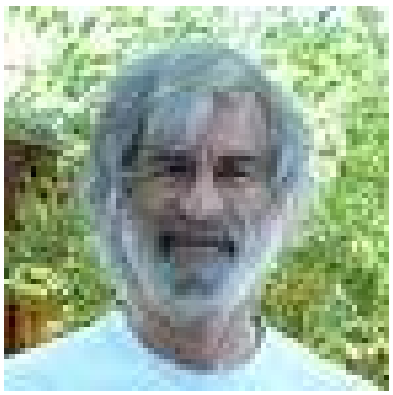


Figura 72 – Leslie Lamport - A ordem dos eventos em sistemas distribuídos.

Fonte: https://pt.wikipedia.org/wiki/Relação_de_ordem.

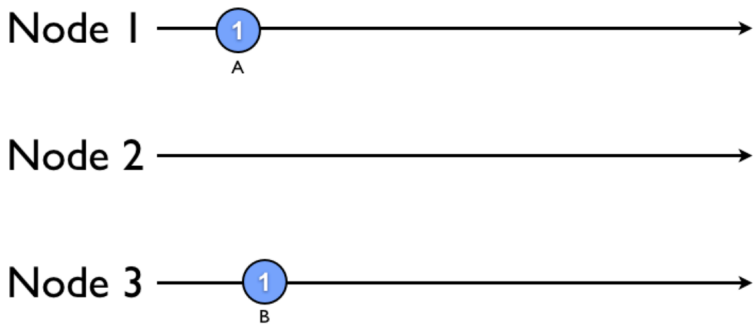


Figura 73 – Os nodos 1 e 3 têm tratado os eventos A e B.

Fonte: https://pt.wikipedia.org/wiki/Relação_de_ordem.

Na Figura 73, os nodos 1 e 3 têm tratado os eventos A e B, incrementando suas respectivas marcas de tempo de Lamport para 1. Mas, eles ainda não estão sincronizados com o nodo 2 ou uns com os outros, então vamos adiante para a Figura 74.

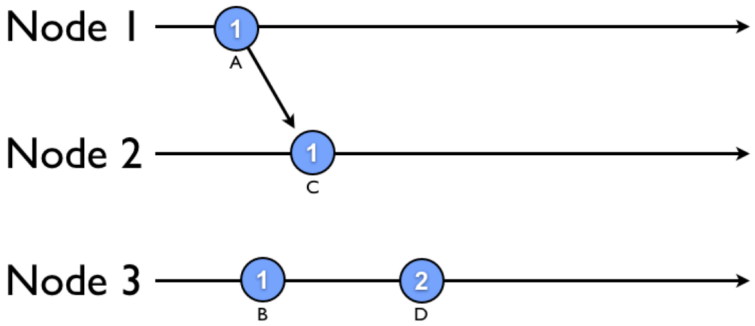


Figura 74 – Os nodos 1 e 2 foram sincronizados e o nodo 1 enviou uma mensagem ao nodo 2.

Fonte: https://pt.wikipedia.org/wiki/Relação$_d e_o rdem$.

Agora, na Figura 74 os nodos 1 e 2 foram sincronizados e o nodo 1 enviou uma mensagem ao nodo 2, considerando o seu rótulo de tempo, incrementando rótulo de tempo do nodo 2 para 1. Vamos adiante mais uma vez. Ver na Figura 75).

Na Figura 75 o nodo 3 trata de dois eventos D e E, e sincronizou com os outros dois nodos 2 e 1. Observe que o rótulo de tempo de **Lamport** do nodo 2, é incrementado para 3, saltando para o valor 2, porque o rótulo de tempo do evento de E já está em 3, que é um valor maior.

Nossos nodos agora, estão todos sincronizados, mas o que os nossos valores rótulos de tempos realmente tem a nos dizer? A prova de Lamport para este teorema é

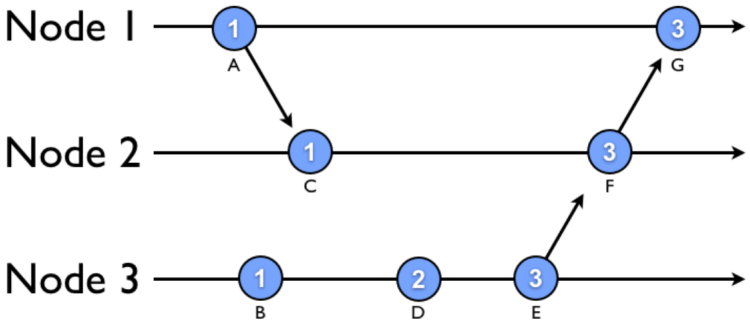


Figura 75 – O nodo 3 trata de dois eventos, D e E.

Fonte: https://pt.wikipedia.org/wiki/Relação_de_ordem.

"difícil", por isso não vamos falar sobre os detalhes do algoritmo aqui, mas sabemos no sentido causal (causalidade entre os eventos), imaginado por **Lamport**, em que o evento B veio antes do evento D, E aconteceu antes de F, e F aconteceu antes do evento G.

Infelizmente, há algumas coisas que não sabemos, já que não estamos armazenando informações sobre o estado dos outros nodos. Por exemplo, não temos nenhuma maneira de saber se C aconteceu antes ou depois ou B, pois são concorrentes. Nós precisaríamos de usar vetorr de relógios para discernir significativamente esta informação. Esta questão será vista mais adiante, nesta mesma seção, no tópico relogios-vetoriais.

Exemplo (**Relação de ordem em Computação**) - Num sistema de computação, eventos acontecem de forma ordenada, caracterizando uma relação de ordem. Num terminal de auto-atendimento, eventos de uma transação bancária, estão ordenados, desde o início até o término da transação.

Definição : (**Relação de Ordem**)

Diz-se que uma relação R sobre um conjunto E é uma relação de ordem se, e somente se, são verificadas as seguintes condições:

- O1 - $\forall\, x \in E$, tem-se $x\ R\ x$, *propriedade reflexiva.*
- O2 - $\forall\, x, y \in E$, se $x\ R\ y$ e $y\ R\ x$ então $x = y$, *propriedade anti-simétrica.*
- O3 - $\forall\, x, y, z \in E$, se $x\ R\ y$ e $y\ R\ z$ então $x\ R\ z$, *propriedade transitiva.*

Se R é uma *relação de ordem* sobre E diz-se que R é uma *ordem* sobre E. Também, pode-se dizer que E é um conjunto ordenado pela ordem R ou que E é *parcialmente ordenado* pela ordem R.

Diz-se que uma relação R sobre um conjunto E é uma *pre-ordem* se, e somente se, R é reflexiva e transitiva, isto é, R satisfaz as consições O1 e O3.

Exemplo (Computação - **Relação de ordem parcial numa sequência de eventos**)

No terminal de auto-atendimento, visto, como um único processo, os eventos são ordenados exclusivamente pelos tempos de um relógio local, ou seja, o tempo dado pelo relógio de um processador da máquina local ao terminal. Entretanto, como mostrado por LAMPORT (1978), não podemos sincronizar perfeitamente os relógios físicos em um sistema distribuído. Em geral, não podemos usar o tempo físico para mencionar a ordem de qualquer par de eventos arbitrários que ocorram dentro dele. Sendo um sistema distribúido, agora temos não mais um só processo, mas digamos, no caso mais simples, dois processos, onde ocorrem eventos que em processos diferentes. Para ordenar esses eventos, podemos, em geral, usar um esquema semelhante à causalidade física. E essa ordenação é baseada em dois fatos simples e óbvios:

- Se dois eventos ocorrem no mesmo processo p_i $(i = 1, 2, ..., N)$, então eles ocorrem na ordem em que o processo p_i os observou.
- Quando uma mensagem é enviada entre processos, o evento de envio da mensagem no processo emissor, ocorre antes do evento de recepção da mensagem no processo receptor.

Como em Coulouris, Dollimore e Kindberg (2007), textbfLamport observou a generalização desses dois relacionamentos de uma **relação de ordem**, chamada aqui, "*ocorreu-antes*", também conhecida como *relação de ordenação causal* ou *ordenação causal potencial*. Ele visualizou uma ordenação parcial entre eventos de um sistema distribuido de computação.
Pode-se, assim, definir a relação "*ocorreu-antes*". Denotamos essa ordem por $\rightarrow$.

- OA1: Se num processo p_i, se e ocorreu-antes de e' $(e \rightarrow_i e')$ então $e \rightarrow_i e'$.
- OA2: Se existem dois processos, um emissor e outro receptor de mensagens, paara uma mensagem m, a relação "*ocorreu-antes*"é: $envio(m) \rightarrow recebe(m)$, onde $envio(m)$ e $recebe(m)$ correspondem aos eventos de envio e recepção de m, respectivamente.
- OA3: Se e, e' e e'' são eventos tais que $e \rightarrow e'$ e $e' \rightarrow e''$, então $e \rightarrow e''$.

Desta forma, se e e e' são eventos e se $e \rightarrow e'$, então pode-se encontrar um conjunto de eventos ordenados $e_1, e_2, ..., e_n$que formam uma sequência de eventos em um ou mais processos, tal que $e = e_1$ e $e' = e_n$ e, para $i = 1, 2, ..., N - 1$, OA1 ou OA2 se aplica a aplica entre e_i e e_{i+1}. Isto significa, que ou os eventos ocorrem sucessivamente em um processo ou existe uma mensagem m tal que $e_i = envio(m)$ e $e_{i+1} = recebe(m)$. A sequência de eventos $\langle e_1, e_2, ..., e_n \rangle$ não precisa ser única.

A relação $\rightarrow$ ("*ocorreu-antes*"), pode ser ilustrada na Figura **??**para três processos p_1, p_2 e p_3. Suponha que em p_1 ocorram dois eventos sucessivos a e b. Em p_2 ocorram os eventos sucessivos c e d e que em p_3 ocorram dois eventos sucessivos e e f. Também, entre os eventos b e c existe o envio de uma mensagem m_1 entre p_1 e p_2. Também, entre os eventos d e f existe o envio de uma mensagem m_2 entre p_2 e p_3.

O que se pode concluir sobre a relação $\rightarrow$ ("*ocorreu-antes*")?

Note que, combinando estas relações, pode-se dizer, também, que $a \rightarrow f$. Mas, também que, nem todos os eventos estão relacionados pela relação $\rightarrow$ ("*ocorreu-antes*"). Por exemplo $a \nrightarrow e$ e $e \nrightarrow a$, pois eles ocorrem em diferentes processos ou não existe nenhum encadeamento de envio e recepção de mensagens entre eles. Neste caso, dizemos que os eventos a e e que não são relacionados pela relação $\rightarrow$ ("*ocorreu-antes*"), são eventos concorrentes, e escrevemos $a \parallel e$.

A relação $\rightarrow$ captura um fluxo de dados entre dois eventos. Note também que, os dados podem fluir de maneiras diferentes da passagem de mensagens. Veja o caso em que alguém envia uma mensagem a outra pessoa e depois, avisa a essa pessoa, que por sua vez, faz seu processo enviar outra mensagem para outra pessoa, então o envio da primeira mensagem claramente ocorreu antes da segunda, mas a relação $\rightarrow$, como definida, não relaciona nenhuma mensagem de rede enviada entre as pessoas emitentes, e neste caso, não podemos modelar esse tipo de relacionamento com tal relação $\rightarrow$.

Outra questão a ser notada é que, se a relação ("*ocorreu-antes*") vale entre dois eventos, então o primeiro, poderia ou não, ter causado o segundo. No caso de um servidor que recebe uma mensagem de requisição e, subsequentemente, envia uma resposta, então o evento de envio, obviamente, causou o evento de resposta. Ou o evento de resposta foi causado pelo envio da requisição. Entretanto, a relação $\rightarrow$ ("*ocorreu-antes*"), captura apenas, a *causalidade em potencial*, pois dois eventos podem estar relacionados por $\rightarrow$, mesmo que não exista nenhuma conexão entre eles. No caso do servidor receber uma requisição e enviar subsequentemente outra mensagem a cada 10 minutos, sem nenhuma relação específica com a primeira mensagem, nenhuma causalidade real existe, mas a relação $\rightarrow$ ordenaria esses eventos.

Relógios Lógicos - Lamport criou um mecanismo por meio do qual a ordenação ("*ocorreu-antes*") pode ser capturada numericamente, chamado *relógio lógico* Coulouris, Dollimore e Kindberg (2007). Este é uma variável no software de cada processo, um contador que aumenta a contagem monotonicamente, e seu valor não tem qualquer relacionamento com um relógio físico. Cada processo p_i mantém seu próprio relógio L_i, que usa para indicar tempo lógico nos eventos. Denota-se a indicação de tempo do evento e em p_i como $L_i(e)$.

Para capturar a relação $\rightarrow$("*ocorreu-antes*"), os processos precisam atualizar seus relógios e transmitir os valores de seus relógios em mensagens, seguindo as seguintes

regras:

- RL1: L_i é incrementado antes da ocorrência de um evento no processo p_i: $L_i = L_i + 1$
- RL2:
  - (a) Quando um processo p_i envia uma mesnagem m, m leva junto o valor $t = L_i$.
  - (b) Quando da recepção de (m, t), um processo p_j calcula o maior tempo $L_j = max\{L_j, t\}$ e, então, aplica RL1 antes de indicar o tempo do evento $recebe(m)$.

Pode ser mostrado por indução (...) sobre o tamanho da sequência dos eventos, que, relacionando-se dois eventos e e e', que $e \rightarrow e' \Rightarrow L(e) < L(e')$. Note que o inverso, não é verdade. Se $L(e) < L(e')$, não podemos concluir que $e \rightarrow e'$. Note, também que, para os eventos b e e, $L(b) > L(e)$, mas $b \parallel e$.

Exemplo (**Computação - Relação de ordem total numa sequência de eventos**)

A definição 10.2.3 diz respeito a uma relação de ordem parcial. Para se conseguir uma relação de ordem total a partir da relação $\rightarrow$ ("*ocorreu-antes*"), a seguinte regra O4, acrescentada à definição 10.2.3, define o que vem a ser uma **relação de ordem total**. Se uma relação de ordem R sobre um conjunto E, verificar a condição:

- O4 - $\forall\, x, y \in E$, se $x\ R\ y$ ou $y\ R\ x$, diz-se que R é uma *relação de ordem total* sobre E ou que E é um conjunto totalmente ordenado pela ordem R.

Com as regras sobre os relógios para rótulos de tempo, alguns pares de eventos distintos, gerados por processos distintos, podem ter rótulos de tempo numericamente idênticos. Entretanto, podemos criar uma ordem total nos eventos. Uma ordem para qual todos os pares de eventos distintos, sejam ordenados levando-se em conta os identificadores dos processos em que os eventos ocorrem.

Assim, se e é um evento ocorrendo em p_i com indicação de tempo local T_i e e' é um evento ocorrendo em p_j com indicação de tempo local T_j, define-se os rótulos de tempo globais lógicas para esses eventos como (T_i, i) e (T_j, j) respectivamente. E define-se $(T_i, i) < (T_j, j)$, se e somente se, $T_i < T_j$ ou $T_i = T_j$ e $i < j$. Essa ordenação não tem nenhum significado físico, porque os identificadores de processos são arbitrários.

Relógios Vetoriais - Como em Coulouris, Dollimore e Kindberg (2007), sob o fato de que se $L(e) < L(e')$, não se pode concluir que $e \rightarrow e'$, MATTERN (1989) e

FIDGE (1991) desenvolveram relógios vetoriais para superar a deficiência dos relógios de **Lamport**.

Um relógio vetorial para um sistema de N processos é um vetor de N inteiros. Cada processo mantém seu próprio relógio vetorial V_i, o qual é utilizado para rotular o tempo dos eventos locais. As mensagens dos processos levam, junto, os rótulos de tempo vetoriais nas mensagens que trocam si e existem regras para atualizar os relógios como segue:

- RV1: No início, $V_i[j] = 0$, $j = 1, 2, ..., N$
- RV2: Imediatamente antes de p_i, rotular o tempo de um evento, ele configura $V_i[i] = V_i[i] + 1$.
- RV3: p_i inclui o valor $t = V_i$ em cada mensagem que envia.
- RV4: Quando p_i recebe um rótulo de tempo t em uma mensagem, ele configura $V_i[j] = max\{V_i[j], t[j]\}$, para $j = 1, 2, ..., N$.

Para um relógio vetorial V_i, $V_i[i]$ é o número de eventos em que p_i indicou o tempo e $V_i[j](j \neq i)$ é o número de eventos ocorridos em p_j, nos quais p_i foi potencialmente afetado. O processo p_j pode ter indicado o tempo de mais eventos nesse ponto, mas ainda nenhuma informação sobre eles fluiu para p_i nas mensagens.

Pode-se comparar as indicações de tempo vetoriais, como segue:

- $V = V'$, se e somente se $V[j] = V'[j]$, para $j = 1, 2, ..., N$
- $V \leq V'$, se e somente se, $V[j] \leq V'[j]$, para $j = 1, 2, ..., N$
- $V < V'$, se e somente se, $V \leq V' \wedge V \neq V'$

Seja $V(e)$ o rótulo de tempo vetorial aplicada pelo processo em que o evento e ocorre. Pode-se mostrar por indução, que no tamanho de qualquer sequência de eventos relacionados a dois eventos e e e', que $e \rightarrow e' \Rightarrow V(e) < V(e')$ e que o inverso é verdadeiro, se $V(e) < V(e')$, então $e \rightarrow e'$.

Os rótulos de tempo vetoriais tem a desvantagem, quando comparados com os rótulos de tempo de **Lamport**, porque ocupam espaço de armazenamento e carga útil nas mensagens proporcional ao número de processos N.

Uma relação de ordem parcial ou total, é indicada pelo símbolo $\leq$ (leia-se menor, precede). A ordem oposta pode ser indicada pelo símbolo $\geq$ (leia-se, maior, sucede), com a igualdade que está na regra O3.

Definição (**Relação de Ordem Estrita**)

Usada em Coulouris, Dollimore e Kindberg (2007), uma terceira definição de **ordem**, é a de uma **ordem estrita** associada à ordem $\leq$, é indicada por $<$. E a ordem estrita associada a $\geq$ é indicada por $>$. Portanto, $a < b$ significa que $a \leq b$ e $a \neq b$ deve ser lido como "a é estritamente menor que b"ou "a precede b". Enquanto $a > b$ significa que $a \geq b$ e $a \neq b$ deve ser lido como "a é estritamente maior que b"ou "a sucede b". Uma relação de ordem estrita é o caso em que a *igualdade* é excluida da definição da relação.

Diz-se que uma relação R sobre um conjunto E e consideremos uma relação $R*$ sobre E definida por:

$xR * y$ se, e somente se, xRy e $x \neq y$.

Neste caso, verifica-se que $R*$ é uma *relação de ordem estrita* se, e somente se, são verificadas as seguintes condições:

- O1' - $\forall\, x \in E$, tem-se $x \neg R *\ x$.
- O2' - $\forall\, x, y \in E$, se $x\ R *\ y$ então $y \neg R * x$.
- O3' - $\forall\, x, y, z \in E$, se $x\ R *\ y$ e $y\ R *\ z$ então $x\ R *\ z$, *propriedade transitiva.*

Pode-se verificar que se a ordem R é total, então a ordem estrita associada a R é total.

10.3 Funções

Função é um dos conceitos mais importantes da matemática e úteis em várias ciências. Existem várias definições, dependendo da forma como são expostas, de maneira informal a mais formal das definições. As funções são entidades matemáticas que atribuem resultados únicos para determinadas variáveis. Neste tópico, é mostrado como se pode avaliar, representar graficamente, analisar e criar vários tipos de funções. De um modo geral, existem as funções naturais (reais), que existem na natureza, mas existem as funções altamente artificiais, que nunca se mostram em nenhum processo relacionado ao mundo real. O que estes dois caso tem em comum é que em ambas as situações existem domínios onde são definidas, contra-domínios onde são avaliadas e, um mapeamento é considerado entre o conjunto-domínio e o conjunto do contra-domínio.

10.3.1 Origem das Funções

O primeiro passo é sabermos a origem do conceito de função. Em comparação a outras questões matemáticas, como o sistema de numeração, por exemplo, a origem conceitual de função é bem mais recente. Acredita-se que a primeira menção teria

surgido a partir dos estudos do cálculo infinitesimal, por volta do século XVII, nos tempos de **Isaac Newton** (1642-1727) e **Wilhelm von Leibniz** (1646-1716). O primeiro a citar o conceito foi o inglês **Isaac Newton**. Todavia, ele deu um nome tanto quanto confuso para as suas ideias. **Newton** descrevia "relatia quantias", para a variável dependente e, "genita", para a quantidade sendo avaliada.

O uso de "função"como um termo matemático foi iniciado por **Leibniz**, em 1673, para designar uma quantidade relacionada a uma curva, tal como a sua inclinação em um ponto específico Arp e Caplan (2013a). As funções que **Leibniz** considerou são atualmente chamadas de *funções diferenciáveis* (deriváveis). Em relação a este tipo de função, pode-se falar em *limites* e *derivadas*. Estes conceitos são medidas dos valores de saída ou de sua variação em relação aos valores de entrada, e formam a base do *cálculo diferencial* (cálculo infinitesimal). A palavra *função* foi, posteriormente, usada por **Euler** em meados do século XVIII para descrever uma expressão envolvendo vários argumentos (variáveis em que são definidas).

Com o tempo foi-se ampliando a definição de funções. No final do século XX, funções foram identificadas como importantes para a construção de modelos físicos de fenômenos, como por exemplo, o *Movimento Browniano* que é o movimento aleatório das partículas suspensas num fluido (líquido ou gás), resultante da sua colisão com átomos rápidos ou moléculas no gás ou líquido. Um modelo matemático pode se referir para descrever tais movimentos aleatórios de partículas.

10.3.2 Definição Formal de Função

Johann Peter Gustav Lejeune Dirichlet (1805-1859) foi um matemático alemão, a quem se atribui a moderna definição formal de função. Na probabilidade e estatística, existe a *Distribuição de Dirichlet*, tendo atuado também na Teoria dos Números

Considere dois conjuntos: um conjunto X com elementos x e um conjunto Y com elementos y. Diz-se que a relação f é uma função de X em Y, que relaciona cada elemento x em X, num único elemento $y = f(x)$ em Y. A função f é uma relação binária entre os dois conjuntos tal que Stewart (2002):

1. f é unívoca: se $y = f(x)$ e $z = f(x)$, então $y = z$;
2. f é total: para todo x em X, existe um y em Y tal que $y = f(x)$.

Se a primeira condição é atendida, mas a segunda não, temos uma *função parcial*, que atende a certas situações que podem ocorrer em computação.

O conjunto $Y' = \{f(x), x \in X, f(x) \in Y\}$ é chamado de conjunto *imagem*, porque é o conjunto de todos os elementos de Y que são associados pela regra de mapeamento de f aplicado em X.

Figura 76 – Dirichlet - A quem se atribui a moderna definição formal de função.

Fonte: https://www.google.com.br/?gws_rd=ssl#q=Dirichlet.

Uma **transformação** é uma função onde o domínio é o mesmo que o contra-domínio. Diz-se, neste caso, existir, uma transformação de S sobre S. Em Janos (2009), em seu capítulo 5 sobre **Estruturas**, são mostradas as formas de *transformação* mais utilizadas: (1) *rígidas* (rotação, reflexão, translação), (2) *transformação da inversão* e as (3) *transformações afins*. Através do conceito de **transformação**, somos levados ao estudo das **Simetrias**, que introduz uma das mais importantes ideias da Matemática, os **Grupos**. Seu estudo é feito com base em transformações. Na **Teoria dos Grupos ??** procura-se capturar padrões e colocá-los em forma que nos possibilita associar matematicamente simetrias e grupos. No estudo sas simetrias e grupos surge o conceito de **regularidade**, onde são estudadas as maneiras que a Matemática encontrou de preencher o plano e o espaço tridimensional.

10.3.3 Tipos de Funções

Gráfico de uma função - As funções são comumente representadas em gráficos. O gráfico de uma função $f : X \to Y$ é o conjunto dos pares ordenados em $X \times Y$ da forma $(x, f(x))$, ou seja: $\{(x, y) \in X \times Y \| x \in X, y = f(x)\}$.

Do ponto de vista de como se configuram os elementos avaliados no contra-domínio, podemos ter:

Função Injetora - Cada elemento da imagem está associado a apenas um elemento do domínio, isto é, quando $x \neq y$ no domínio, tem-se $f(x) \neq f(y)$ no contradomínio.

Função Sobrejetora - Todos os elementos do contradomínio estão associados a algum elemento do domínio.

Função Bijetora (bijeção) - São ao mesmo tempo sobrejetoras e injetoras, isto é, cada elemento do domínio está associado a um único elemento do contra-domínio e vice-versa.

Função Inversa - Do ponto de vista de como se configuram os elementos avaliados no domínio em relação aos elementos no contra-domínio, temos o caso das *funções inversas*. A função inversa de $f^{-1} : B \to A$ é uma função com gráfico $(f(x), x)$, definida no contra-domínio, onde pode-se obter o gráfico de $f^{-1}(x)$, relacionado em torno de $y \to x$. Dizemos que f^{-1} é a função inversa de f. Uma função pode ter a sua inversa, ou não. Em computação, funções que não tem inversas tem sua utilidade, particularmente, na criação das chamadas funções *hash*, muito úteis em segurança da informação, para verificar a integridade (erros) dos conteúdos de grandes arquivos transmitidos (em geral, baixados) à longa distância numa rede como a Internet.

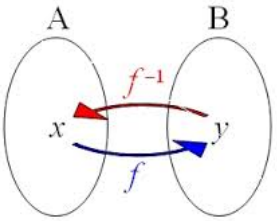


Figura 77 – A inversa f^{-1}de uma função f está representado nas associações na cor laranja.

Fonte: infopedia.pt.

10.3.4 Composição de funções

Seja $f : A \to B$ e $g : B \to C$. A função denotada por $g \circ f : A \to C$ é denominada a composição de f e g.

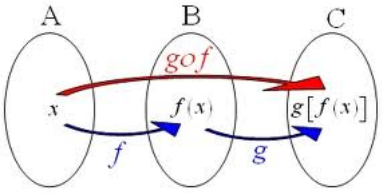


Figura 78 – A composição de duas funções f e g proporcionando $g(f(x))$.

Fonte: infopedia.pt.

10.3.5 Funções Lambda

Nos anos 30, **Alonzo Church** (1903-1995) criou uma notação para descrever funções, como um modelo para *computabilidade*, e foi fundamental para a ciência da computação, desde sua origem até os dis atuais. Na época, já introduzido por **Herbrand-Gödel**, a discussão sobre funções pairava sobre a ideia das *funções recursivas*, uma

forma de repetir a avaliação de uma função e, se obter resultados infinitos, a partir da repetição de uma definição (expressão da função) finita.

Utiliza-se, em geral, variáveis x e y para representar as entradas (argumentos) de funções. Uma forma de representar uma função é expor o mapeamento explícito, ou seja, o processo de avaliar uma função. Por exemplo, como em $x \longmapsto 2x + 5$. O símbolo $\longmapsto$ indica *associação*. Como em Carnielli e Epstein (2005), tal notação sugere o aspecto dinâmico das funções.

Se não houver um símbolo padrão para denominar uma função, usualmente nomeia-se as letras, tais como, f, g, φ ou ψ, para dar nomes às funções. Pode-se escrever, também, $x \longmapsto f(x)$.

Se escrevemos, contudo, $f(x) = 2x + 5$, a notação será ambígua Carnielli e Epstein (2005). Não estará claro, se nos referimos à função f, ou se estamos nos referindo à avaliação de uma entrada arbitrária x, considerando uma saída para aquele x particular. Isto é, pode ocorrer: (1) $f(x)$ pode significar a própria função f, ou (2) o valor de f aplicada a um valor particular x. Da mesma forma, quando escrevemos $f(x) = 5$, estamos nos referindo a algum valor particular de x, tal que $f(x) = 5$? Ou significa a função-constante $f(x) = 5$?

Se tivermos, agora, uma função de duas variáveis, $(x, y) \longmapsto x + y$, onde x e y são números reais, embora se saiba que para um soma finita de parcelas, a ordem nao altera a soma, comumente, na avaliação de uma função, a ordem das parcelas é importante e, parte da regra de avaliação da função é a ordem das entradas. Assim, toma-se sempre, a entrada de uma função de várias variáveis como uma coleção ordenada de números (tuplas ordenadas). Neste caso, então, $(x, y) \longmapsto x + y$ (lê-se (x, y) é mapeado para $x + y$) e temos que $(3, 5) \longmapsto 8$ e $(5, 3) \longmapsto 8$, como explicado em Carnielli e Epstein (2005).

Mas, se tivermos que distinguir entre $f(3, 5) = 3 + 5$, uma função de *duas* variáveis, e $g(3) = 3 + 5$, uma função de *uma* variável? Aí, surgiu a ideia da notação λ, criada por **Church**. Escreve-se $\lambda \;\; x \;\; (x + 5)$ para indicar que estamos vendo a função de duas variáveis $(x, y) \longmapsto x + y$ como uma função apenas da primeira variável, com a segunda variável matida fixa como 5. Escreve-se então $\lambda \;\; x \;\; (x + y)$ significando que vemos a função de duas variáveis $(x, y) \longmapsto x + y$ como uma função apenas da primeira variável, com a segunda variável mantida fixa. Nesta notação, y é dito ser um parâmetro visto como fixo, apesar de não especificarmos o valor que está sendo usado para y. Dependendo do que escolhermos para y, temos uma função diferente. Se escolhermos $y = 9$, teremos a função $\lambda \;\; x \;\; (x+9)$. Portanto, se quisermos representar uma função de duas variáveis x e y, escrevemos $\lambda \;\; x \;\; y \;\; (x + y)$. O símbolo λ define quais são as *variáveis* na expressão da função. Usa-se esta notação λ sempre que o contexto não tornar o significado claro. E agora, pode-se escrever $\lambda \;\; x \;\; (9)$ para a função-constante de saída 9.

10.3.6 Linguagens Funcionais

A notação λ foi criada, para se descrever funções de forma não-ambígua, antes mesmo de existir o computador. A notação é muito simples, mas poderosa, e é baseada sobre a **abstração** de função, para generalizar expressões, através da introdução de nomes de variáveis, e a aplicação da função para avaliar expressões generalizadas por se atribuir valores particulares aos nomes dessas variáveis. **Abstração** é baseada sobre o uso de nomes para representar objetos concretos e operações sobre esses, para generalizar as instâncias , uma **especialização** como uma forma de se associar um valor a um nome, como explicado em Michaelson (1989).

O que se descobriu depois com a existência do computador? Como explicado em Michaelson (1989), a notação λ tem um número de propriedades que se adequam muito bem para descrever linguagens de programação: (1) A notação por ser simples é fácil para se implementar. (2) Somente a abstração e a aplicação são necessárias para desenvolver representações para construções de linguagens de programação. Tudo que a notação provê são nomes, abstração de funções e a aplicação de funções. E assim é possivel desenvolver construções de linguagens funcionais, a partir desta base teórica para funções, para executar construções de uma linguagem, caracterizada por diferir das características das contruções das linguagens imperativas (as comumente usadas), particularmente, nas *atribuições* e nas *repetições*. Sobre atribuições, pode-se afirmar que em linguagens imperativas, o mesmo nome pode ser associado com diferentes valores, enquanto nas linguagens funcionais, um nome é somente associado com um valor. Sobre a repetição, isto significa fazer a mesma coisa zero ou mais vezes. E em linguagens funcionais, repetição é baseada sobre a ideia de **recursão**: a definição de alguma coisa em termos de si própria, descrita formalmente em termos da notação λ.

Uma outra grande contribuição da notação λ, foi o seu uso na abordagem de **Christopher Strachey** (1916-1975), um cientista britânico da ciência da computação que construiu para descrições de linguagens imperativas baseadas na notação λ, de modo que toda construção imperativa teria uma denotação de funcão equivalente. A abordagem de **Strachey** foi fortalecida pela descrição teórica do*lattices* de **Dana Stewart Scott** (1932-), para a notação λ. Em matemática, um *lattice* (reticulado) é um conjunto parcialmente ordenado em que cada dois elementos têm um supremo exclusivo (também chamado de um menor limite superior) e um ínfimo exclusivo (também chamado de um maior limite inferior). Um exemplo é dado pelos números naturais, parcialmente ordenado pela relação de *divisibilidade*, para o qual o *supremo* único é o *mínimo múltiplo comum* (m.m.c) e o *ínfimo* único é o *máximo divisor comum* (m.d.c). *Lattices* (reticulados) também podem ser caracterizados como estruturas algébricas que satisfaçam determinados axiomas. Atualmente, semântica denotacional é usada para dar definições formais de linguagens de programação Loeckx e Sieber (1987). Linguagens funcionais estão proximamente relacionadas à semântica de linguagens baseada na notação λ, como em Schmidt (1986).

10.4 Bibliografia e Fonte de Consulta

MONTEIRO, L. H. J. (1969) Elementos de Álgebra. IMPA. Ao Livro Técnico SA, Cap.2, pgs.22-23.

NACHBIN, L. (1971) Introdução à Álgebra. McGraw-Hill. Rio de Janeiro.

Rylan Dirksen - ⟨https://blog.8thlight.com/rylan-dirksen/2013/10/04/synchroniza\penalty\@M\hskip\z@skip\discretionary{-}{}{}\penalty\@M\hskip\z@skiption-in\penalty\@M\hskip\z@skip\discretionary{-}{}{}\penalty\@M\hskip\z@skip-a-distri\penalty\@M\hskip\z@skip\discretionary{-}{}{}\penalty\@M\hskip\z@skipbuted-system.html⟩

COULOURIS, G., DOLLIMORE J., KINDBERG, T.. Distributed Systems: Concepts and Design. Addison Wesley Plublishers. 4th Edition.2005.

ARP, Robert; CAPLAN, Arthur. 1001 Ideas That Changed the Way We Think. Nova Iorque: Simon and Schuster, 2013. pp. 374.

STEWART, James. Cálculo Vol. I - 4ª edição. São Paulo: Pioneira Thomson Learning, 2002. Página 12.

10.5 Referências - Leitura Recomendada

LAMPORT, L. (1978). Time, clocks and the ordering of events in a distributed system. *ACM Communications* , Vol. 21, No. 7, p.558-565.

MATTERN, F. (1989). Virtual Time and Global States in Distributed Systems. Em Cosnard, M. et al. (eds), *Proceedings Workshop on Parallel and Distributed Algorithms*. Amsterdan, Holanda, pgs.215-226.

FIDGE, C. (1991). Logical Time in Distributed Computing Systems. *IEEE Computer*, Vol 24, No.8, pgs.28-33.

FRANK AYRES, Philip A. Schmidt. Matemática para Ensino Superior - 3ª edição. São Paulo: Editora Artmed, 2003. Página 16.

STEWART, James. Cálculo Vol. I - 4ª edição. São Paulo: Pioneira Thomson Learning, 2002.

FRANK AYRES, Philip A. Schmidt. Matemática para Ensino Superior - 3ª edição. São Paulo: Editora Artmed, 2003.

LIMA, Elon Lages. Curso de análise volume 1. 11ª edição, 2004. página 13

Christopher Strachey - ⟨https://en.wikipedia.org/wiki/Christopher_Strachey⟩

Dana Stewart Scott - ⟨https://en.wikipedia.org/wiki/Dana_Scott⟩

R. J. Connor and J. E. Mosiman 1969. Concepts of independence for proportions with a generalization of the Dirichlet distibution. Journal of the American Statistical Association, volume 64, p.194-206.

CAPÍTULO 11

Grupos e Corpos

Uma das realizações mais importantes da Matemática é ter mostrado que estruturas aparentemente dissimilares podem ter muitos atributos em comum. Esses atributos podem ser codificados em um conjunto de axiomas, e conclusões podem ser deduzidas para todas as estruturas que satisfaçam esses axiomas. Uma das mais importantes estruturas é chamado de *grupo*. Seguindo a sequência de surgimento, sobre as extensões das definições de estruturas algébricas, depois da estrutura de *grupo*, são definidas as estruturas de *anel* e de um *corpo* algébrico. A partir deste último define-se a estrutura de um *espeço vetorial*, que tem como base uma estrutura de um *corpo* algébrico. Mas, por enquanto, fiquemos, para fins de compor o roteiro deste livro, apenas com a definição de um *grupo*. Os espaços abstratos gerados por vetores de comprimento finito conduziram aos espaços métricos abstratos que hoje levam o nome de **Hilbert**. E os espaços de **Hilbert** fornecem a base matemática para o futuro da ciência da computação: a *computação quântica*.

Na Álgebra moderna, um **grupo** é um conjunto de elementos, munido de uma operação que combina dois elementos quaisquer, para formar um terceiro pertencente ao conjunto. A operação deve satisfazer algumas condições chamadas **axiomas de grupo**: **associatividade**, um **elemento neutro** sobre a operação dos elementos do conjunto, e **elementos inversos** (simetrizáveis) diante da operação que define o *grupo*.

Na área da geometria, **grupos** compartilham um parentesco fundamental com a noção de **simetria**. Um *grupo de simetria* guarda informações sobre as simetrias de um objeto geométrico.

A ubiquidade dos grupos em inúmeras áreas - dentro e fora da matemática - os tornam um princípio organizador central da Matemática contemporânea. Um **grupo** consiste do conjunto de transformações que preservam o objeto inalterado e a operação de combinar duas dessas transformações aplicando-as uma após a outra. Tais grupos de simetria têm um importante papel em muitas disciplinas. Grupos de matrizes, por

exemplo, podem ser usados para compreender leis físicas fundamentais na Teoria da Relatividade e fenômenos em Química molecular. *Grupos* estão por trás de muitas estruturas algébricas, como **corpos** e **espaços vetoriais**, e são uma importante ferramenta para o estudo de **simetrias**. Por estas razões, a **Teoria de Grupos** é considerada uma área importante da matemática moderna, e tem muitas aplicações, até mesmo, por exemplo em física de partículas.

O conceito de grupo emergiu do estudo de equações de polinômios com **Évariste Galois** na década de 1830. Após contribuições vindas da teoria dos números e geometria, a noção de *grupo* foi generalizada e se consolidou por volta de 1870.

Além das propriedades abstratas, matemáticos estudam as diferentes maneiras em que um grupo pode ser expresso concretamente (as representações do grupo), tanto de um ponto-de-vista teorético quanto prático-computacional. Em particular, uma teoria bastante desenvolvida é a dos **grupos finitos**, que culminou com a classificação dos **grupos simples finitos**, completada em 1983.

Antes de definir o que é um **grupo**, são mostrados alguns conceitos fundamentais no contexto da álgebra abstrata, entre os quais podemos destacar uma definição para a estrutura de um **semi-grupo** (que pode ser comutativo), de um **monóide**, a noção de **elemento simetrizável** e de **elemento regular**, a definição de uma **estrutura de grupo** e o uso de uma **relação de ordem total** sobre os elementos de um **grupo**.

11.1 Propriedades dos Grupos

As seguintes propriedades são pertinentes à Teoria dos Grupos.

Definição (**Operação Associativa**):

Diz-se que uma operação $*$ sobre um conjunto E é associativa se, e somente se, a seguinte condição estiver verificada:

$\forall\, x, y, z \in E$ tem-se $(x * y) * z = x * (y * z)$

Definição (**Elementos Permutáveis**)

Seja uma operação $*$ definida sobre um conjunto E e sejam x e y dois elementos de E. Diz-se que x e y sáo *permutáveis* (*ou comutam*) se, e somente se, $x*y = y*x$.

Definição (**Operação Comutativa**)

Diz-se que uma operação $*$ sobre um conjunto E é *comutativa* se, e somente se, dois elementos quaisquer de E são permutáveis, isto é, $x * y = y * x$.

Definição (**Elemento Neutro**)

Seja "*"uma operação definida sobre um conjunto E; diz-se que um elemento e, de E, é elemento neutro para a operação "*", se , e somente se, $\forall\, x \in E$, tem-se $x * e = e * x$.

Se $E = \mathbb{N}, \mathbb{Z}, \mathbb{R}$ e se "*"for a operação "+"ou "."para estes conjuntos, temos que os elementos neutros para tais conjuntos são 0 e 1, para as operações "+"ou ".", de adição e multiplicação, respectivamente, pois $x + 0 = 0 + x$ e $x * 1 = 1 * x$.

Teorema (**Unicidade do Elemento Neutro**)

Se uma operação "*"definida sobre um conjunto E, tem elemento neutro, então esse elemento neutro é único.

Definição (**Estrutura de Semi-Grupo**)

Diz-se que uma operação "*"definida sobre um conjunto E, define uma estutura de semi-grupo sobre E se, e somente se, o seguinte axioma estiver verificado:

G1 (*Propriedade Associativa*): $\forall\, x, y, z \in E$, (x*y)*z = x*(y*z)

Ou seja, em um *semi-grupo* só há a propriedade associativa.

Definição (**Conjunto Fechado**)

Seja "*"uma operação definida sobre um conjunto E e seja A um subconjunto de E. Diz-se que A é fechado em relação à operação $*$ se, e somente se, $\forall\, x, y \in A$, tem-se que $x * y \in A$.

Definição: (**Elemento Simetrizável**)

Seja "*"uma operação definida sobre um conjunto E suponhamos que esta operação tenha um elemento neutro e, de E. Diz-se que um elemento $a \in E$ é simetrizável para a operação $*$ se, e somente se, $\exists\, a' \in E$ se, e somente se, tem-se $a * a' = e = a' * x$.

- O elemento a' de E é chamado de simétrico de a.
- O elemento neutro e é simetrizável.
- Indicaremos por $U(E)$ o conjunto de todos os elementos simetrizáveis de E para a operação "*".
- Se E é um monóide multiplicativo, então um elemento simetrizável é denominado elemento inversível, e seu simétrico a' é chamado inverso de a, ou inverso

multiplicativo, e indicado por a^{-1}. A expressão $a * x = e = x * a$ é, então, escrita sob a forma $a.a^{-1} = 1 = a^{-1}.a$.

- Se E é um monóide aditivo, então um elemento simetrizável é denominado elemento inversível, e seu simétrico a' é chamado oposto de a, ou inverso aditivo, e indicado por $-a$. A expressão $a * x = e = x * a$ é, então, escrita sob a forma $a + (-a) = 0 = (-a) + a$.

Teorema (**Unicidade de um elemento simétrico**)

Se a é um elemento simetrizável de um monóide $(E, *)$, então existe um único elemento $x \in E$ tal que $a * x = e = x * a$.

Teorema (**Elementos Simetrizáveis de um Monóide**)

Sejam a e b dois elementos simetrizáves de um monóide $(E, *)$. Então:

- se a' é o simétrico de a, então a' é simetrizável e seu simétrico é o próprio a.
- $a * b$ é simetrizável e seu simétrico é $b' * a'$, onde a' e b' são, respectivamente os simétricos de a e b.

Corolário do Teorema

Se E é um monoíde em relação a uma operação $*$, e seja $U(E)$ o conjunto de todos os elementos simetrizáveis de E para a operação "*". Então:

- O elemento neutro $e \in U(E)$.
- $U(E)$ é fechado em relação à operação $*$.
- O simétrico de todo elemento de $U(E)$ pertence a $U(E)$.

Teorema - Sejam a e b dois elementos permutáveis de um monóide $(E, *)$. Então:

1. se b é simetrizável, então a comuta com o simétrico b' de b.
2. se a e b são simetrizáves, então seus simétricos a' e b' são permutáveis.

Teorema - Se a e b são dois elementos quaisquer de um monóide $(E, *)$ e se b é simetrizável, então existem elemento x e y únicos, de E, tal que $b * x = a$ e $y * b = a$.

Nesta caso, temos que $x = b' * a = a * b'$, onde b' é o simétrico de b. Dependendo da operação $*$, $x = b' * a = a * b'$ tem um nome especial. Por exemplo, se $*$ for a operação multiplicatica, o único elemento x tal que $b * x = a$ é denominado **quociente** de de a por b, denotado por $a \mid b$ que é o mesmo que $\frac{a}{b}$.

Portanto, temos a definição $\frac{a}{b} = ab^{-1}$. E em particular, temos $b.\frac{a}{b} = a$, $\frac{b}{b} = 1$

e $\frac{1}{b} = b^{-1}$, quaisquer que sejam a e b em E, com b inversível (simetrizável).

A função $div : E \times U(E) : (a, b) \longmapsto \frac{a}{b}$ é denominada **divisão**.

No caso da operação de adição, o único elemento x tal que $b + x = a$ é denominada diferença entre a e b, o que é indicado por $a - b$. Portanto, po definição: $a - b = a + (-b)$, e em particular $b + (a - b) = a$, $b - b = 0$, $0 - b = -b$, quaisquer que sejam a e b em E, com b simetrizável.

A função $sub : E \times U(E) : (a, b) \longmapsto a - b$ é denominada subtração.

Definição (**Elementos regulares à esquerda e à direita**) (*Lei do Cancelamento*)

Diz-que um elemento a de um **semi-grupo** $(E, *)$ é **regular à esquerda** e **regular à direita** para a operação $*$ se, e somente se, está verificada a seguinte condição:

- quaisquer que sejam x e y em E, se $a * x = a * y$ (regular à esquerda).
- quaisquer que sejam x e y em E, se $x * a = y * a$ (regular à direita).
- um elemento regular à esquerda e à direita é chamado de **elemento regular**.
- um elemento regular é também chamado **elemento cancelável**. Lembra que em certas equações podemos cancelar elementos em ambos os lados de uma equação ?

11.2 Grupos Algébricos

Definição (**Estrutura de Grupo**)

Diz-se que uma operação "*"definida sobre um conjunto G, define uma estrutura de grupo sobre G se, e somente se, os seguinte axiomas estiverem verificados Monteiro (1969):

G1 (Propriedade Associativa): $\forall\, x, y, z \in E$, (x*y)*z = x*(y*z)

G2 (Existência de Elemento Neutro): $\exists\, e \in E$, tal que $\forall\, x \in E$, tem-se $x * e = e * x$.

G3 (Existência de Elemento Simetrizável): $\forall\, x, \exists\, x' \in G$ tal que $x * x' = e = x' * x$.

Se $*$ satisfaz ao axioma G4:

G4 Se G for comutativo temos a propriedade (Propriedade Comutativa): $\forall\, x, y \in G$, tem-se $x * y = y * x$. Diz-se que G é um **grupo comutativo**, também conhecido por **grupo abeliano**.

Definição (**Semi-Grupo Ordenado**)

Seja $(E, +)$ um **semi-grupo comutativo** e seja $\leq$ uma **relação de ordem** sobre o conjunto E. Diz-se que a operação de $+$ e a ordem $\leq$ são *compatíveis* se, e somente se, o seguinte axioma estiver verificado:

OA $\forall\, \forall\, x, y, z \in E$, se $x \leq y$, então $x + z \leq y + z$.

Neste caso, diz-se que $(E, +, \leq)$ é um *semi-grupo parcialmente ordenado*. Para este caso, valem os axiomas G1, G4, O1, O2, O3 e O4. Se o axioma O4 for verdadeiro, $(E, +, \leq)$ é um **semi-grupo totalmente ordenado**.

11.3 Exemplos de Grupos

- Considere que a operação "*" de um grupo G é a adição usual. Então, neste caso, temos $(G, +)$, onde o elemento neutro é o 0 e o inverso de a é representado por $-a$. Um exemplo de grupo aditivo é o conjunto dos inteiros $(\mathbb{Z}, +)$.
- O conjunto $(\mathbb{Z}_{\ltimes}, +)$, formado pelos números entre 0 e $n-1$, em que a soma é feita módulo n, é um grupo finito. Por exemplo, em $(\mathbb{Z}_{\not\geq\not\leq}, +)$ temos que $20+30$, não é 50, mas a soma é feita na artimética modular e dá como resultado, 8 (resto da divisão de 50 dividido por 42, que dá resto 8).
- O conjunto $\{1, -1\}$ é um grupo relativamente à multiplicação usual.
- O conjunto de todas as bijecções do conjunto $\{1, 2, 3, ..., n\}$ em si próprio é um grupo se se considerarar como operação binária a **composição**. Este grupo representa-se por S_n.
- O grupo de simetrias de um polígono regular de n lados, chamado Dn ou grupo diedral. Por exemplo, n é igual a 4, temos o caso do grupos das simetrias de um quadrado.

11.4 Grupo das Permutações

Seja o conjunto $U = \{1, 2, 3, ..., n\}$. Uma **permutação** em U, é uma função f tal que f é bijetora. O conjunto de todas as permutações em U é chamado de **conjunto das permutações** de n elementos. Uma **permutação** pode ser representada de forma matricial, montando uma matriz de forma que a primeira linha seja os elementos de U e uma segunda linha seja a representação de uma permutação desses elementos. Na segunda linha da matriz, troque os elementos nas posições das colunas e uma permutação surge. Na análise combinatória, a noção de grupo de permutação é frequentemente utilizados para simplificar a contagem de um conjunto de objetos.

Grupo de simetrias de um quadrado - Quando construímos polígonos regulares, podemos ordenar os seus vértices, para formar uma espécie de referência. Seja um polígono regular de ordem n, ao considerarmos apenas as diversas configurações que não alteram o formato do polígono - modificando, portanto, somente as posições de seus vértices - temos o conjunto diedral de ordem n (representado por D_n).

A **Teoria de Galois**, que é a origem histórica do conceito de **grupo**, procura descrever as simetrias das equações satisfeitas pelas soluções de uma equação polinomial. **Grupos abelianos** (comutativos) estão presentes em várias estruturas estudadas em álgebra abstrata, como em corpos algébricos.

Na topologia algébrica, grupos são usados para descrever os invariantes de espaços topológicos. Eles são chamados de "invariantes"porque não mudam se o espaço é submetido a uma transformação.

A compreensão da teoria de grupos é fundamental, também, na Física, onde é utilizada para descrever as simetrias que as leis da Física devem obedecer. O interesse da Física na representação de grupos é grande, especialmente nos grupos de Lie, pois suas representações podem apontar o caminho para "possíveis"teorias físicas. Em Química, grupos são utilizados para classificar estruturas cristalinas e a simetrias das moléculas.

O conceito de grupo é fundamental para a álgebra abstrata: outras bem conhecidas estruturas algébricas, como os anéis, corpos e espaços vetoriais, podem todas ser vistas como grupos dotados de operações e axiomas adicionais. Grupos ocorrem em todas as partes da matemática, e os métodos da teoria dos grupos influenciaram fortemente vários ramos da álgebra, e nos interessa neste livro, a sua aplicação à criptografia na área de segurança computacional da informação.

11.5 Curiosidades sobre a Teoria dos Grupos

Para ver o relacionamento com a **ciência da computação**, imaginemos na área da **computação gráfica**, o conceito de **transformações** - que são as formas de se classificar figuras geométricas - como por exemplo, girar uma figura em torno de seu eixo ou deslocá-la de um ponto no espaço a outro. Através do conceito de **transformações**, somos levados a conceito de **simetria**. A própria natureza, e mesmo as mais diversas construções do homem, estão repletas de exemplos contendo **simetria**. A ideia de **simetria** introduz uma das mais importantes ideias da matemática - **os grupos**. Assim, na forma poética que Nathan C. Carter colocou - **Teoria dos grupos** é o ramo da matemática que responde à questão "**O que é simetria?**". Seu estudo pode ser feito do ponto de vista das **transformações**. O estudo das **simetrias**, também tem a ver com o conceito de **regularidade** - a maneira que a matemática encontrou de preencher o espaço bidimensional (o plano) e o espaço tridimensional (o espaço que nos situamos).

Até bem pouco tempo, a simetria - um tipo especial de transformação - que, embora movendo um objeto, permite que ele permaneça o mesmo era uma busca indecifrável no campo da matemática. No entanto, no século XX, emergiu como elemento central das noções mais essenciais da física e da cosmologia. Ao escrever Uma história da simetria na matemática, o genial escritor e divulgador da ciência **Ian Stewart**, em Stewart (2012), conta de modo simples e atraente como uma sucessão de matemáticos e físicos, à procura de soluções para equações algébricas, acabou por construir uma teoria que revolucionou nossa visão sobre o Universo. Uma linha do tempo é construída que vai da antiga Babilônia à Física do século XXI. Um caminho cheio de histórias de matemáticos e suas buscas, como a de **Girolamo Cardano**, um italiano que "obteve" o método para solucionar as equações cúbicas e publicou o primeiro livro importante de álgebra. E **Evariste Galois**, revolucionário francês que morreu aos 21 anos, num duelo por causa de uma mulher, deixando inédita a teoria dos grupos, que viria a remodelar o modo de calcular a simetria. Um livro que nos revela, sobretudo, que a história da matemática depende das descobertas produzidas por pensadores persistentes e inconformados.

Em Janos (2009), o capítulo 5 aborda "**Estruturas**", onde estes conceitos são colocados com detalhes, e o assunto pode ser discutido em outro volume da coleção "**Matemática** & **Computação**".

Por exemplo, em duas dimensões, nosso problema é análogo ao problema de azulejar o espaço plano de uma parede, ou de assentar cerâmicas num piso, da forma que surgem desenhos harmoniosos, obedecendo um certo padrão. Procuramos identificar a maneira mais eficiente de preencher o espaço, por exemplo, no problema do empacotamento de discos, onde as maneiras mais óbvias de empacotar são a forma retangular e a forma hexagonal. **Gauss** provou que o empacotamento com a grade hexagonal é o mais denso de todas as formas de empacotamento, quando a disposição dos pontos forma uma **grade**. No plano, uma grade é um conjunto de pontos dispostos de uma maneira regular. Para formar uma grade, os pontos podem ser dispostos unidos formando quadrados, retângulos, hexágonos ou outras formas que mantenham algum padrão de regularidade.

Papéis de parede, são configurações simétricas desenhadas no plano. Existem várias possibilidades disponíveis que a computação nos dá para organizar figuras geométricas regulares, de forma a preencher uma parede. Para desenhar um papel de parede, o que se tem de fazer é escolher uma ou mais das possibilidades de padrões, aplicar um determinado número de transformações como translações, rotações e reflexões do ladrilho unitário, inserir uma padrão artístico no ladrilho, e ir preenchendo um pedaço do papel até que todo o papel estaja coberto.

Do ponto de vista da **Teoria dos Grupos**, um grupo de papéis de parede é obtido por transformações rígidas no plano (chamadas de isometrias), sendo que dois padrões (grupos) de papéis são iguais, se eles são obtidos pelas mesmas transformações afins,

como uma translação ou uma rotação no plano, não afetam o padrão do papel de parede. Um papel de parede pode ter milhares de padrões, mas aqui, não imaginemos que uma tigorosa classificação dos padrões possa ser feita. Não considerando as variações de cores, tamanhos, tipo do papel, entre outros detalhes, mas nos concentrando na estrutura básica, pode-se provar o fato surpreendente que existem somente 17 padrões de papéis de parede, ou seja existem 17 grupos de papéis de parede. Dizem que todos esses 17 padrões estão presentes nos objetos árabes Janos (2009).

11.6 Definindo um Corpo

Os axiomas que definem uma estrutura de um corpo comutativo. Seja um conjunto K que tem pelo menos dois elementos, e sobre esse conjunto estão definidas as operações de adição e multiplicação $(a, b) \longmapsto (a + b)$ e $(a, b) \longmapsto (a.b)$ que e que satisfazem aos seguintes axiomas.

Sejam a, b e c elementos quaisquer de A, então:

A1 : $(a + b) + c = a + (b + c)$	M1 : $(a.b).c = a.(b.c)$
A2 : $a + b = b + a$	M2 : $a.b = b.a$
A3 : $a + 0 = a$	M3 : $a.1 = a$
A4 : $a + (-a) = 0$	M4 : $a.a^{-1} = 1$
D : $a.(b + c) = a.b + a.c$	

Sejam a e b dois elementos quaisquer de um corpo K, com $b \neq 0$; como b é inversível, existe o quociente $\frac{a}{b} = a.b^{-1}$.

11.7 História da Teoria dos Corpos Álgébricos

Historicamente, em 1871, **Richard Dedekind** deu o nome de "corpo" a um conjunto de números reais ou complexos que são fechados para as quatro operações aritméticas. Em 1881, **Leopold Kronecker** definiu aquilo a que chamou "domínio de racionalidade", e que hoje é geralmente conhecido como "*corpo de polinômios*". Em 1893, **Heinrich Weber** deu a primeira definição clara de um *corpo abstrato*. Em 1910, **Ernst Steinitz** publicou o influente artigo *Algebraische Theorie der Körper* (**Teoria Algébrica dos Corpos**). Neste artigo ele estuda axiomaticamente as propriedades dos corpos e define conceitos importantes da teoria. **Évariste Galois** é reconhecido como o primeiro matemático a unificar a **teoria dos grupos** e a **teoria dos corpos**, originando a designação **Teoria de Galois**. No entanto, foi **Emil Artin** quem primeiro desenvolveu a **relação entre grupos e corpos** de forma mais desenvolvida e detalhada entre 1928-1942.

11.8 Exemplos de estrutura de Corpo

São exemplos mais conhecidos de **estruturas de corpo**:

- O conjunto $\mathbb{Q}$ dos **números racionais** é um corpo em relação às operações de adição e multiplicação, chamado de corpo dos números racionais.
- O conjunto $\mathbb{R}$ dos **números reais** é um corpo em relação às operações de adição e multiplicação, chamado de corpo dos números reais.
- O corpo dos **números algébricos**;
- O conjunto $\mathbb{C}$ dos **números complexos** é um corpo em relação às operações de adição e multiplicação, chamado de corpo dos números complexos

11.9 Corpos Finitos e Aritmética Modular

Definição (**Corpo Finito**)

Um **corpo finito** é um corpo em que o conjunto dos elementos é finito.

Exemplos: (**Corpos Finitos**)

Da aritmética modular, considere-se o conjunto de números que tem somente 3 números, tais como $\{0, 1, 2\}$. E sejam as operações de adição e multiplicação sobre este conjunto serem as mesmas como a adição e multiplicação ordinárias, com a seguinte exceção: se um número q, resultante de uma operação de adição e multiplicação, é igual ou excede a 3, esse resultado é para ser dividido por 3, o quociente é descartado, e o resto da divisão é usado no lugar de q. As Figuras 9 e 10 são duas tabelas que mostram os resultados da adição e da multiplicação sobre este conjunto, e são chamadas, respectivamente, **adição módulo 3** e **multiplicação módulo 3**.

Tabela 9 – Adição (mod 3)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Fonte: Deo (1974).

Similarmente, podemos definir qualquer sistema aritmético módulo m, consistindo de m elementos $\{0, 1, 2, ..., m-1\}$ e relacionando para qualquer $q > m-1$, donde: $q - m.p + r \pmod{m}$ e $r < m$.

Tabela 10 – Multiplicação (mod 3)

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Fonte: Deo (1974).

11.10 Corpos de Galois

Das tabelas nas Figuras 9 e 10, pode ser verificado que o conjunto $\{0, 1, 2\}$ com as operações de adição e multiplicação módulo 3 é um **corpo**. Existe o elemento identidade 0 para a adição módulo 3, e a identidade 1 para a multiplicação módulo 3. Todo elemento tem um único inverso aditivo e todo elemento diferente de 0 tem um inverso multiplicativo.

Por meio das tabelas como as Figuras 9 e 10, é facilmente mostrado que módulo 2, 5 e 7 são também corpos. Por outro lado, para o conjunto $\{0, 1, 2, 3\}$ com a adição e a multiplicação módulo 4, este não é um corpo, porque o inverso de 2 não existe para a multiplicação módulo 4.

Genericamente, de fato, para todo conjunto finito $\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}$ com a adição e multiplicação módulo m é um corpo, se, e somente se, m é um número **primo**. Tal corpo é chamado **Corpo de Galois** módulo m, denotado por $GF(m)$.

Um *corpo finito de Galois* é bastante útil na sua aplicação à criptografia. Um exemplo de algoritmo criptográfico que utiliza o corpo $GF(2^m)$) é o algoritmo **ElGamal**. Este algoritmo, na literatura de criptografia, é um sistema criptográfico para uso com **chaves assimétricas** (uma chave pública e uma chave privada) criado pelo egípcio **Taher Elgamal** em 1984. Sua segurança se baseia na dificuldade de solução que o **Problema do Logaritmo Discreto** pode apresentar. Neste algoritmo é suficiente que $GF(2^m)$ seja visto como um **grupo**, para que o *Problema do Logaritmo Discreto* faça aparecer a dificuldade computacional.

Vimos que **grupos** podem ser aplicados, através do **Problema do Logaritmo Discreto**, à criptografia de chave pública através do algoritmo de **ElGamal**. Mas, quais **grupos**? Um exemplo de grupos G para os quais o **Problema do Logaritmo Discreto** é computacionalmente inviável é um *Corpo finito de Galois*.

11.11 Bibliografia e Fonte de Consulta

MONTEIRO, L. H. J. - Elementos de Álgebra. IMPA. Ao Livro Técnico SA, Cap.2, pgs.22-23, 1969.

Michel Janos - Matemática e Natureza, Livraria da Física, 2009.

Narsingh Deo - Graph Theory with Applications to Engineering and Computer Science, Prentice-Hall, 1974.

James D. Stein - Como a Matemática Explica o Mundo - O poder dos números no cotidiano, Ed. Campus-Elsevier, 2008.

Grupos de Permutações - https://pt.wikipedia.org/wiki/Grupo_de_permutação

11.12 Referências - Leitura Recomendada

Teoria dos Grupos - https://pt.wikipedia.org/wiki/Teoria_dos_grupos

Teoria dos Corpos - https://pt.wikipedia.org/wiki/Teoria_dos_corpos

MONTEIRO, L. H. J. (1969) Elementos de Álgebra. IMPA. Ao Livro Técnico S.A.

https://pt.wikipedia.org/wiki/Número_algébrico

CAPÍTULO 12

Século XIX - Conjuntos e Enumeração

Em matemática, estamos interessados em abstrações, e na ciência da computação estamos mais interessados em representações de objetos matemáticos ou objetos físicos. *Conjuntos* são abstrações que permeiam toda a matemática, e consequentemente transpassam, também, o mundo da Ciência da Computação que vivemos.

Na matemática, como vimos no capítulo 3, vimos que nos *Axiomas de Peano*, usamos a palavra **número** várias vezes. Mas, o que são números? Normalmente, se responde a esta pergunta partindo da existência dos números naturais, que são parte dos números racionais, que são parte dos números reais, ..., como fizemos no capítulo 3.

Entretanto, usando-se a noção abstrata de *conjunto*, podemos explicar o que são **números**, não a partir dos números naturais, mas construindo a infinitude dos números naturais a partir de um conjunto que nada tem. Mais precisamente, a partir do **conjunto vazio** - o conjunto que não contém nenhum elemento. Este é um conjunto, que apesar de não ter nada, é importante, pois ele é um elemento de qualquer conjunto. Também não podemos falar de **um** conjunto vazio, pois a Teoria dos Conjuntos prova que o conjunto vazio é único.

Então, fazemos o seguinte:

- Defina o número 0 como sendo o conjunto vazio ϕ.
- 1 será definido como sendo um conjunto unitário - de um elemento - denotado por $\{\phi\}$.
- 2 será definido como sendo o conjunto $\{0, 1\}$.
- 3 será definido como sendo o conjunto $\{0, 1, 2\}$.
- ... ...

- n será definido como sendo o conjunto $\{0, 1, 2, ..., n\}$.

Esta é uma **definição axiomática**, pois não fornece os elementos de $\mathbb{N}$, mas descreve **propriedades** que dizem respeito aos elementos de $\mathbb{N}$.

12.1 Definição Axiomática

Como em Janos (2009), começamos com uma definição axiomática da Teoria dos Conjuntos, que pode prover as bases para tratar do entedimento da noção de infinito desenvolvida por Cantor. Também pode ser base para se entender a Teoria dos Conjuntos não Cantoriana, desenvolvida no século XX (ver Bertrand Russel), devido aos paradoxos encontrados na Teoria dos Conjuntos de Cantor.

O método axiomático usado no desenvolvimento de uma determinada teoria matemática ou lógica, se configura a partir de:

1. Termos indefinidos.
2. Relações indefinidas.
3. Axiomas relacionando os termos indefinidos com as relações indefinidas.

No desenvolvimento axiomático da Teoria dos Conjuntos, as noções de **conjunto** e **elemento** são termos indefinidos. Portanto, a relação "**elemento pertencente a um conjunto**"é uma relação indefinida. Para os nossos propósitos, o axioma da Teoria dos Conjuntos a ser destacado é:

Dois conjuntos A e B são iguais se, e somente se, eles tem os mesmos elementos, ou seja, se cada elemento de A pertence a B, e se cada elemento de B pertence a A.

Este axioma deve ser bem entendido, pois o conjunto $\{x_1, x_2, x_3\}$ é igual ao conjunto $\{x_1, x_2, x_3, x_1\}$, dado que ambos contém somente os elementos x_1, x_2 e x_3. Note que, também a **ordem** dos elementos no conjunto não importa.

A coleção como construída neste exemplo $\{x_1, x_2, x_3, x_1\}$, faz parte de uma outra teoria denominada *Bag Theory*, que pode ser usada para especificar sistemas de computação Spivey (1989), mas que extrapola o conteúdo deste livro.

Por causa dos conjuntos infinitos, a Teoria dos Conjuntos é uma matemática dos infinitos. Foi a partir desta teoria que **Cantor** chegou ao conceito de **número transfinito**, incluindo as classes numéricas dos **cardinais**. Aparentemente, conjuntos infinitos nada tem a ver com a Ciência da Computação. Mas, como veremos, posteriormente, o raciocínio com o infinito serve para provar certos fatos importantes para a Ciencia da Computação, como a **existência de funções não-computáveis** e a **existência de problemas indecidíveis**.

Um **número transfinito** é a forma rigorosa usada pela matemática para contar o número de elementos de conjuntos infinitos. **Georg Cantor** estudou sistematicamente o conceito de potência (tamanho) de um conjunto, e concluiu que:

(**Cantor**) - **"os conjuntos infinitos não são todos iguais"** (equipotentes).

Naquela época, pensava-se que todos os conjuntos de infinitos possuíam a mesma grandeza (**cardinalidade**), mas **Cantor** provou de forma conclusiva que isso não era verdade, pois:

"**a quantidade de números do conjunto dos reais $\mathbb{R}$ era maior do que a dos racionais $\mathbb{Q}$**"

Cantor dizia que os **números Reais** podiam ser subdivididos de duas maneiras:

- Como **Racionais** e **Irracionais**
- Como **Algébricos** e **Transcendentes**

Cantor demonstrou que o conjunto dos números algébricos possuem a mesma "potência"(tamanho, magnitude) dos números inteiros, então, são os transcendentes que dão a "densidade"que resulta em uma potência maior.

Foram essas observações de **Cantor** que levaram ao desenvolvimento da **Teoria dos Conjuntos**.

Cantor designou os **números cardinais infinitos** pela letra $\aleph$ - "aleph", primeira letra do alfabeto hebraico. E utilizou índices i para designá-los:

Ao conjunto dos **naturais** ele atribuiu o cardinal transfinito $\aleph_0$; este é um número infinito e, portanto, não há como compará-lo com um número natural.

Existem outros conjuntos com o mesmo "infinito"dos naturais, ou a mesma potência (**cardinalidade**) $\aleph_0$, como o conjunto dos números pares $\{0, 2, 4, 6, 8...\}$, o conjunto dos números ímpares $\{1, 3, 5, 7, 9, ...\}$, etc.

O conjunto dos pares tem "aparentemente"metade dos números existentes no conjunto dos números Naturais, ou seja $\frac{\aleph_0}{2}$. Mas como $\aleph_0$ é um "número infinito"então qualquer comparação com um número não diz nada, e portanto, $\frac{\aleph_0}{2}$ é infinito.

Os números racionais também possuem a mesma **cardinalidade** $\aleph_0$.

Podemos enumerar os racionais de forma $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, ...$ e eliminando os elementos que podem ser simplificados, então fazemos uma equivalência com os números **naturais** $\mathbb{N}$ mostrando que os **racionais** possuem uma cardinalidade.

Existem ainda diversos conjuntos que possuem o mesmo infinito, mas todos são feitos a partir da enumeração de números naturais.

Exemplo ($\mathcal{P}(\mathbb{N})$, **o conjuntos das partes de** $\mathbb{N}$ **não-contável**).

Então podemos fazer um conjunto $\mathcal{P}(\mathbb{N})$ em que cada elemento é um subconjunto dos naturais (o conjunto das partes). Se fossemos tentar ordenar esse conjunto segundo a soma dos elementos de cada subconjunto, não haveria forma de expressar os subconjuntos infinitos. Cantor conseguiu uma prova rigorosa de que este conjunto $\mathcal{P}(\mathbb{N})$ não pode ser enumerado, o que levou-o a propor o cardinal $\aleph_1$ para $\mathcal{P}(\mathbb{N})$.

O fato de um conjunto possuir o **cardinal** $\aleph_1$ significa que ele é um conjunto infinito e tal maneira que não pode ser colocado em correspondência bi-unívoca com o conjunto dos números naturais $\mathbb{N}$. A classe de todos os conjuntos equivalentes ao conjunto das partes dos números naturais define o número cardinal $\aleph_1$.

Cantor, portanto, conseguiu mostrar que **o conjunto das partes dos números naturais tem mais elementos que o conjunto dos números naturais**, mas não conseguiu mostrar que não existe um conjunto intermediário, ou seja, que **não existe um conjunto** X **que tem mais elementos que o conjunto dos números naturais e menos elementos que** $\mathcal{P}(\mathbb{N})$. Esta hipótese ficou conhecida na matemática como a **hipótese do contínuo**, e só foi resolvida adequadamente várias décadas depois.

Agora, se considerarmos o conjunto dos reais $\mathbb{R}$, este conjunto contém o conjunto dos números **inteiros**, **racionais** e **irracionais**. Mas, pode-se provar que ele **não** é equivalente ao conjunto dos naturais. Pode-se provar que o conjunto dos números reais $\mathbb{R}$ tem a mesma cardinalidade do conjunto das partes dos números naturais $\mathcal{P}(\mathbb{N})$, e então, segundo Cantor (e a hipótese do contínuo) sua cardinalidade é $\aleph_1$.

12.2 Conjuntos Contáveis e Não Contáveis

Esta parte é baseada em Sudkamp (1988). A seção apresenta a importante contribuição de **Georg Cantor**, que se usa para provar a existência de funções não computáveis e de problemas indecidíveis. Estes fatos, como serão colocados posteriormente no Capítulo 4 do Volume 2, são cruciais, diante das limitações descobertas sobre a computação e o computador, antes mesmo dessa máquina vir a existir. **Cantor** criou a base matemática, que depois foi usada para se provar tais limitações.

Cantor provou que os conjuntos infinitos não têm todos a mesma potência (potência significando "tamanho"). Fez a distinção entre conjuntos enumeráveis (em inglês chamam-se countable) - que se podem contar, e conjuntos contínuos (ou não-enumeráveis) (em inglês uncountable) - que não podem ser contados.

Provou que o conjunto dos números racionais $\mathbb{Q}$ é enumerável, enquanto que o conjunto dos números reais $\mathbb{R}$ é contínuo (logo, não-enumerável, e maior que o anterior). Foi ele quem utilizou pela primeira vez o símbolo $\mathbb{R}$ para representar o conjunto dos números reais. Na demonstração foi utilizado o mátodo da diagonal de **Cantor**.

Em 1897 foram descobertos alguns paradoxos suscitados pela teoria dos conjuntos. Apesar dos paradoxos encontrados na Teoria de Cantor, ela não foi desprezada, podendo ser pensada ou usada, hoje, como uma forma de se modelar o mundo em conjuntos.

Agora, é explicado o que são os conjuntos **contáveis** e conjuntos **não-contáveis** como em Sudkamp (1988).

Cardinalidade é a medida que compara os tamanhos de conjuntos. Intuititivamente, a **cardinalidade** de um conjunto é o número de elementos no conjunto. Esta definição informal é suficiente quando tratando-se com conjuntos finitos. No caso finito, a cardinalidade pode ser obtida por contar os elementos do conjunto. Mas, em se tratando de conjuntos infinitos, existem as dificuldades óbvias de se contar conjuntos infinitos e se estender esta abordagem.

Para dois conjuntos finitos pode ser mostrado ter o mesmo número de elementos por contruir um mapeamento um-a-um entre os elementos dos conjuntos.

Exemplo (**Conjuntos finitos de mesmo tamanho**)

Sejam os conjuntos $E = \{a, b, c\}$ e $F = \{1, 2, 3\}$. Para comparar estes dois conjuntos observe que estes são conjuntos finitos de mesma cardinalidade. Considere o mapeamento: $a \to 1$, $b \to 2$ e $c \to 3$. Isto mostra que os dois conjuntos E e F tem o mesmo tamanho (magnitude).

Esta abordagem do mapeamento funciona, igualmente, bem para conjuntos **finitos** ou **infinitos**.

Definição (**Conjuntos de mesma cardinalidade**)

- Dois conjuntos E e F tem a mesma cardinalidade, se existe uma função total um-a-um f, com $f : E \to F$.
- A cardinalidade de um conjunto E é menor ou igual a cardinalidade de um conjunto F, se existe uma função total um-a-um f, com $f : E \to F$.

A cardinalidade de um conjunto de um conjunto E é denotada por $card(E)$. As relações em (1) e (2) são denotadas $card(E) = card(F)$ e $card(E) \leq card(F)$, respectivamente.

A cardinalidade de E é dita ser estritamente menor que a cardinalidade de F e é denotada por $card(E) < card(F)$, se $card(E) \leq card(F)$ e $card(E) \neq card(F)$.

A cardinalidade de um conjunto finito é denotada pelo número de elementos no conjunto. Assim, $card(\{a, b, c\}) = 3$.

Um conjunto que tenha a mesma cardinalidade como o conjunto $\mathbb{N}$ é chamado **infinitamente contável** ou **enumerável**. O termo **contável** se refere a conjuntos que são **finito** ou **infinitamente contável**. Um conjunto que nao é **contável** é chamado de **não-contável**.

12.3 Conjuntos Infinitos

Definição (**Subconjunto**)

Em teoria dos conjuntos, quando todo elemento de um conjunto B é também elemento de um conjunto A dizemos que B é um subconjunto ou uma parte de A; e denotamos $A \subseteq B$.

Definição (**Subconjunto Próprio**)

Dizemos que um conjunto B é um subconjunto próprio de um conjunto A, se $B \subseteq A$ (B é subconjunto de A) e $B \neq A$ (B é diferente de A). Em particular, o conjunto vazio ϕ é um subconjunto próprio de todo conjunto não-vazio.

Definição (**Conjunto Infinito**)

Como em Sudkamp (1988), um conjunto é **infinito**, se ele tem um **subconjunto próprio** de mesma **cardinalidade**.

12.4 Funções

Dois tipos de funções são agora importantes: (a) *Função Total*, (b) **Função Parcial**. Embora, a matemática só considere funções totais, para a ciência da computação, as funções parciais existem em várias situações reais em certos estados dos sistemas de computação.

Definição (**Função Total**)

Sejam E e F dois conjuntos numéricos e seja f uma relação de E em F. Neste caso, f é um subconjunto do produto cartesiano de $E\ X\ F$. Diz-se que f é uma *função total* de E em F, se e somente se, estiverem verificadas as seguintes condições:

- A1 - $\forall\, x \in E$, $\exists\, y \in F$ tal que $(x, y) \in f$
- A2 - $\forall\, x, y, y'$, com $x \in E$, e y e y' em F, se $(x, y) \in f$ e $(x, y') \in f$ então $y = y'$.
- A3 - É imediato de A1 e A2 que, $\forall\, x \in E$, existe um único $y \in F$ tal que $(x, y) \in f$

Definição (**Função Parcial**)

Em computação é importante salientar o fato de que algumas funções não são definidas para todos os elementos do seu domínio (conjunto de entrada). Isto corresponde a situação do que é chamada uma *função parcial*. Caso em que alguns elementos do domínio de uma função, podem não corresponder a nenhum elemento no contra-domínio da função. Ou seja, a função comporta elementos do seu domínio, mas que não tem imagem no seu contra-domínio. Na prática da computação, isto tem cabimento, muito embora, no campo da matemática, não se valorize esta situação. No nosso contexto, sempre usaremos o termo função, no sentido da acepçãomais geral de função parcial.

Na ciência da computação, em vários contextos, funções são cidadãos de primeira classe. Em muitas partes deste livro aparecerão funções aplicadas às questões da ciência da computação, isto é, funções parciais.

Em resumo:

- De forma geral, se f é parcial, f não precisa estar definida para todo elemento de E.
- O dominio de f é o conjunto $dom(f) \subseteq E$, dos elementos em que f é definida.
- Se f é total, ela é definida para todo elemento de E.
- Toda função total, é um caso especial de uma função parcial.
- É importante salientar que o termo mais correto a ser tecnicamente usado, é *função não total* ou *função parcial não total*, porque a definição de função parcial não implica em restrição de domínio, como indicado no item anterior.
- Para funções totais define-se:
  1. f é injetiva (1-a-1), se $\forall\, x \in E, com x_1 \neq x_2, f(x_1) \neq f(x_2)$.
  2. f é sobrejetiva, se $\forall\, y \in F, \exists\, x \in E, tal\ que\ f(x) = y$.
  3. f é bijetiva, se f for injetiva e sobrejetiva.

Exemplo (**Conjunto infinitamente contável**)

O exemplo é de Sudkamp (1988). O conjunto $\mathbb{N} - \{0\}$ é **infinitamente contável**

Tabela 11 – Tabela: Números reais não enumeráveis

Linha	Representação do Número
0	$r_{0,0}\ r_{0,1}\ r_{0,2}\ r_{0,3}\ r_{0,4}\ \ldots$
1	$r_{1,0}\ r_{1,1}\ r_{1,2}\ r_{1,3}\ r_{1,4}\ \ldots$
2	$r_{2,0}\ r_{2,1}\ r_{2,2}\ r_{2,3}\ r_{2,4}\ \ldots$
3	$r_{3,0}\ r_{3,1}\ r_{3,2}\ r_{3,3}\ r_{3,4}\ \ldots$
4	$r_{4,0}\ r_{4,1}\ r_{4,2}\ r_{4,3}\ r_{4,4}\ \ldots$
5	$r_{5,0}\ r_{5,1}\ r_{5,2}\ r_{5,3}\ r_{5,4}\ \ldots$
6	$r_{6,0}\ r_{6,1}\ r_{6,2}\ r_{6,3}\ r_{6,4}\ \ldots$
...	... ...

Fonte: Prolo (2004).

(enumerável), pois pode-se considerar a função $f(n) = n + 1$ que define um mapeamento $f : \mathbb{N} \to \mathbb{N} - \{0\}$.

Pode ser paradoxal que o conjunto $\mathbb{N} - \{0\}$, obtido removendo-se o número 0 de $\mathbb{N}$, tenha o mesmo número de elementos de $\mathbb{N}$. Neste caso, claramente, *não existe* um mapeamento um-a-um de um conjunto finito sobre um **subconjunto próprio** dele próprio. É esta propriedade que diferencia conjuntos finitos de infinitos.

Exemplo Sudkamp (1988) (**Conjunto dos Naturais Ímpares**)

O conjunto do número naturais ímpares é **infinitamente contável**. A função $f(n) = 2n + 1$ estabelece uma função um-a-um entre $\mathbb{N}$ e o conjunto dos naturais ímpares.

Exemplo (**Pontos de uma grade infinita de duas dimensões**)

Pode ser mostrado, como em Sudkamp (1988), que o conjunto dos pontos de uma grade (em inglês, *grid*) infinita de duas dimensões é **infinitamente contável**. A grade é construída por rotular os eixos (duas dimensões) com os números naturais. A posição definida por linha i e coluna j é denotada pelo par ordenado $[i, j]$. Os elementos da grade podem ser listados sequencialmente. Isto pode ser visto na Tabela 11 seguinte:

Os elementos da grade podem ser listados sequencialmente, por considerar-se a seguinte correspondência

$0 \to [0,0],\ 1 \to [0,1],\ 2 \to [1,0],\ 3 \to [2,0],\ 4 \to [1,1],\ 5 \to [0,2],\ 6 \to [0,3],\ 7 \to [1,2]$ ...

o qual mostra que $\mathbb{N} \times \mathbb{N}$ é **infinitamente contável** ou **enumerável**.

O conjuntos de interesse na Teoria das Linguagens e na Teoria da Computabilidade são quase, exclusivamente, finitos ou infinitamente contáveis, o que é o mesmo

que enumeráveis.

Teorema (**Propriedades dos Conjuntos Contáveis**) Sudkamp (1988)

- A união de dois conjuntos contáveis é um conjunto contável.
- O produto cartesiano de dois conjuntos contáveis é contável.
- O conjunto de subconjuntos finitos de um conjunto contável é contável.
- O conjunto de sequências de comprimento finito consistindo de elementos de um conjunto contável não vazio é infinitamente contável (enumerável).

12.5 Enumeração

Enumeração é um conceito muito importante, pois a cadinalidade de um conjunto é dada pela comparação deste conjunto com outro que serve como referência. Além de se verificar a equivalência entre dois conjuntos. O conceito de **equivalência** é muito útil em ciência da computação. Por exemplo, no paradigma de programação orientada a objeto, objetos de uma mesma classe são equivalentes.

Tomando-se dois conjuntos A e B, dizemos que eles são **equivalentes** se a cada componente de A corresponder um único componente de B, e se cada componente de B, corresponder a um único elemento de A.

A equivalência em conjuntos finitos coincide com a noção de número de elementos. Mas, não é preciso saber o números de elementos para se saber se dois conjuntos são equivalentes.

Exemplo (**Conjuntos Equivalentes**)

Por exemplo, o conjunto de todas as cadeiras ocupadas em uma sala é **equivalente** ao conjunto de pessoas sentadas. A ideia de Cantor foi estender o conceito de equivalência de conjuntos finitos para conjuntos infinitos.

Formalmente, uma **enumeração** dos elementos de um conjunto E pode ser definida como:

- Um **mapeamento sobrejetivo** de $\mathbb{N}$ (os números naturais) a E. Essa definição é adequada para questões de **computabilidade** e **teoria dos conjuntos**.
- Um **mapeamento bijetor** de E para um segmento dos números naturais $\mathbb{N}$. Essa definição é adequada para questões de combinatória e conjuntos finitos. Assim, o início do segmento dos números naturais é $\{1, 2, ..., n\}$ para algum n que é a cardinalidade de E.

Cantor definiu que o **número transfinito** que representa o número de elementos de um conjunto enumerável é $\aleph_0$. Foi demonstrado por **Cantor** em 1874, que existem números cardinais acima de $\aleph_0$. **Cantor** usou um método que hoje é conhecido como *método da diagonal de Cantor* Sudkamp (1988).

Em ciência da computação, considera-se como um requisito adicional para **enumerações**, que o mapeamento de $\mathbb{N}$ para um conjunto E seja **computável**. Esse mapeamento é uma função, e nesse caso, diz-se que a função é computável. O conjunto E é então chamado **recursivamente enumerável**, referindo-se ao uso na Teoria da Recursividade (Teoria da Computabilidade) na formalização do que significa ao mapeamento ser **computável**.

Exemplos (**Conjuntos Enumeráveis**)

1. Os números naturais são enumeráveis pela função $f(n) = n$. Nesse caso, $f : \mathbb{N} \to \mathbb{N}$ é simplesmente a função identidade.

2. O conjunto $\mathbb{Z}$ dos números inteiros é enumerável. Seja a função $f : \mathbb{N} \to \mathbb{Z}$, tal que:

$$f(n) = -(n+1)/2, \text{ se } n \text{ é impar, e } f(n) = n/2, \text{ se } n \text{ é par.}$$

Esta função é uma **bijeção**, já que para cada número natural existe exatamente um número inteiro como imagem em $\mathbb{Z}$.

3. Todos os conjuntos finitos são enumeráveis.

4. Exemplo (**Conjunto Não-Enumerável**) - **Os números reais não possuem enumeração**, como provado pelo argumento de diagonalização de Cantor.

12.6 Propriedades da Enumeração

- Existe uma **enumeração** para um conjunto, somente se o conjunto for **contável**. Na matemática, um conjunto **contável** é um conjunto de **mesma cardinalidade** (número de elementos) de um subconjunto qualquer do conjunto dos números naturais. Um conjunto é dito não-contável quando ele não é contável. O termo foi criado por **Georg Cantor**. Os elementos de um conjunto contável podem ser contados um por vez, mesmo que a contagem nunca termine, e cada elemento do conjunto será eventualmente associado com um número natural.

- Se um conjunto é **enumerável** ele terá uma número infinito de diferentes enumerações, exceto nos casos de conjunto vazio ou conjuntos com um elemento.

Definição (**Recursivamente Enumerável**)

Na Teoria da Computação, um conjunto E é chamado **recursivamente enumerável** ou **parcialmente decidível** se:

- existe um **procedimento efetivo** que reconhece os elementos do conjunto E, para qual, o procedimento **pára**, e é exatamente o conjunto de números em E; e **não pára**, se o elemento não está em E. Esta primeira definição sugere porque o termo **parcialmente decidível** às vezes é usado.
- Ou, equivalentemente: Existe um procedimento que enumera os membros de E. Isso significa que sua saída é simplesmente uma lista de membros de E : $[e_1, e_2, e_3, ..., e_n, ...]$. Esta segunda definição sugere porque o termo **computavelmente enumerável** é usado.

Os **conjuntos recursivamente enumeráveis** são importantes na Teoria da Computação, no que tange a complexidade computacional, pois considera-se a classe de complexidade que contém todos conjuntos recursivamente enumeráveis.

12.7 Alguns conjuntos não-enumeráveis

Como em Prolo (2004), nas próximas seções mostramos alguns conjuntos não-enumeráveis importantes, utilizando método na seção 12.7.1. Ao final, pode-se concluir que a partir de resultados sobre **cardinalidade** de conjuntos, que:

- Existem funções não-computáveis.
- Existem problemas não-decidíveis (indecidíveis).

12.7.1 O conjunto dos Reais não-enumerável

O conjunto dos números reais $\mathbb{R}$ é **não-enumerável**.

Para provar este fato, vamos nos restringir aqui, por simplicidade, apenas ao intervalo (0,1]. É óbvio que $\mathbb{R}$ não pode ser menor do que (0,1].

1. A prova é por contradição (ou redução ao absurdo) e tem 7 passos. Primeiro assumimos como hipótese que o conjunto é enumerável. Ora, nós queremos provar exatamente o contrário, isto é, ao final concluímos que se tal hipótese for verdadeira chega-se a uma contradição, e portanto a hipótese não é verdadeira: o conjunto dos reais não é enumerável.

2. Ora, se o conjunto é enumerável por hipótese, então deve existir uma enumeração para ele (mesmo que nós não saibamos qual/como ela é): $r0, r1, r2, r3, r4, r5, r6$

3. Considere que todo número real pode ser representado em decimal com mantissa infinita. Alguns tem mantissa como $0.033333\ldots$, π, $\sqrt{abc}$. Mesmo os que tem mantissa finita, como 0.25, podem ser representados como $0.2499999\ldots$. Isto mostra

Tabela 12 – Tabela: Números reais não enumeráveis

Linha	Representação do Número
0	$r_{0,0}\ r_{0,1}\ r_{0,2}\ r_{0,3}\ r_{0,4}\ \ldots$
1	$r_{1,0}\ r_{1,1}\ r_{1,2}\ r_{1,3}\ r_{1,4}\ \ldots$
2	$r_{2,0}\ r_{2,1}\ r_{2,2}\ r_{2,3}\ r_{2,4}\ \ldots$
3	$r_{3,0}\ r_{3,1}\ r_{3,2}\ r_{3,3}\ r_{3,4}\ \ldots$
4	$r_{4,0}\ r_{4,1}\ r_{4,2}\ r_{4,3}\ r_{4,4}\ \ldots$
5	$r_{5,0}\ r_{5,1}\ r_{5,2}\ r_{5,3}\ r_{5,4}\ \ldots$
6	$r_{6,0}\ r_{6,1}\ r_{6,2}\ r_{6,3}\ r_{6,4}\ \ldots$
...	... ...

Fonte: Prolo (2004).

que representações com mantissa infinita (sem zeros não significativos à esquerda) tem correspondência bijetora (biunívoca) com os reais.

4. O diagrama abaixo mostra esquematicamente uma enumeração qualquer do intervalo $(0, 1]$, que deve existir de acordo com 2 acima. Cada linha representa um número. Cada número é uma sequência infinita de dígitos a partir do ponto decimal (Como estamos representando apenas o intervalo $(0, 1]$, antes do ponto decimal é sempre 0, que não é representado). O número $\pi/10$, por exemplo, seria representado como $31415\ldots$, e deve ser listado em uma linha $k \in \mathbb{N}$. $r_{k,0} = 3$, $r_{k,1} = 1$, $r_{k,2} = 4$, $r_{k,3} = 1$, $r_{k,4} = 5$, ... Na verdade, para todo número no intervalo $(0, 1]$ deve haver um $k \in \mathbb{N}$, tal que o número é representado na linha k da Tabela 12.

5. Imagine agora o número real x, cuja representação é: $x_0x_1x_2x_3x_4 \ldots x_l \ldots$. Este é construído da seguinte forma:

$x_0 = 9 - r_{0,0}$
$x_1 = 9 - r_{1,1}$
$x_2 = 9 - r_{2,2}$
$x_3 = 9 - r_{3,3}$
$x_4 = 9 - r_{4,4}$
... ...
$x_l = 9 - r_{l,l}$

Para cada $l \in \mathbb{N}$, o l-ésimo dígito de x após o ponto decimal é o complemento de 9 do l-ésimo dígito do número listado na linha l da enumeração.

6. A construção acima representa um número real no intervalo $(0, 1]$. Portanto, o número deve pertencer à enumeração, por exemplo numa linha $k \in \mathbb{N}$ qualquer. Mas pela definição o k-ésimo dígito de x é diferente do k-ésimo dígito desta linha. Ou seja, x não corresponde a nenhum dos elementos da enumeração. Isto é uma *CONTRADIÇÃO!* A hipótese original é, portanto, falsa.

7. OBSERVAÇÃO 1: O método de **Cantor**, acima, é chamado de *método da diagonal* porque o número x foi definido utilizando os elementos da diagonal $(r_{k,k})$ da tabela da enumeração da hipótese.

Como mostrado em Prolo (2004), a partir da contribuição de **George Cantor** sobre conjuntos **enumeráveis** e **não-enumeráveis**, pode-se mostrar resultados importantes para a **teoria da computabilidade**, sobre a **não computabilidade de funções** e os **problemas não-decidíveis**.

12.7.2 Problemas de Decisão

Um problema de decisão, é uma função total binária, cujo contradomínio tem apenas os valores $\{verdade, falso\}$ ou $\{0, 1\}$ ou $\{sim, nao\}$.

$$PD : U \to \{0, 1\}$$

12.7.3 Problemas Decidíveis

Um problema de decisão é dito ser **decidível**, se existe um procedimento efetivo P, tal que PD decide. Se a entrada do procedimento é x:

- se $x \in PD$, P gera como saída (1, verdade, sim).
- se $x \notin PD$, P gra como saída (0, falso, não).

O leitor deve notar que, isto é o mesmo que dizer que χ_{PD} é **computável**.

12.7.4 Funções não-enumeráveis

O conjunto de funções totais dos naturais para os naturais, como segue,

$F = \{f : \mathbb{N} \to \mathbb{N} \mid ftotal\}$ **é não-enumerável**.

1. Primeiro, note que ao provarmos que F é não-enumerável, provamos também que as **funções parciais** não o são, pois F é um subconjunto das parciais. O motivo da restrição para totais é por força do argumento que será utilizado abaixo.

2. O método é o mesmo usado acima. Primeiro assumimos como hipótese que o conjunto F é enumerável. Ora, nós queremos provar exatamente o contrário, isto é, ao final concluímos que se tal hipótese for verdadeira chega-se a uma contradição, e portanto a hipótese não é verdadeira: o conjunto das funções de $\mathbb{N}$ em $\mathbb{N}$ é não-enumerável.

3. Ora, se o conjunto é enumerável por hipótese, então deve existir uma enumeração para ele (mesmo que nós não saibamos qual/como ela é):

Tabela 13 – Tabela: Conjunto de funções não enumeráveis

Função	Argumentos
0	$f_0(0)$ $f_0(1)$ $f_0(2)$ $f_0(3)$ $f_0(4)$ ...
1	$f_1(0)$ $f_1(1)$ $f_1(2)$ $f_1(3)$ $f_1(4)$ ...
2	$f_2(0)$ $f_2(1)$ $f_2(2)$ $f_2(3)$ $f_2(4)$ ...
3	$f_3(0)$ $f_3(1)$ $f_3(2)$ $f_3(3)$ $f_3(4)$ ...
4	$f_4(0)$ $f_4(1)$ $f_4(2)$ $f_4(3)$ $f_4(4)$ ...
5	$f_5(0)$ $f_5(1)$ $f_5(2)$ $f_5(3)$ $f_5(4)$ ...
6	$f_6(0)$ $f_6(1)$ $f_6(2)$ $f_6(3)$ $f_6(4)$ ...
...	....

Fonte: Prolo (2004).

f_0, f_1, f_2, f_3, f_4, f_5, f_6

4. Duas funções f, g $(\in \mathbb{N})$ são iguais, se e somente se, elas são iguais para todo elemento do domínio; são diferentes, se e somente se, existe algum $x \in \mathbb{N}$ para o qual $f(x) \neq g(x)$. Podemos, portanto, representar uma tal função f como uma sequência infinita

$f(0), f(1), f(2), f(3), ...$

ou imagine o grafo de $f = \{(0, f(0)), (1, f(1)), (2, f(2)), (3, f(3)), ...\}$.

5. O diagrama abaixo mostra uma enumeração qualquer de F, que deve existir pela hipótese. Cada linha representa uma função. Cada coluna x corresponde ao valor da função aplicada a x. Para toda a função de F deve haver um $k \in N$ tal que a função é representada na linha k da Tabela 13.

6. Imagine agora a função $f \in F$, cuja representação $f(0)f(1)f(2)f(3)f(4)...f(l)...$ é construída da seguinte forma:

$f(0) = f_0(0) + 1$
$f(1) = f_1(1) + 1$
$f(2) = f_2(2) + 1$
$f(3) = f_3(3) + 1$
$f(4) = f_4(4) + 1$
$f(5) = f_5(5) + 1$
...
$f(l) = f_l(l) + 1$
...

Para cada $l \in N$, f é diferente da função f_l da linha l da enumeração, pois por construção, f é diferente de f_l quando aplicada ao argumento l $(f(l) = f_l(l) + 1)$.

Portanto, f não pertence à enumeração. Mas como $f \in F$, por hipótese, f pertence à enumeração. Novamente chegamos a uma contradição. A hipótese original é portanto falsa. F é não-enumerável.

12.8 Conclusões Importantes

CONCLUSÃO 1: **Existe função não-computável**. Vimos que o conjunto de todos os procedimentos efetivos em uma dada linguagem (ALGORITMOS) é **enumerável**. Mas o conjunto das funções F, tais que:

$F : \mathbb{N} \to \mathbb{N}$ sobre os naturais $\mathbb{N}$ **é não-enumerável**,

pois $card(F) > \aleph_0$. Portanto, não existe bijeção entre ALGORITMOS e F. Neste caso, não se tem como associar um procedimento efetivo para cada função. Ou seja, existem "mais"funções do que programas. Donde se conclui que existem funções não-computáveis (na verdade muitas!, infinitas!), isto é:

Existem "mais"**funções não-computáveis** do que **funções computáveis**.

CONCLUSÃO 2: **Existe problema não-decidível**.

1. Com argumento similar ao usado para o conjunto F das funções totais dos naturais para os naturais, pode-se mostrar o subconjunto de F, das funções totais binárias de naturais:

$$FB = \{f : N \to \{0, 1\} \| f \ total\}$$

também não é enumerável. Esta prova pode ficar como um exercício para o leitor.

2. Ora, FB é exatamente o conjunto dos **problemas de decisão** (definidos anteriormente) para os naturais. Em termos de conjuntos, FB representa o conjunto potência de $\mathbb{N}$ ($2^{\mathbb{N}}$, o conjunto de todos os subconjuntos de naturais). De fato, cada membro f de FB é a função característica de um subconjunto dos naturais.

3. Ou seja o número de problemas de decisão não é enumerável. Visto que ALGORITMOS é enumerável, novamente concluímos pela existência de (infinitos) problemas que não são decidíveis.

4. Note que $FB \subset F$, portanto o fato de que FB não é enumerável por si só implica que F também não é.

CONCLUSÃO FINAL:

- **Existem funções matemáticas que não podem ser computadas** (não podem ser expressas por procedimento efetivo, um algoritmo).

- **Problemas que não podem ser decididos** por computador.
- **Conjuntos que não podem ser enumerados** por programa de computador.

12.9 Números Contáveis e Números Computáveis

Nesta seção, estamos tratando de conjuntos infinitos: *infinitamente contável*, o que é o mesmo que *enumerável*. Quando um conjunto possui o mesmo tamanho dos naturais $\mathbb{N}$, dizemos que ele é um conjunto contável (Aleph-zero, $\aleph_0$). Porém nem todos os conjuntos são contáveis, como o conjunto dos números Reais $\mathbb{R}$, provado pelo método de diagonalização (ver em Sudkamp (1988)), ou seja, podemos dizer que o infinito dos Reais $\mathbb{R}$ é maior que o infinito dos naturais $\mathbb{N}$.

Mas se o conjunto dos números Reais $\mathbb{R}$ é composto pelo conjunto dos Racionais $\mathbb{Q}$ e Irracionais $\mathbb{I}$, e foi provado que os Racionais $\mathbb{Q}$ possuem o mesmo tamanho dos Naturais $\mathbb{N}$, então podemos afirmar que quem faz a diferença na contagem são os números Irracionais $\mathbb{I}$. Mas, que Irracionais $\mathbb{I}$ fazem essa diferença? Existem vários tipos deles também. Alguns irracionais são construídos como raízes de polinômios com coeficientes inteiros, chamados de *irracionais Algébricos*.

Porém, pela mesma técnica de **Godel** (ver o capítulo 15), podemos provar que os Irracionais algébricos também são contáveis, associando cada coeficiente do polinômio a um expoente de um número primo. Já que os *Irracionais algébricos* são contáveis, quem faz a diferença são justamente os irracionais não-algébricos, chamados transcendentes. Mas, mesmo dentre os *transcendentes*, existem diferentes tipos, como o número π, por exemplo, que não podemos ter ele como raiz de um polinômio, mas podemos aproximá-lo tão precisamente quanto desejemos por meio de um algoritmo. Números dessa forma são chamados *Computáveis*.

Mas ainda podemos provar que os *Computáveis* também são contáveis. Fazemos isso provando que se existe um algoritmo que aproxima o número (chamado computável), então esse algoritmo pode ser implementado numa linguagem (mostrado por Turing). Mas como existem contáveis codificações em uma linguagem finita, então existem contáveis números Computáveis.

Então, quem são os não-contáveis? Existem números que não podemos gerar por meios de algoritmos, por exemplo: a *constante de Chaitin*. Resumidamente, podemos construir calculando o seguinte somatória: para cada algoritmo existente (cujo natural associado é n), se o algoritmo pára, soma-se $2 - n$, senão, não soma nada. Como a somatória não pode ser calculada porque não podemos saber se um algoritmo pára (Problema da Parada), então a *constante de Chaitin* é um número não-computável. Em ciência da computação, na sub-área de teoria da informação algorítmica, a constante de **Chaitin** (número Ômega de Chaitin) ou probabilidade de parada é um número real que informalmente representa a probabilidade de que um programa construído de forma aleatória irá parar. Estes números são formados

de uma construção de **Gregory Chaitin**.

Então quais números fazem os números Reais serem um infinito maior que o dos números naturais? São os números que não podemos construir, não podemos aproximar e não podemos descrever, ou seja, nem dá pra pensar sobre eles.

12.10 Definições Recursivas

Muitos dos conjuntos envolvidos na geração de linguagens contém um número infinito de elementos. Precisamos definir um conjunto infinito em uma maneira que permita seus membros serem construídos e manipulados.

Uma **definição recursiva** de um conjunto X especifica um método para construir os elementos do conjunto. A definição utiliza dois componentes: os elementos-base e o conjunto finito de operadores. A base consiste de elementos explícitos projetados como membros de X. Os operadores são usados para construir novos elementos do conjunto, a partir dos membros definidos previamente. O conjunto X gerado recursivamente consiste de todos os elementos que podem ser gerados a partir da base, por um número finito de aplicações dos operadores.

A palavra-chave aqui é *gerar*. Claramente, nenhum procedimento pode listar o conjunto completo dos números naturais $\mathbb{N}$. Qualquer número natural, contudo, pode ser obtido começando-se do 0 e construindo a sequência inicial dos números naturais. Isto, intuitivamente, descreve o procedimento de gerar recursivamente os números naturais. Esta ideia é formalizada pela seguinte definição recursiva, como em Sudkamp (1988).

Definição (**Geração recursiva dos números naturais** $\mathbb{N}$)

Uma **definição recursiva** de $\mathbb{N}$ é construída usando a função-sucessor s, tal como em SUDKAMP (1988):

1. Base: $0 \in \mathbb{N}$,
2. Etapa recursiva: Se $n \in \mathbb{N}$, então $s(n) \in \mathbb{N}$,
3. Fecho: $n \in \mathbb{N}$, se ele pode ser obtido a partir do 0, por um número finito de aplicações da função s.

Definição (**Definição recursiva da soma de naturais**)

A definição recursiva da soma de m e n é feita sobre n, o segundo membro da soma: SUDKAMP (1988)

1. Base: Se $n = 0$, então, $m + n = m$,

2. Fecho: $m + n = k$ somente se esta igualdade pode ser obtida de $m + 0 = m$, usando-se finitamente várias aplicações da operação em (2).

12.11 Bibliografia e Fonte de Consulta

Janos, M. Matemática e Natureza, Livraria da Física, 2009.

Sudkamp, Thomas A. Languages and Machines: an introduction to the Theory of Computer Science, Addison-Wesley, 1988.

Prolo - https://www.inf.pucrs.br/ prolo/Disciplinas/07I/TComp590/aula19.08.04.pdf

12.12 Referências - Leitura Recomendada

Hércules de Araújo Feitosa; Mauri Cunha do Nascimento; Alexys Bruno Alfonso. Teoria dos Conjuntos - Sobre a Fundamentação Matemática e a Construção de Conjuntos Numéricos. Ciência Moderna.

Constante de Chaitin - https://pt.wikipedia.org/wiki/Constante_de_Chaitin

Números - https://pt.wikipedia.org/wiki/Números

CAPÍTULO 13

A Aritmética nos Séculos XIX e XX

A necessidade do formalismo na Aritmética não era apreciada até o trabalho de **Hermann Günther Grassmann** (1809-1877), que mostrou em 1861, que muitos fatos da aritmética poderiam ser derivados de fatos mais básicos sobre a operação de *sucessor* e o conceito de *indução*.

Figura 79 – Hermann Grassmann - A primeira formulação axiomática da aritmética.

Fonte: pt.wikipedia.org.

13.1 Teorias Axiomatizadas da Aritmética

Teorias Axiomatizadas da Aritmética são apresentados neste capítulo. De forma semelhante a várias outras teorias da matemática, apesar de ser extensivamente utilizada há bastante tempo, só foi formalizada no século XIX. A formalização mais conhecida é a feita através de um conjunto de axiomas conhecidos como axiomas de **Peano**, os quais foram propostos em 1889 pelo matemático italiano **Giuseppe**

Peano. É importante ressaltar que a aritmética usual utiliza a semântica da lógica clássica (podendo ser tanto de primeira-ordem, como de ordens superiores). Esta aritmética é conhecida como aritmética de Peano e é comumente abreviada como PA (*Peano Arithmetic*). Para tal precisamos conhecer algumas construções que correspondem à teorias aritméticas.

Grassmann expôs a primeira fórmula axiomática da aritmética, usando amplamente o princípio de *indução*. Seus seguidores citaram amplamente seu trabalho. Em 1881, **Charles Sanders Peirce** mostrou uma forma de axiomatização da aritmética de números naturais. Em 1888, **Richard Dedekind** propôs uma coleção de axiomas sobre os números, e em 1889, **Giuseppe Peano** publicou uma versão mais precisamente formulada das anteriores, em uma coleção de axiomas no seu livro, "Os principios da Aritmética apresentados por um novo método"(Em Latim: *Arithmetices principia, nova methodo exposita*).

Quando **Peano** formulou seus axiomas, a linguagem da lógica matemática ainda era nova. O sistema de notação lógica por ele criado para a apresentação de seus axiomas não se mostrou popular, apesar de ser a gênese da notação moderna de pertencimento ($\in$, derivado do ϵ utilizado por **Peano**) e implicação ($\supset$, derivado do "C"invertido de **Peano**). Ele manteve uma distinção clara entre a simbologia lógica e a matemática, o que não era ainda comum na matemática; tal separação foi introduzida pela primeira vez no *Begriffsschrift*, trabaho de **Gottlob Frege** no capítulo **??**, publicado em 1879. **Peano** desconhecia o trabalho de **Frege** e independentemente recriara suas técnicas lógicas se baseando nos trabalhos de *Boole* e **Schröder**. Os **axiomas de Peano** definem as propriedades aritméticas de números naturais, geralmente representadas como o conjunto $\mathbb{N}$ ou a assinatura (os *símbolos não-lógicos* de uma linguagem formal) para os axiomas incluem o símbolo de constante 0 e o símbolo de função-unária *sucessor*. Ver no Capítulo 3, quando foram apresentados os vários conjuntos de números mais usados.

A partir da *notação lógica* de **Peano**, um sistema axiomático para a aritmética, pôde ser construído através de **axiomas lógicos** da lógica de primeira ordem e mais axiomas aritméticos descritos na forma da álgebra.

Mais tarde, em 1929, **Mojzesz Presburger** (1904-1943), um matemático, lógico e filósofo polonês de origem judaica, aluno de **Alfred Tarski**, ficou conhecido, quando ainda estudantepor, por ter inventado a *aritmética de Presburger*. Formalmente, são bem conhecidas as aritméticas de **Peano** e **Presburger**.

13.2 Sobre a Aritmética de Peano

Os axiomas de **Peano** contêm três tipos de declarações. O primeiro axioma afirma a existência de pelo menos um membro no conjunto "números". As quatro seguintes são afirmações gerais a respeito de igualdade. Os próximos três axiomas são declarações

da lógica de primeira ordem sobre números naturais expressando as propriedades fundamentais da operação de *sucessor*. O nono e último axioma, é uma declaração da lógica de segunda ordem do *princípio da indução matemática* sobre os **números naturais**. Um sistema de primeira ordem mais "fraco"chamado **aritmética de Peano** é obtido ao adicionar os símbolos de adição e multiplicação e substituir o axioma de indução de segunda ordem, por um esquema axiomático de primeira ordem.

Quando **Peano** formulou seus axiomas, a linguagem da lógica matemática ainda era nova. O sistema de notação lógica por ele criado para a apresentação de seus axiomas não se mostrou popular, apesar de ser a gênese da notação moderna de pertencimento ($\in$, derivado do ϵ utilizado por **Peano**) e implicação ($\supset$, derivado do "C"invertido de **Peano**). Ele manteve uma distinção clara entre a simbologia lógica e a matemática, o que não era ainda comum na matemática; tal separação foi introduzida pela primeira vez no *Begriffsschrift*, trabalho de **Gottlob Frege** (Capítulo 8), publicado em 1879.

Peano desconhecia o trabalho de **Frege** e independentemente recriara suas técnicas lógicas se baseando nos trabalhos de *Boole* e **Schröder**. Os **axiomas de Peano** definem as propriedades aritméticas de números naturais, geralmente representadas como o conjunto $\mathbb{N}$ E os *símbolos não-lógicos* para os axiomas, incluem o símbolo da constante 0 e o símbolo de função unária *sucessor*. Ver no Capítulo 3, quando foram apresentados os vários conjuntos de números mais conhecidos.

Os axiomas de Peano também podem ser derivados de construções *conjunto-teóricas* de números naturais e axiomas da Teoria dos Conjuntos como a de **Zermelo-Fraenkel**. A construção padrão dos naturais, devido a **John von Neumann** (também contribuiu para a Teoria dos Conjuntos), começa com a definição de 0 (zero) como o conjunto vazio , e um operador s nos conjuntos, definido como:

$s(a) = a \cup \{a\}$.

O conjunto dos números naturais $\mathbb{N}$, também pode ser definido como a intersecção de todos os conjuntos fechados sob s que contém o conjunto vazio. Cada número natural é igual (como conjunto) ao conjunto de números naturais menor que ele:

$$
\begin{aligned}
0 &= \emptyset \\
1 &= s(0) = s(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\} \\
2 &= s(1) = s(\{0\}) = \{0\} \cup \{\{0\}\} = \{0, \{0\}\} = \{0, 1\} \\
3 &= ... = \{0, 1, 2\}
\end{aligned}
$$

Figura 80 – O conjunto dos números naturais $\mathbb{N}$ é definido como a interseção de todos os conjuntos fechados.

e assim em diante. O conjunto $\mathbb{N}$, junto com 0 e a função sucessor $s : \mathbb{N} \to \mathbb{N}$ satisfaz os axiomas de Peano.

A *aritmética de Peano*, que é uma aritmética dotada da operação de multiplicação, **não é decidível**, isto é, não existe um procedimento efetivo, que decide se qualquer declaração dada na aritmética de Peano é verdadeira ou falsa. Pelo teorema da incompletude de Gödel (ver no capítulo 15), a aritmética de Peano é **incompleta** e sua **consistência** não é demonstrável internamente, como o leitor conhecerá no Teorema 2 de Gödel.

13.3 Sobre a Aritmética de Presburg

Aritmética de Presburger é a teoria de primeira-ordem dos **números naturais** com a opração de *soma*. Tem esse nome em honra de **Mojzesz Presburger**, o qual a apresentou em 1929. A aritmética de **Presburguer** contém apenas a operação de *adição* e *equalização*, suprimindo a operação de *multiplicação* totalmente. Isso inclui o esquema de indução matemática sobre o números naturais, mostrada no Capítulo **??**. A aritmética de **Presburger** é muito mais fraca do que aritmética de **Peano**, que inclui tanto a operação de *adição* quanto a de *multiplicação*. Ao contrário da aritmética de Peano, a aritmética de Presburger é uma *teoria decidível*. Isto significa que é possível efetivamente determinar, por qualquer sentença na **linguagem da aritmética de Presburger**, se essa sentença é dedutível dos axiomas da aritmética de Presburger. A propósito do tempo de funcionamento assintótico da complexidade computacional deste problema de decisão, esse é duplamente exponencial, como mostrado por **Fischer** e **Rabin** (1974) (ver o capítulo "Sobre a Teoria da Complexidade", no segundo volume da série, intitulado "Da Computabilidade Formal às Maquinas Programáveis).

A linguagem da *aritmética de Presburger* contém constantes 0 e 1 e a função binária "+", interpretada como *adição*. Nessa linguagem, os axiomas da aritmética Presburger tem as propriedades:

(1) $\neg(0 = x{+}1)$ (2) $x{+}1 = y{+}1 \to x = y$ (3) $x{+}0 = x$ (4) $(x{+}y){+}1 = x{+}(y{+}1)$

Se $P(x)$ for uma fórmula de primeira ordem na linguagem da aritmética de Presburger, então a fórmula segue um axioma:

(5) $(P(0) \wedge \forall\, x(P(x) \to P(x+1))) \to \forall\, yP(y)$

O ítem (5) é um esquema de *axioma de indução*, o que representa um número infinito de axiomas. Uma vez que os axiomas no esquema em (5) não podem ser substituídos por qualquer número finito de axiomas, a aritmética de Presburger não é *finitamente axiomatizable*. A aritmética de **Presburger** não pode formalizar conceitos tais como a *divisibilidade* ou *números primos*. Geralmente, qualquer conceito de *número* levando a multiplicação não pode ser definida na aritmética de Presburger, uma vez que leva à incompletude e indecidibilidade. No entanto, pode-se formular

exemplos individuais de divisibilidade, como, por exemplo, se revelar "para todo x, existe y: $(y+y=x)\vee(y+y+1=x)$". Isto indica que cada número é par ou ímpar.

Presburger provou que sua aritmética é: (a) **consistente**: não há nenhuma declaração na aritmética de Presburger que pode ser deduzida a partir dos axiomas de tal forma que sua negação pode também ser deduzida; (b) **completo**: para cada operação na aritmética de **Presburger**, ou é possível deduzi-la a partir dos axiomas ou é possível deduzir a sua negação; (c) **decidível**: existe um procedimento efetivo, que decide se qualquer declaração dada na aritmética de Presburger é verdadeira ou falsa. Estes trës conceitos serão abordados nos capítulos 14 e 15 e no segundo volume, no capítulo intitulado "Turing - A Computação sem Computador".

Mojzesz Presburger provou que a sua aritmética é: (1) **consistente**: Não há nenhuma declaração na aritmética de Presburger que pode ser deduzida a partir dos axiomas de tal forma que sua negação pode também ser deduzida; (2) **completa**: Para cada instrução na aritmética de Presburger, ou é possível deduzi-la a partir dos axiomas ou é possível deduzir a sua negação; (3) **decidível**: Existe um procedimento efetivo, que decide se qualquer declaração dada na aritmética de Presburger é verdadeira ou falsa.

13.4 Uma Aritmética de Primeira Ordem

Em Carnielli e Epstein (2005), Parte III, Lógica e Aritmética, o capítulo 20, trata da construção da *aritmética de primeira ordem*. O apresentando em (A): uma **linguagem formal para a aritmética** na p.235, uma aritmética de primeira ordem.

Definição (**Uma definição não-construtiva de Aritmética**)

Uma **aritmética** é a coleção de todas as *fórmulas bem-formadas* na linguagem apresentada, em que são verdadeiras a respeito dos números naturais.

Em (B), Capítulo 20, p.237, temos os **princípios de inferência e axiomas lógicos**. Além disso, em (C), Cap.20, p.240, é apresentado o **sistema axiomático** chamado Q, constituído de um *axiomas lógicos* e *regras de inferência* e, mais *sete axiomas aritméticos*, formando um particular *fragmento da aritmética* de primeira ordem, construído acrescentando-se à parte (B), alguns axiomas específicos para a aritmética.

13.4.1 Prova de consistência e verdade em Q

Supondo a interpretação padrão. Neste caso, o simbolismo foi projetado para fazer referência aos números naturais, onde + é interpretado com a operação de adição, "."como a operação de multiplicação, e ""como a operação sucessor.

Tendo em mente esta interpretação, afirmarmos que uma *fbf* (*fórmula bem-formada*)

é verdadeira nos números naturais. E mais, se as hipóteses de uma regra são verdadeiras, então também é a sua conclusão. Portanto, todos os teoremas de Q são, imaginamos, verdadeiros sobre os números naturais.

Como **Hilbert** fazia, não se considera questões de veracidade e significado enquanto estudamos as propriedades sintáticas de um sistema formal. Em vez, disso, é assumido de forma explícita que o sistema Q tem a propriedade sintática de ser *consistente*: ou seja, *não existe uma fórmula bem formada* A, *desta aritmética, tal que* $\vdash_Q A$ e $\vdash_Q \neg A$ se verifiquem simultaneamente.

Algumas provas em Q de propriedades da *igualdade* - Note, que na linguagem da aritmética e nos axiomas, faz parte o símbolo de igualdade "=". Em Carnielli e Epstein (2005) são provados dois teoremas a respeito de propriedades da igualdade. Ver no Capítulo 20, p.242-244.

13.4.2 A Debilidade de Q

Como em Carnielli e Epstein (2005), se tivermos assumido o suficiente sobre os números naturais, para podermos representar toda *função recursiva* em Q, então este sistema deveria ser poderoso o suficiente para demonstrar *quase* todas as propriedades básicas da aritmética. Mas, um fato bem simples quanto $x \neq x'$ não pode ser demonstrado em Q. Como então podemos demonstrar este fato? Sabemos como demonstrar que uma sentença é um teorema. Basta exibir a prova. Mas, como se pode argumentar que *não existe* uma prova?

13.4.3 Provas sobre Q como Procedimentos Computáveis

Em Carnielli e Epstein (2005), Cap.22, seção A, é provado que Q é indecidível. Isto é, não existe procedimento de decisão para o conjunto de teoremas de Q e, assim, podemos concluir pela *indecidibilidade da aritmética de primeira ordem* baseada em Q. O que então, se pode afirmar? O que se pode provar é que:

- **Teorema** *Se* Q *é consistente, então* Q *é recursivamente indecidível.*
- **Corolário** Se Q é consistente, então assumindo-se a tese de Church, Q é indecidível.

13.5 Fragmentos de Aritmética

Por *fragmentos de aritmética*, podemos entender a aritmética definida com a linguagem em Carnielli e Epstein (2005), mas modificada sem o símbolo funcional "."da *multiplicação*. Um outro exemplo de fragmeto de aritmética é a mesma aritmética, mas definida sem os símbolos funcionais "+"para *adição*, e ""para *sucessor*. Alternativamente, se mantivermos a mesma linguagem original em Carnielli e Epstein (2005) e eliminarmos um dos sete axiomas Q1-Q7, que foram acrescentados para

formar o sistema Q, e assumindo que temos a consistência, não poderemos mais representar todas as funções recursivas. Deste modo, Q (modificado) será o mais simples fragmento da aritmética, que poderemos estar interessados.

13.6 Provas de Consistência

Mas, do ponto de vista genérico, a prova de *consistência* é uma prova matemática de que uma determinada teoria axiomática é *consistente*. O desenvolvimento inicial da teoria da prova matemática foi impulsionado pelo desejo de fornecer provas de consistência finitárias para toda a matemática como parte do programa de **Hilbert**. Mas, o programa de **Hilbert** foi fortemente impactado pela teoremas da incompletude de Gödel, que mostraram que teorias de prova suficientemente fortes não podem provar sua própria consistência (desde que eles são de fato consistente). O leitor verá no Capítulo 15, o teorema que Gödel provou sobre a incompletude da axiomática consistente da aritmética em seuTeorema 1 (de Gödel).

13.7 Bibliografia e Fonte de Consulta

Carnielli e Epstein - Computabilidade, Fun;óes Computáveis,, Lógica e os Fundamentos da Matemática, Unesp, 2005.

Dirk J. Struik - História Concisa das Matemáticas, Ed. Gradiva, 1987.

Florian Cajori - Uma História da Matemática, Ed. Ciência Moderna, 2007

Aritmética - ⟨https://pt.wikipedia.org/wiki/Aritmetica⟩

Euclides - Os Elementos, 1 ed. São Paulo: Editora Unesp, 2009.

Serre, Jean-Pierre - A Course in Arithmetic (em inglês). New York: Springer, 1973. 115 p. ISBN 978-0-38790040-7

Garbi, Gilberto Geraldo - A Rainha das Ciências: Um passeio histórico pela maravilhoso mundo da matemática. 3 ed.

Aritmética de Presburger - ⟨https://pt.wikipedia.org/wiki/Aritmetica_de_Presburger⟩

Axiomas de Peano - ⟨https://pt.wikipedia.org/wiki/Axiomas_de_Peano⟩

Mojzesz Presburger, 1929, "*Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*", in Comptes Rendus du I congrès de Mathématiciens des Pays Slaves, Warszawa: 92-101.

13.8 Referências e Leitura Recomendada

Plofker, Kim (autor do capítulo);Katz, Victor J. (editor). The Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook. New Jersey: Princeton University Press, 2007. Capítulo: Mathematics in India. , 712 p. ISBN 978-0-69111485-9

Alencar Filho, Edgard de. Teoria Elementar dos Números. 3ª ed. São Paulo: Nobel, 1992. 386 p. p. 68-83;116-136. ISBN 85-213-0040-9

Karlson, Paul. A Magia dos Números. Porto Alegre: Globo, 1961. Capítulo: Os Gregos, 608 p., p. 80-154.

Ifrah, Georges. História Universal dos Algarismos: A Inteligência dos Homens Contada pelos Números e pelo Cálculo. Rio de Janeiro: Nova Fronteira. 735 p. p. 162-180; 346-354; 404-409. 2 vol. vol. 1. ISBN 85-209-0841-1

Rudman, Peter Strom. How Mathematics Happened: The First 50,000 Years. Amherst, New York: Prometheus Books, 20007. p. 64. ISBN 978-1591024774

Florian Cajori - Uma História da Matemática, Ed. Ciência Moderna, 2007

Paulo Roberto Martins Contador - Matemática: uma Breve História, Vol 1-3, Ed. Livraria da Física, 2005-2008.

John A. Fossa (organizador) et al. - Matemática e Medida: Três Momentos Históricos, Livraria da Física, 2009.

James D. Stein - Como a Matemática Explica o Mundo: O poder dos números no cotidiano, Elsevier, 2008.

CAPÍTULO 14

Hilbert - Formalismo e Sistemas Axiomáticos

No século XVIII, **Leibniz** (1646-1716) desejava em sua época, dar uma visão matemática da lógica de **Aristóteles**. **Leibniz** acreditava que para resolver todos os problemas da cooperação humana bastaria uma **linguagem universal** e um **cálculo do raciocínio**, que ele chamou de (*calculus ratiocinator*). **Leibniz** desenvolveu uma técnica pela qual todo raciocínio poderia ser resolvido a um cálculo matemático. Proposições poderiam ser estabelecidas e provadas com um número pequeno de símbolos. É o que chamamos hoje de **Lógica Proposicional** e o **Cálculo Proposicional**.

Em razão de divergências nos próprios fundamentos da matemática, surge no final do século XIX e início do século XX, o matemático alemão **David Hilbert** (1862-1943), numa busca intensa para resolver qual a melhor forma de ver a matemática (e a lógica) e contornar várias outras dificuldades.

Figura 81 – David Hilbert - O precursor dos sistemas formais.

Fonte: ⟨https://pt.wikipedia.org/wiki/David_Hilbert⟩.

No final do século XIX, **Hilbert** tentou desenvolver uma formulação **completa** e **consistente** da matemática, na qual sentenças poderiam ser estabelecidas e provadas com um pequeno número de símbolos. Assim surgiu a parceria entre a Lógica e a Matemática, que foi chamada de **Lógica Simbólica** Janos (2009). Tal **completude** da matemática significava que **tudo que fosse verdadeiro poderia ser provado**. Mas, também precisava que a matemática fosse **consistente**, o que significava que **tudo que fosse provado seria verdadeiro**.

14.1 O Formalismo de Hilbert

No decorrer dos capítulos foram mostradas as várias corrente filosóficas, cada qual indicando os fundamentos da matemática, de que forma deveria ser a matemática quanto as formas de provas. Cada corrente defendia sua maneira de fazer as demosntrações matemáticas. Dentre estas correntes, interessa-nos, neste capítulo, o entendimento da corrente *formalista* liderada por **Hilbert**. A posição filosófica de **Hilbert**, a respeito dos fundamentos da matemática é chamada de *formalismo* Carnielli e Epstein (2005). Ele foi o criador e principal representante do formalismo. **Hilbert** fundou um escola com vários adeptos. Entre os mais famosos estudantes de **Hilbert** estavam **Ernst Zermelo** (quem formalizou a Teoria dos Conjuntos de Cantor), **John von Neumann** (o arquiteto do computador digital e criador da teoria dos autômatos), **Haskell Curry** (o criador da linguagem funcional Haskell) e vários outros seguidores, como por exemplo, **Herbrand** que focalizamos sobre a metamatemática (a linguagem que fala da matemática). Bastante conhecido na França e com forte influência no Brasil, é o grupo de matemáticos de concepções hilbertianas que escreve sob o nome de *Nicholas Bourbaki*.

O formalismo nasceu do progresso alcançado pelo chamado *método axiomático*. Na ciência da computação, quando se pensa em construir sistemas, esses precisam ser especificados e aí entra a ideia dos métodos de especificação *construtivos* (baseados em álgebra) e dos métodos de especificação *axiomáticos* baseados na Lógica. Também, junto com a aparição do computador digital, sistemas formais tiveram grande importância na construção da dos modelos de computação, quanto ao uso da Lógica, da Álgebra e do Cálculo, na criação das várias linhas de pesquisa da Ciência da Computação, e estes sistemas formais serão explicados mais rigorosamente neste livro no Capítulo 17 Costa (2008).

Segundo **Hilbert**, para se estudar uma teoria pelo método axiomático, escolhe-se certo número de **noções primitivas** (axiomas) aceitas sem demonstração, mais **proposições primitivas**, não interessando se são evidentes ou não (aceitas sem demonstração) e, as **proposições demonstradas** (por meio de raciocínio logicamente corretos a partir das regras de inferência), suficientes para edificar a teoria, aceitando-se outras proposições mediante, definições e demonstrações. Deixa-se de

lados os *significados* intuitivos dos conceitos primitivos. De modo geral as lógicas dedutivas fundamenta-se de acordo com o método em questão Costa (2008).

O *método axiomático* encontra aplicação praticamente em toda a matemática e lógica, constituindo-se hoje, na técnica básica destas ciências. A filosofia formalista transforma o método axiomático, de técnica que é, na essência da matemática e da lógica. **Hilbert**, ao contrário dos logicistas, não desejava reduzir a matemática à lógica, mas fundamentar a matemática e a lógica em bases sólidas. O matemático ou o lógico pode estudar as propridades dos objetos (na ciência da computação, um objeto pode ser um sistema de computação), somente por meio de símbolos do albabeto de uma linguagem com características formais (sintaxe), independentes dos significados que por ventura se possam atribuir aos símbolos. Este assunto será focalizado no capítulo **??**. Os formalistas afirmam, apenas, que o matemático e o lógico investiga as propriedades estruturais dos símbolos (e, portanto, de todos os objetos), independentemente de suas significações Costa (2008).

Hilbert pretendia reduzir o infinito, por um sistema formal de prova, livre de contradições, cuja validade dessas sentenças pudesse ser provada por **meios finitos**. Para **Hilbert**, o matemático pode estudar qualquer sistema simbólico, admitindo-se que o sistema não encerre contradições, isto é, no sistema axiomático não se possa provar uma proposição e, ao mesmo tempo, sua negação. Este é o princípio da "não-contradição". Tal ausência de contradição se chama **consistência** da teoria, no sentido de que "tudo que pode ser provado seja verdadeiro". Segundo **Hilbert**, basta provar a consistência de uma teoria, para torná-la inteiramente lícita. **Hilbert** edificou até uma meta-teoria, a **metamatemática** ou teoria da demonstração, cuja finalidade básica seria demonstrar a consistência das diversas teorias matemáticas.

Hilbert apostou na criação de uma linguagem puramente sintática, *sem significado*, a partir da qual se poderia deduzir a respeito da veracidade ou falsidade de enunciados. Isto deu surgimento ao que se chama hoje, de um *sistema formal*: uma linguagem e um sistema dedutivo. Tal linguagem formou a concepção **formalista** da matemática. Grande parte da comunidade matemática mundial acreditava na existência de uma matemática segura, provadamente correta e livre de inconsistências. Ledo engano.

Hilbert criou uma forma de se provar a consistência de uma teoria. A prova de consistência de uma teoria A pode ser reduzida à consistência de outra teoria, digamos B, da seguinte maneira: dentro da teoria B, elabora-se um *modelo* de A, ou seja, escolhe-se um sistema conveniente, S, de objetos de B, de tal forma que para esse sistema sejam satisfeitas as proposições primitivas de A; S constitui, assim, um *modelo* da teoria A. Então constata-se, como consequência, que se B for consistente, A também o será. Embora a consistência possa ser provada por meio da *teoria de modelos*, muitas vezes é feito de uma forma puramente sintática. Para entendimento deste fato, precisamos entender os teoremas de **Gödel** no Capítulo 15.

Na lógica dedutiva clássica, uma *teoria consistente* é aquela que não contém contradição. A ausência de contradição pode ser provada tanto em termos semânticos ou sintáticos. A definição semântica de que uma teoria é *consistente* é se, e somente se ela tem um *modelo*, ou seja, existe uma interpretação segundo a qual todas as fórmulas na teoria são verdadeiras. Este é o sentido usado na lógica aristotélica tradicional. A definição sintática afirma que uma teoria é *consistente* se, e somente se não existe uma fórmula P tal que P e sua negação $\neg P$ sejam demonstráveis a partir dos axiomas da teoria sob o seu sistema dedutivo associado.

Se essas definições sintáticas e semânticas são equivalentes, para qualquer teoria formulada usando uma lógica dedutiva particular, a lógica é chamada *completa*. A *completude* do cálculo proposicional foi provado por **Paul Bernays** em 1918 [3] e **Emil Post** em 1921 [4], enquanto a completude do cálculo de predicados foi provado por **Kurt Gödel** em 1930 [5]. E provas de consistência para a aritmetica, restritas ao *axioma da indução* foram provadas por **Ackermann** (1924), **von Neumann** (1927) e **Herbrand** (1931) [6]. Lógicas mais fortes em expressividade, como a lógica de segunda ordem, não são *completas*.

Veja as notas sobre os fatos históricos referidos anteriormente:

1 **Alfred Tarski** (1946) afirma que: "A teoria dedutiva é chamado consistente ou não contraditórias, se nenhuma duas declarações desta teoria se contradizem", ou em outras palavras, "se de quaisquer duas sentenças contraditórias, pelo menos uma não pode ser provada", onde **Tarski** define contraditório como segue: "... duas sentenças, das quais a primeira é uma negação do segunda, são chamados sentenças contraditórias". Esta definição requer uma noção de "prova". **Gödel** (1931) define a noção da seguinte maneira: "a classe de fórmulas demonstráveis é definida como sendo a menor classe de fórmulas que contém os axiomas e é fechada sob a relação de *consequência lógica imediata*, isto é, uma fórmula c decorrente de a e b é definida como uma consequência imediata em termos de uma regra *modus ponens*, conforme **Gödel** (1931) e **van Heijenoort** (1967). **Tarski** define "prova", informalmente, como "declarações se sucedem em uma ordem definida de acordo com certos princípios ... e por considerações destinadas a comprovar a sua validade, isto é, uma conclusão verdadeira para todas as premissas verdadeiras **Reichenbach** (1947). **Tarski** (1946), **Kleene** (1952) definem a noção de *prova*, em relação a qualquer uma indução sobre uma sequência finita de fórmulas, de tal modo que cada fórmula na sequência é, ou um axioma ou uma "consequência imediata"das fórmulas anteriores; a *prova* é dita ser uma prova da sua última fórmula, e esta fórmula é dita ser formalmente provável, ou ser um teorema demonstrável (formalmente), como **Kleene** (1952).

2 *Lógica Paraconsistente* tolera contradição, mas a tolerância à contradição não implica em consistência.

3 **van Heijenoort** (1967) afirma que **Bernays** determinou a independência dos axiomas de *Principia Mathematica*, um resultado não publicado até 1926, mas ele nada diz sobre **Bernays** provando sua consistência.

4 **Post** prova a consistência e a completude do cálculo proposicional; comentários de **van Heijenoort** e **Post** (1931) sobre à *introdução de uma teoria geral da proposições elementares* (1967), como também **Tarski** em (1946).

5 Comentário de **van Heijenoort** e **Gödel** (1930), sobre a *Completude dos Axiomas da Lógica como Cálculo Funcional* em **van Heijenoort** em 1967.

6 Comentário de **van Heijenoort** e **Herbrand** de 1930, sobre a consistência da aritmética em *van Heijenoort* 1967.

14.2 O Trabalho de Hilbert

Em 1900, o matemático alemão **David Hilbert** lançou, no *II Congresso Internacional de Matemática*, em Paris, um desafio aos matemáticos da época. Ele reuniu uma lista de 23 problemas da matemática em aberto, e convocou uma união de esforços para que se buscasse a solução daqueles problemas. Alguns problemas relacionavam-se com áreas mais gerais da matemática, mas a maioria desses estavam ligados aos fundamentos lógicos desta ciência. **Hilbert** imaginava tais problemas proporcionando um programa de pesquisas e sendo focalizados pela comunidade matemática mundial da época. **Hilbert** queria unir a comunidade para se chegar a uma visão de um sistema matemático livre de inconsistências.

Este episódio foi muito importante na busca pela fundamentação rigorosa da matemática. Naquela época, os matemáticos e filósofos se sentiam incomodados com a existência de problemas cuja falsidade ou veracidade, até então, não haviam sido provadas. A presença de problemas supostamente verdadeiros ou supostamente falsos permeando todo aparato matemático representava uma ameaça ao rigor matemático que se buscava.

14.3 Os Problemas Importantes para a Ciência da Computação

Dos 23 problemas matemáticos, propostos por **Hilbert**, destacam-se o de número 2, que estava relacionado com a confiabilidade do raciocínio matemático. Ou seja:

Problema 2 (Consistência): "**Se ao seguir as regras de um raciocínio matemático (dedução num sistema formal), não se poderia chegar a contradições.**"

E ligado ao problema 2, o problema 10, que enunciava:

Problema 10 (Decisão): "**Descreva um procedimento efetivo que determinasse que uma equação polinomial do tipo** $P(u_n, u_{n-1}, ..., u_1, u_0) = 0$**, onde** P **é um polinômio com coeficientes inteiros, tem solução (raízes) dentro do conjunto dos números inteiros.**"

Surge, então, com **Hilbert**, o importante **problema da decidibilidade**.

Este, consiste em indagar se existia um *procedimento efetivo* (mecânico) para determinar, **"se todos os enunciados matemáticos verdadeiros poderiam ser ou não provados".**

Isto é, se poderiam ser deduzidos a partir de um conjunto de premissas (hipóteses). Este é o *problema de decisão em matemática* e corresponde ao problema da **completude** de um sistema formal.

Mais tarde, este tipo de problema surgiu novamente nas pesquisas de **Alan Turing**, como será explicado no Capítulo 4 do Volume 2. Na realidade, **Turing** se inspirou nas ideias de **Hilbert**, como será contado posteriormente.

Sobre a questão da **consistência**, também importante para **Hilbert**, era uma condição necessária para a ideia de sistema axiomático que ele tinha em mente. **Aristóteles**, em seu tempo, já havia demonstrado que se um sistema é *inconsistente*, qualquer enunciado poderia ser provado como verdadeiro ou falso. Neste caso, não poderia haver algum fundamento científico sólido, para qualquer tipo de conhecimento matemático ou não. **David Hilbert** em 1920, prenunciado no famoso discurso que ele deu em 1900, fundou a abordagem "*formalista*" em Filosofia da Matemática.

Hilbert defendeu em 1921, que o objetivo principal dos pesquisadores da matemática e da lógica fosse o estabelecimento de matemática e lógica, sobre uma base sólida e comprovadamente *consistente* de axiomas, a partir do qual, em princípio, todas as verdades matemáticas poderiam ser deduzidas, pelos métodos padrão de primeira ordem ou lógica dos "predicados").

Hilbert acreditava na matemática como um **sistema formal**, organizado por um conjunto de símbolos, um número pequeno de **axiomas**, juntamente com um sistema dedutivo composto de regras. O sistema axiomático seria **completo**, no sentido de que tudo que é verdadeiro possa ser provado pelo sistema axiomático. E também, **consistente**, no sentido de que tudo que é provado será verdadeiro.

Então, em 1928, ele formulou sua ideia sobre o "*Entscheidungsproblem*" ou "**problema de decisão**" em matemática. Este problema originou o termo "*decidibilidade*".

14.4 Consistência, Completude e Decidibilidade

Aqui podemos ver estes três fatos distintos de interesse de **Hilbert**.

1. Em primeiro lugar, a **consistência**: o conjunto de axiomas deve ser comprovadamente consistente: tudo que é dedutível é verdadeiro.
2. Em segundo lugar, **completude**: todas as verdades matemáticas devem, em princípio, ser dedutíveis a partir dos axiomas.
3. Em terceiro lugar, **decidibilidade**: deve haver um procedimento claramente formulado, tal que, dada qualquer afirmação matemática no sistema axiomático, tal procedimento pode estabelecer definitivamente, dentro de um tempo finito ou não, se essa afirmação é dedutível a partir dos axiomas.

Nos tratamentos formais dessas noções, elas são interpretadas sintaticamente (ou seja, em termos de relações estruturais entre as fórmulas) ao invés de semanticamente (ou seja, em termos de verdade e significado). Assim entendido:

Definição (**Consistência**)

Um sistema **consistente** é aquele em que nunca é possível provar, ao mesmo tempo (com os mesmos axiomas), uma proposição P e sua negação não P. Porque se pudermos provar, encontaremos uma **contradição**.

Nunca é possivel provar P **E** provar não P.

Definição (**Completude**)

Um sistema **completo** é aquele em que é sempre possível provar P ou não P, para qualquer proposição P que pode ser expressa dentro do sistema.

É possível provar P **OU** provar não P, para qualquer P verdadeiro.

Então, **consistência** e **completude** estão intimamente relacionados, e pode ser entendida de forma totalmente independente da questão de:

"*Se os axiomas são ou não verdadeiros*" e "*as regras são válidas*" (ou seja, preservando a verdade).

Se, no entanto, formos capazes de alcançar um sistema **consistente** e **completo** da aritmética, *com axiomas verdadeiros e regras válidas*, então qualquer proposição aritmética seria demonstrável, se e somente se, ela é verdadeira.

Definição (**Decidibilidade**)

Poderia um procedimento eficaz ser concebido, que demonstrasse, em um tempo

finito, se qualquer proposição matemática dada, era ou não, dedutível de um dado conjunto de axiomas? Se tudo fosse resolvido assim, uma grande parte do objetivo de **Hilbert** seria realizado!

No esforço dos matemáticos da época, as pesquisas queriam mostrar que a matemática era: **consistente**, **completa** e **decidível**. De 1900 a 1930 (inicio do século XX), a matemática estava centrada sobre três sistemas axiomáticos: a **aritmética**, a **análise matemática** (Análise é o ramo da matemática que lida com os conceitos introduzidos pelo cálculo diferencial e integral, medidas, limites, séries infinitas e funções analíticas) e a **teoria dos conjuntos**. **Hilbert** propôs a demonstrar a consistência (coerência) da **aritmética**, para posteriormente estender tal consistência (coerência) no contexto dos demais sistemas axiomáticos. Para provar tal consistência da aritmética é preciso que se entenda o que vem a ser uma **aritmética**.

Kurt Gödel era um discípulo de **Hilbert** e trabalhava num dos seus grandes projetos: demonstrar a consistência dos axiomas da aritmética, para estabelecer de uma vez, que pelo menos este ramo das matemáticas estava para sempre livre de toda contradição interna. **Hilbert** baseava-se na formulação da aritmética e de suas proposições pelos símbolos de uma linguagem formal da aritmética.

Considerava-se o conjunto de todas as proposições corretamente formadas na linguagem formal da aritmética, incluindo as operações correntes de adição, subtração, multiplicação, divisão inteira (com resto inteiro) e exponenciação. Considerava que todos os axiomas necessários ali figuravam em boa ordem. O problema que se tratava em resolver era mostrar que toda proposição do conjunto podia-se atribuir um valor de verdade único por meio de uma demonstração, isto é, de uma sequência finita de implicações lógicas (ou consequências lógicas) que tivessem origem nos axiomas Omnes (1996).

As matemáticas de hoje repousam inteiramente numa base axiomática. Fundamentam-se num sistema de símbolos sem relação direta com a realidade (não considera a semântica desses simbolos) e submetido as suas próprias regras, cuja característica dominante é uma completa submissão à lógica, também simbolizada e formalizada Omnes (1996). Por exemplo, a aritmética se preocupa com as operações sobre os números naturais, as custas de seus axiomas aritméticos (envolvendo operações aritméticas), mas para se provar propriedades sobre esses números e operações, precisa-se da lógica, com seus axiomas lógicos. O importante nas matemáticas é construir provas, e os axiomas da lógica em que essas se fundamentam são supostamente os mais fundamentais.

Os axiomas são considerados absolutamente gerais, conhecidos por intuição ou por tê-los extraídos da acumulação dos fatos. A corrente *formalista* então, se baseia na concepção *logicista* desenvolvida por **Bertrand Russel** (1872-1970) e **Alfred North Whitehead** (1861-1947), que se esteia no *método axiomático* e, as vezes, é esquematizada dizendo-se que a matemática se reduz à lógica Omnes (1996). Mas,

para os formalistas as matemáticas são inteiramente redutíveis à manipulação de símbolos. Assim, em meados do século XX, a axiomática tal como fora formulada por **Hilbert** e codificada pelos livros de **Bourbaki**, torna-se dominante e, também, muito relevante na concepção dos sistemas formais em que a ciência da computação se fundamenta. As matemáticas não nos interessam aqui por si mesmas, mas sim, por seus significados para as áreas da ciência da computação.

14.5 Outras Contribuições de Hilbert

Hoje, o nome de **Hilbert** é muitas vezes mais lembrado através do conceito de **espaço de Hilbert**. **Irving Kaplansky** Kaplansky que fez grandes contribuições para a *teoria dos anéis*, *teoria dos grupos* e *teoria de corpos*, escrevendo sobre ele, explica o trabalho de **Hilbert**:

*O trabalho de **Hilbert** em equações integrais por cerca de 1909, levou diretamente à investigação no século XX, sobre análise funcional (o ramo da matemática em que as funções são estudados em conjunto). Este trabalho também estabeleceu a base para seu trabalho no espaço de dimensão infinita, mais tarde chamado **espaço de Hilbert**, um conceito que é útil na análise matemática e **mecânica quântica**. Fazendo uso de seus resultados em equações integrais, **Hilbert** contribuiu para o desenvolvimento da física matemática por suas memórias importantes sobre a teoria cinética dos gáses e da teoria da radiação.*

Suas contribuições à matemática são diversas:

- Consolidação da *teoria dos invariantes*, que foi o objeto de sua tese.
- Transformação da *geometria euclidiana em axiomas*, com uma visão mais formal que Euclides, para torná-la consistente, publicada no seu Grundlagen der Geometrie (Fundamentos da geometria).
- Trabalhos sobre a *teoria dos números algébricos*, retomando e simplificando, com a ajuda de seu amigo Minkowski, os trabalhos de **Kummer**, **Kronecker**, **Dirichlet** (1805-1859) e **Dedekind**, e publicando-os no seu *Zahlbericht* (Relatório sobre os números).
- Criação dos espaços que levam seu nome, durante seus trabalhos em análise sobre equações integrais.
- Contribuição para as formas quadráticas, base matemática da **teoria da relatividade** de **Albert Einstein**.

A partir de 1933, **Hilbert** vivenciou o fim da dinastia matemática da Universidade de Göttingen, quando Adolf Hitler assumiu o poder na Alemanha, tendo então os nazistas afastado a maior parte dos membros da faculdade. Quando **Hilbert** faleceu em 1943, os nazistas tinham praticamente acabado com a universidade, uma vez que

muitos de seus membros eram judeus, ou casados com judeus.

Em 1934 e 1939 foram, ainda, publicados dois volumes de *Grundlagen der Mathematik*, que tinham a intenção de levar a uma "teoria da prova", sobre a **consistência** da matemática, que **Gödel**, em 1931, mostrou que seu objetivo era e é, impossível.

Entre seus estudantes famosos, estavam vários nomes, mas para nossos propósitos, destacam-se **Ernst Zermelo** que formalizou as ideias geniais de Cantor sobre a Teoria dos Conjuntos , e **John von Neumann**, quem o leitor conhecerá no próximo capítulo sobre O Legado de von Neumann, no volume II.

Enfim, o melhor de **Hilbert** para a ciência da computação foi sua contribuição, de forma indireta, sobre o que procurava para respostas dos seus problemas 2 e o 10, contribuindo sobre a ideia de sistemas formais para a matemática, que proporcionou a **John von Neumann**, **Kurt Gödel** (capitulo 15 e **Allan Turing** (capitulo **??**, trabalharem essas questões, muito bem aproveitadas para os fundamentos da ciência da computação na Teoria da Computabilidade.

Talvez a melhor contribuição para a matemática tenha sido os **espaços de Hilbert**. Esses são uma generalização do espaço euclidiano que não precisa estar restrita a um número finito de dimensões. É um espaço vetorial dotado de produto interno, ou seja, com noções de distância e ângulos. Os espaços de **Hilbert** permitem que, de certa maneira, noções intuitivas sejam aplicadas em espaços funcionais (de funções). **Os espaços de Hilbert são de importância crucial para a Mecânica Quântica.**

Os elementos do **espaço de Hilbert** abstrato são chamados vetores. Em aplicações, eles são tipicamente *sequências funções*. **Espaços de Hilbert** desempenham um papel fundamental em toda a Física Quântica e em várias áreas da Matemática. Em Mecânica Quântica, por exemplo, um sistema físico é descrito por um espaço de Hilbert complexo (números complexos) que contém os vetores de estado, e todas as informações do sistema e complexidades multifocais. Por isto, forma a base matemática de qualquer pesquisa em direção ao estudo da **criptografia quântica**. Para os pretendentes em criptografia quântica, aqui é dada a definição de um **espaço de Hilbert**.

Um **espaço de Hilbert** é um espaço vetorial $\mathcal{H}$ sobre o corpo dos complexos $\mathbb{C}$ e dotado de um produto escalar $u,\ v \in \mathcal{H} \mapsto \langle hu \rangle \in \mathbb{C}$. $\mathcal{H}$ é dito ser um **espaço de Hilbert**, se for completo em relação à métrica d definida por esse produto escalar:

$$d(u,v) = \|u - v\| = \sqrt{\langle u - v, u - v \rangle}, \text{ onde } u,\ v \in \mathcal{H}.$$

Hilbert recebeu muitas honrarias. Em 1905, a *Hungarian Academy of Sciences* deu uma citação especial para Hilbert. Ele foi agraciado com o *Prêmio Bolyai* em 1910, e eleito membro da *Royal Society* em Londres, em 1928. Em 1930, Hilbert já aposentado e a sua cidade natal (Königsberg) fez dele um cidadão honorário da cidade.

Como citado em Hodges (1970), **Hilbert** acreditava que em matemática não existia - *nós não sabemos e não saberemos*".

Hilbert mencionou **George Cantor**, de quem era admirador, proferindo uma frase de efeito sobre este:

"*Ninguém nos tirará, do paraíso que Cantou nos deu.*"

E deixou seis palavras, mostrando o seu entusiasmo pela matemática e sua vida dedicada à resolução de problemas matemáticos:

"*Wir müssen wissen, wir werden wissen-* "*We must know, we shall know.*"

14.6 Bibliografia e Fonte de Consulta

Biography's Hilbert - ⟨http://www-history.mcs.st-and.ac.uk/Biographies/Hilbert.html⟩

As contribuições de Hilbert à matemática - ⟨https://pt.wikipedia.org/wiki/David_Hilbert⟩

Walter Carnielli, Richard L. Epstein - Computabilidade Funções Computáveis - Lógica e os Fundamentos da Matemática. Ed. UNESP, 2005.

Michael Sipser. Introdução à Teoria da Computação. Cengage Learning. 2007.

Michel Janos. Matemática e Natureza. Ed. Livraria da Física. 2009.

Wamberto W. M. P. Vasconcellos - O Tempo como Modelo: a aplicação de Lógica Temporal na especificação formal de sistemas distribuídos. Dissertação de mestrado. COPPE-CCO-UFRJ, 1989.

Hilbert, Gödel e Turing - ⟨http://www.philocomp.net/home/hilbert.htm⟩

On Consistency - ⟨https://en.wikipedia.org/wiki/Consistency⟩

Biografia de Bishop - ⟨http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Bishop.html⟩

14.7 Referências - Leitura Recomendada

Hilbert, David. 1926. Uber das Unendliche. ¨ Mathematische Annalen 95: 161-90. Lecture given Münster, 4 June 1925. English translation in (van Heijenoort, 1967,

367-392).

Hilbert, David and Paul Bernays. 1939. Grundlagen der Mathematik, vol. 2. Berlin: Springer.

David Hilbert - ⟨https://en.wikipedia.org/wiki/David_Hilbert⟩

David Hilbert 1862-1943 - ⟨http://genealogy.math.ndsu.nodak.edu/id.php?id=7298⟩

Richard Zach, "Hilbert's Program", The Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/entries/hilbert-program/.

David Hilbert em Mathematics Genealogy Project - https://pt.wikipedia.org/wiki/Mathematics_Ger

David J. Darling. The Universal Book of Mathematics. [S.l.]: John Wiley and Sons, 2004. p. 151. ISBN 978-0-471-27047-8.

Jean van Heijenoort - Lógica como Cálculo y Lógica como Linguaje.

Stephen Kleene (1952) - 10th impression 1991, Introduction to Metamathematics, North-Holland Publishing Company, Amsterday, New York, ISBN 0-7204-2103-9.

Hans Reichenbach, 1947, Elements of Symbolic Logic, Dover Publications, Inc. New York, ISBN 0-486-24004-5.

Alfred Tarski, 1946, Introduction to Logic and to the Methodology of Deductive Sciences, Second Edition, Dover Publications, Inc., New York, ISBN 0-486-28462-X.

Jean van Heijenoort (1967) - From Frege to Gödel: A Source Book in Mathematical Logic, Harvard University Press, Cambridge, MA, ISBN 0-674-32449-8.

H.D. Ebbinghaus, J. Flum, W. Thomas - Mathematical Logic.

Jevons, W.S. (1870) - Elementary Lessons in Logic.

CAPÍTULO 15

Gödel - Os Limites dos Sistemas Formais

A História da computação mostra que foram os matemáticos e os lógicos que criaram a ciência da computação, tendo influenciado na criação de todas as áreas atuais desta ciência. Este capítulo esclarece este fato, descrevendo vários acontecimentos relevantes dos matemáticos, que fizeram culminar com a ciência da computação.

15.1 De Hilbert à Gödel

Seguindo do capítulo precedente, em 1928, um novo problema é lançado por **Hilbert**. Parte desse problema abordava a questão do que **von Neumann** apontara sobre a **consistência** da matemática. **Hilbert** queria saber se era possível provar toda assertiva matemática que fosse verdadeira. Isto é, tudo que fosse verdadeiro poderia ser provado pela matemática? Este era o problema que estava relacionado à busca de um sistema formal *completo*, mas que também se fosse *consistente*, seria ainda melhor. O que **Hilbert** queria era que, para uma determinada afirmação matemática, houvesse um *procedimento* que, após um número finito de passos, parasse e indicasse que aquela afirmação poderia ou não ser provada em determinado sistema formal. **Hilbert** estava interessado num sistema formal que fosse finitísticamente descritível. **Hilbert** dizia que tal sistema deveria ser construído com um número finito de axiomas e um número finito de regras, e toda prova dentro do sistema deveria ter um número finito de passos. Isto é, o sistema formal deveria ser consistente, completo e suficientemente poderoso para abranger a aritmetica ordinária Filho (2007). Particularmente, **Hilbert** queria ter uma Teoria da Aritmética, isto é, o problema da *consistência* da matemática seria reduzido ao problema da **consistência** da aritmética.

Os fundamentos matemáticos da **Ciência da Computação** moderna começaram a ser definidos por **Kurt Friedrich Gödel** (1906-1978) com seu *Teorema da Incompletude* (1931).

Em 1931, **Kurt Gödel**, então um jovem matemático, publicou em um periódico alemão o artigo intitulado - "*Sobre as Proposições Indecidíveis do Principia Mathematica e Sistemas Correlatos*". As conclusões contidas em tal artigo são um divisor de águas na história da lógica e da matemática predominante nos tempos de **Leibniz** à **Hilbert**.

Gödel provou que sistemas dedutivos (da aritmética, da álgebra e da lógica) não podiam ser completamente axiomatizados e quaisquer métodos que sejam utilizados para demonstrar a consistência desses sistemas, serão tão complexos que sua consistência fica tão aberta a dúvidas quanto a dos próprios sistemas.

Essa teoria mostra que **existem limites no que pode ser provado ou desaprovado em um sistema formal** (ver Stein (2008), Cap.7). Isso levou a trabalhos posteriores por **Gödel** e outros teóricos para definir e descrever tais **sistemas formais**, incluindo conceitos como **recursividade** e o λ-**Cálculo**, que sensibilizaram **Alonzo Church**, como veremos na seção **??**.

Gödel, matemático tcheco naturalizado norte-americano, então com seus 23 anos, em sua tese de doutorado de apenas 30 páginas, considerou diversos resultados relevantes sobre a *completude do cálculo lógico*, no campo da Lógica Matemática.

Figura 82 – Kurt Gödel: A completude da Lógica dos Predicados e o Problema da Incompletude.

Fonte: en.wikipedia.org.

Existem duas definições de **completude**, como apresentadas em Filho (2007) :

- Completude semântica - Um sistema de axiomas é completo, quando todos os teoremas verdadeiros da teoria (por exemplo, a aritmética) podem ser deduzidos a partir do sistema de axiomas.

- Completude sintática - Um sistema de axiomas é completo, quando toda a tentativa de lhe adicionar um axioma, independente dos anteriores, resulta numa *contradição*.

Gödel usava a definição de **completude** no **sentido semântico**. Ele demonstrou que "*toda fórmula válida logicamente do cálculo de primeira ordem* (Cálculo dos Predicados) *pode ser deduzida a partir dos axiomas clássicos deste mesmo cálculo*". Isto significa que o sistema de axiomas do Cálculo de Predicados é *completo*. **Gödel** considerou este resultado como um complemento teórico ao método usual da demonstração da não-contradição, como explicado no que segue.

Modelos e *Consequência Lógica* - Usamos aqui a definição dada em LOECKX (1987).

Seja W um conjunto de fórmulas, tal que $W \subseteq WFF_B$, onde WFF_B é o conjunto de fórmulas bem-formadas da Lógica dos Predicados de base B. $B = (F, P)$, onde F é conjunto de símbolos funcionais e P é o conjunto de símbolos predicativos da Lógica dos Predicados. Uma interpretação $\phi = (D, I)$ é chamada um *modelo* de W, se toda fórmula $w \in W$ éconsequência lógica *válida* ($\models_\phi w$) sob essa interpretação ϕ. Uma fórmula $w \in WFF_B$ é chamada uma consequência lógica de W - denotado por $W \models_\phi w$, se w é válida ($\models_\phi w$) para todo modelo ϕ de W.

O método usual de demonstração de uma não-contradição, consiste em contruir um *modelo*, como definido acima, ou seja oferecer uma *interpretação* semântica, para o sistema considerado. Porque se uma *teoria* admite um *modelo*, então ela é não-contraditória. Gödel provou a recíproca desta propriedade: "todo sistema axiomático de primeira ordem, não contraditório, possui um modelo".

Este resultado parecia confirmar o que desejava **Hilbert**, de construir um teoria rigorosa capaz de descrever toda a matemática. Mas, **Gödel** seguiu um caminho mais prudente em suas pequisas. O que ele havia conseguido como resultado, era com relação aos axiomas de um cálculo de primeira ordem (que somente quantifica variáveis, por exemplo, como: existe $\exists\, x$ ou para todo $\forall\, x$).

Entretanto, os teoremas da *incompletude* de **Kurt Gödel**, vieram por fim à tentativa de unificar a matemática num sistema formal como propôs **Hilbert**. As consequências, nas ciências matemáticas, significam que não é possível chegar a uma teoria rigorosa capaz de descrever toda a matemática. Uma teoria de tudo, como imaginava **Hilbert**. Os teoremas de **Godel** dizem que é impossível definir um sistema de axiomas **completo** que seja simultaneamente *consistente*. Isto é, ou é completo ou é consistente. Um sistema formal diz-se completo, se podemos provar qualquer asserção (afirmação) ou a sua negação a partir dos axiomas. Os axiomas são os alicerces de um sistema formal, são as afirmações iniciais que se consideram evidentes e sem necessidade de prova. Um sistema diz-se *consistente* se

não podemos provar simultaneamente uma afirmação e a sua negação. O leitor pode ver em ⟨http://cronicadaciencia.blogspot.com.br/p/teorema-de-godel.html⟩

Mas, o teorema de **Kurt Gödel** (1931), teorema mais conhecido como **Teorema da Incompletude de Gödel** dizem que: "**é impossível definir um sistema de axiomas completo que seja simultaneamente consistente**. Isto é, ou é completo ou é consistente".

Um sistema diz-se *completo*, se dentro dele, podemos provar qualquer afirmação ou a sua negação a partir dos axiomas. Um sistema diz-se *consistente* se não podemos provar simultaneamente uma afirmação e a sua negação.

Pode-se enunciar os teoremas de **Gödel**, assim:

Teorema de Gödel 1 - O primeiro teorema da incompletude afirma que *nenhum sistema consistente de axiomas* de uma teoria T, cujo conjunto de teoremas é recursivamente enumerável (existe um "procedimento efetivo", qualquer tipo de algoritmo, que reconhece um elemento do conjunto), ou seja, é capaz de provar todas as verdades sobre as relações dos números naturais (aritmética). Para qualquer desses sistemas de axiomas, sempre haverá afirmações sobre os números naturais que são verdadeiras, mas que não podem ser provadas dentro do sistema.

De maneira formal:

"Qualquer teoria axiomática recursivamente enumerável e capaz de expressar algumas verdades básicas de aritmética não pode ser, ao mesmo tempo, completa e consistente. Ou seja, sempre há em uma teoria consistente proposições verdadeiras que não podem ser demonstradas nem negadas."

Teorema de Gödel 2 - O segundo teorema da *incompletude*, uma extensão do primeiro, mostra que tal sistema não pode demonstrar sua própria consistência.

De maneira formal:

"Uma teoria, recursivamente enumerável e capaz de expressar verdades básicas da aritmética e alguns enunciados da teoria da prova (um ramo da lógica matemática que representa provas como objetos matemáticos, facilitando sua análise por técnicas matemáticas), pode provar sua própria consistência se, e somente se, for inconsistente".

Em outras palavras, "para cada teoria T formal que inclua a aritmética e a capacidade de prova, T só é capaz de fazer uma afirmação sobre a sua própria consistência se T for inconsistente". Ou seja, o sistema só pode dizer que é consistente se na realidade não o for.

Os teoremas de Godel só se aplicam a sistemas formais que sejam capazes de "conter"a aritmética. Na realidade é possível criar *sistemas completos e consistentes* desde que estes sejam muito simples, como o Cálculo Proposicional (ordem zero, não expressa e quantifica variáveis) e o Cálculo dos Predicados (primeira ordem, que quantifica variáveis). Os teoremas da incompletude de Gödel são dois teoremas da lógica matemática que estabelecem limitações inerentes a todos, menos aos mais triviais sistemas axiomáticos capazes de fazer aritmética.

Dizendo de uma forma em genérica:

"**Proposições formais poderiam ser indecidíveis. Ou seja, não se poderia dizer se são verdadeiras ou falsas**".

O teorema de **Gödel** foi muito importante. **Gödel**, provou a incompletude matemática. Ou seja, a matemática não poderia ser usada para provar a própria matemática. Os problemas propostas por **Hilbert** poderiam ser indemonstráveis. Ou seja, alguns dos 23 problemas de **Hilbert** poderiam não ter solução. Os teoremas, provados por **Kurt Gödel** em 1931, são importantes tanto para a lógica matemática quanto para a filosofia da matemática. Os dois resultados são interpretados como indicações de que o programa de **Hilbert** para encontrar um conjunto completo e consistente de axiomas para toda a matemática era impossível, e proporcionando uma resposta negativa para o segundo problema de **Hilbert**.

Gödel acabou com o sonho logicista, porque não se pode desenvolver toda a aritmética, e muito menos toda a matemática, num sistema que possa ser ao mesmo tempo **consistente** e **completo**. Também acabou com o sonho formalista: existem enunciados matemáticos que são verdadeiros, mas não são suscetíveis de prova, ou seja, existe um abismo entre verdade e demonstração Filho (2007).

Outro resultado fundamental do teorema da incompletude de **Gödel** é a demonstração de que há **funções** que não podem ser representadas por um algoritmo, isto é, **não podem ser computadas**.

Depois que muitas filosofias da matemática se mostraram inadequadas, **paradoxos** não resolvidos e **inconsistências** na matemática, surge o matemático austríaco **Kurt Friedrich Gödel** (1906-1978), surpreendendo o mundo matemático e da lógica, provando que era **impossível**, o objetivo, de uma linguagem universal para resolver todos os problemas de natureza da cooperação humana, como **Leibniz** desejava, e a ideia de uma formulação completa e consistente, como **Hilbert** queria para toda a matemática.

Kurt Gödel mostrou que nenhum método finito poderia ser utilizado para provar o problema da consistência desse método. A prova de Gödel foi definitiva ou ele apenas mostrou que **alguns** meios não resolviam o problema? O trabalho mais conhe-

cido que acabou prevalecendo foi o **Gödel** provou que nenhum conjunto de axiomas de um sistema formal é suficientemente poderoso para provar sua própria consistência.

Além disso, através do trabalho de **Gödel**, ficou claro que, apenas para sistemas formais mais simples, como nos casos das **lógicas e o cálculo proposicional** e a **lógica e o cálculo dos predicados**, se poderia construir sistemas consistentes e completos, como são os casos dos cálculos das lógicas simbólicas seguintes:

- Lógica e o Cálculo Proposicional - consistente e completo. Manna (1985)
- Lógica e o Cálculo dos Predicados - consistente e completo. Loeckx e Sieber (1987)
- LTLp (Lógica Temporal Linear proposicional) - consistente e completo. Vasconcelos (1989)

Existem sistemas formais que **não** são **consistentes** e **completos**, como nos casos apontados a seguir:

- LTLPo (Lógica Temporal Linear de Primeira Ordem) - consistente, mas incompleta, como provado em Szalas e Holenderski (1988) e Vasconcelos (1989).
- LTTR - consistente, mas de completude em aberto Emerson e Sistla (1984), e completa no caso do sistema $\mathcal{UB}$ de menor expressividade que a LTTR genérica Ben-Ari, Pnueli e Manna (1983).

O leitor poderá entender melhor este problema, nos capítulos sobre o trabalho de Gödel, capítulos 14,15.

Durante a primeira metade do século XX, tempos antes de existir o computador, matemáticos como **Gödel**, e posteriormente, **Alan Turing** e **Alonzo Church** descobriram que certos problemas básicos não poderiam ser resolvidos por imaginados computadores. Um exemplo é o problema:

determinar se um determinado enunciado matemático (um teorema) é verdadeiro ou falso.

Este parece uma questão natural, que reside estritamente no domínio da matemática, mas que nos leva para a existência de um *procedimento efetivo*, para o qual dado tal enunciado, pudesse responder sim (verdadeiro) ou não (falso) Sipser (2011).

A noção de *procedimento efetivo*, é agora, essencial para responder esta questão. Entretanto, entre as consequências desse resultado estava o desenvolvimento de ideias concernentes a modelos teóricos sobre **computabilidade**, que em algum momento futuro ajudasse à construção de computadores reais Sipser (2011). E a noção de *computabilidade*, é agora fundamental para responder esta questão, como colocada

em Carnielli e Epstein (2005).

Em decorrência do trabalho de **Gödel**, e apesar do desapontamento de grande parte da comunidade da matemática e da lógica, a parte da Lógica Simbólica mais básica, consistente e completa, da lógica proposicional e da lógica dos predicados, acabou como base para disciplinas relevantes no estudo da **ciência da computação**, como a Álgebra Booleana (de George Boole) que já existia desde o século XVIII, muito bem aproveitada, no século XX, na segunda metade da década de 40, por **Claude Shanonn**, para a construção de circuitos lógicos, que alicerçaram a construção dos primeiros computadores digitais, cuja a história é contada no Capítulo 8 do Volume 2.

15.2 Ainda sobre o Trabalho de Gödel

Em Nagel e Newman (2001), o leitor é introduzido a uma das descobertas mais importantes do século XX: os teoremas da incompletude de **Gödel**.

Segundo Matheus Silva (2008), em oito capítulos de prosa clara e rigor conceitual, **Ernest Nagel** e **James Newman** narram o percurso histórico que levaria à prova de **Gödel**:

À medida que novas áreas da matemática foram dotadas com conjuntos de axiomas, surge no séc. XIX a esperança de que toda a matemática poderia ser dotada de um conjunto de axiomas. Se fosse possível fornecer uma axiomatização completa da aritmética, axiomatizar as demais áreas da matemática seria apenas uma questão de tempo. A metamatemática de ***Hilbert****, assim como os Principia Mathematics de* ***Russell*** *são exemplos desses modelos axiomáticos que tinham como objetivo fornecer uma prova da aritmética. Essa esperança caiu por terra com as conclusões de Gödel.*

Para ilustrar como isso acontece, tomemos como exemplo a metamatemática de ***Hilbert****. Ela procede a partir da seguinte distinção: a matemática constitui os sistemas formais estudados pelos matemáticos; a teoria acerca desses sistemas denomina-se "metamatemática". As expressões que ocorrem na matemática devem ser compreendidas como isentas de sentido, o que importa são suas estruturas e o modo como se combinam. As expressões que ocorrem na metamatemática, por outro lado, são significativas, e será a partir dela que iremos avaliar se a aritmética é consistente: demonstrar que duas fórmulas contraditórias não podem ser ambas derivadas dos axiomas da aritmética é demonstrar que a aritmética é consistente. Mas, como* ***Gödel*** *demonstrou, esse projeto enfrentou dois obstáculos insuperáveis.*

O primeiro obstáculo é demonstrado pelo ***Primeiro Teorema da Incompletude*** *(prova da existência de proposições indecidíveis no cálculo dos Principia Mathematica e sistemas semelhantes): em qualquer sistema axiomático suficientemente amplo para expressar a aritmética é possível construir uma fórmula aritmética F, verda-*

deira, que é exprimível nesse sistema, mas que não é demonstrável no sistema. Tais fórmulas aritméticas verdadeiras têm um correspondente enunciado metamatemático que afirma que a própria fórmula não é verdadeira. Isto é, F diz de si própria que não é demonstrável. Se F for demonstrável, então é uma verdade da aritmética. Por outro lado, como F afirma que ela própria não é demonstrável, a sua demonstração implica a sua falsidade. Mas se a aritmética admite uma fórmula e a sua negação como verdades, então ela é inconsistente. Portanto, F é verdadeira e não pode ser demonstrada na axiomatização da aritmética, pois se F pudesse ser demonstrada nessa axiomatização teríamos uma contradição. Logo, F é indecidível.

Como conseqüência, a axiomatização da aritmética somente poderá ser consistente, se for inerentemente incompleta e (o que é trivial) só poderá ser completa, se for inconsistente. Qualquer axiomatização consistente da aritmética é incapaz de abranger todas as verdades da aritmética. Alguns sistemas podem abranger mais verdades do que outros, mas nenhum é capaz de abranger todas as verdades da aritmética.

O segundo obstáculo insuperável é demonstrado pelo ***Segundo Teorema da Incompletude de Gödel****, que é um corolário do Primeiro (não é possível provar, no interior do cálculo dos Principia Mathematica e sistemas semelhantes, a consistência do próprio sistema): a consistência de um sistema axiomático suficientemente amplo para conter a aritmética não pode ser demonstrada no interior deste próprio sistema. Se a axiomatização da aritmética proposta por* ***Hilbert*** *for consistente, o enunciado metamatemático que representa a sua própria consistência não é demonstrável nessa axiomatização. A consistência de sistemas como a metamatemática de* ***Hilbert*** *somente pode ser demonstrada com o emprego de princípios logicamente mais complexos do que os próprios princípios da metamatemática de* ***Hilbert****.*

As descobertas de Gödel têm grande importância, mas a extensão do seu alcance ainda não foi totalmente compreendida. Uma das razões para essa incompreensão é que as descobertas de ***Gödel*** *tiveram o mesmo destino de outras descobertas importantes: foram tão deturpadas por interpretações de intelectuais inferiores a Gödel, que se torna difícil perceber sua real significância. O desfile de interpretações vai desde filósofos pós-modernos, que vêem nisso o surgimento de uma ciência pós-moderna, até irracionalistas, que vêem nas conclusões de* ***Gödel*** *uma derrota da lógica clássica. Mas as descobertas de Gödel não têm nenhuma dessas implicações. Os filósofos pós-modernos, como de costume, não tem qualquer argumento para sustentar suas afirmações e a interpretação irracionalista ignora que o próprio Gödel forneceu demonstrações de consistência da lógica clássica ("The Completeness of the Axioms of the Functional Calculus of Logic", 1930).*

Uma conseqüência real dentre várias que podemos inferir das descobertas de Gödel, é que a verdade matemática não pode ser identificada com a dedutibilidade a partir de axiomas ou com meras convenções linguísticas. Esse resultado deita por terra a epistemologia positivista que procurava explicar o conhecimento a priori, reduzindo-o ao mero conhecimento linguístico. Verdades como o último teorema de Fermat perma-

neceram como uma conjectura durante séculos até a descoberta de sua demonstração no século XX. As justificativas racionalistas são inevitáveis nesse caso, pois não podemos esgotar tal verdade matemática em convenções linguísticas. A razão é fonte de conhecimento substancial, tese defendida pelo próprio Gödel.

Outra conseqüência é que, aquilo que denominamos de prova matemática, nada tem a ver com um método axiomático formalizado. Isso porque os axiomas e regras de demonstração, de um método axiomático, inicialmente fixadas não podem impor um limite à criatividade dos matemáticos e a sua capacidade para criar novas demonstrações. O que também vai ao encontro das justificativas racionalistas Nagel e Newman (2001).

15.3 A Enumeração de Gödel

Em Carnielli e Epstein (2005), uma das criações de **Kurt Gödel** para a ciência da computação foi a criação de um mapeamento de vários números naturais em um único número natural. Tal enumeração também é chamada *aritmetização*.

Desde que o artigo de **Gödel** foi publicado em 1931, o termo "*enumeração de Gödel*"tem sido usado para se referir a atribuições mais genéricas dos números naturais a objetos matemáticos. O conceito foi usado pela primeira vez por **Kurt Gödel** para a prova de seu teorema da incompletude.

Um exemplo, dos **números de Gödel** para a computação, pode ser dado. Como um programa de computador é um sequência de bits, ou seja, equivalente a um número natural, podemos transformar (associar) essa sequência em/a outro número natural, chamado **número de Gödel**.

Podemos trabalhar com um alfabeto $\mathcal{A}$, constituído de n símbolos e criarmos as palavras w sobre o alfabeto $\mathcal{A}$. Pode-se, de fato, associar às palavras w, números naturais $G(w)$, de tal forma que cada número natural seja associado a no máximo uma palavra w de $\mathcal{A}$. Tal representação $G(w)$ é chamada de enumeração de Gödel e $G(w)$ o número de Gödel da palavra w. Gödel foi o primeiro a usar esta representação.

15.3.1 Requerimentos para a Aritmetização

Hermes (1969)

Os seguintes requerimentos são feitos para a aritmetização G:

1. Se $w1 \neq w2$, então $G(w1) \neq G(w2)$.

2. Deve existir um procedimento efetivo (mecânico) tal que, para qualquer palavra dada w, o número natural $G(w)$ correspondente, pode ser computado num número finito de passos pela ajuda desse procedimento.

3. Para qualquer número natural n pode ser decidido, num número finito de passos, se n é o número de **Gödel** de uma palavra w sobre $\mathcal{A}$.

4. Existe um procedimento efetivo que, se n é o número de Gödel de uma palavra w sobre $\mathcal{A}$, então a palavra w (que de acordo com o item 1, deve ser única) pode ser construída em um número finito de passos , através desse procedimento efetivo.

Para mostrar que esta enumeração de **Gödel** satisfaz os requerimentos de **Hermes**, aqui referidos, precisamos do **Teorema Fundamental da Aritmética**:

"**Qualquer número natural** $n \geq 2$ **pode ser representado como um único produto de números primos** (a menos da ordem dos fatores)."

Deste modo, pode-se enumerar todo os tipos de objetos, não somente de palavras de símbolos de um alfabeto $\mathcal{A}$. De forma geral, os requerimentos indicados por **Hermes**, para que uma enumeração seja de utilidade, são:

1. Objetos distintos tem números distintos.

2. Dado um objeto, pode-se efetivamente encontrar o seu número.

3. Dado um número, pode-se efetivamente decidir se esse está associado a algum objeto e, se estiver, a qual objeto.

É oportuno observar que o processo de enumeração é uma das formas de se atribuir nomes a objetos. Objetos tem propriedades, independentemente de como atribuimos os nomes Carnielli e Epstein (2005) (Cap.3, p.43).

15.3.2 Exemplo de Enumeração de Gödel

Aqui está um exemplo de uma enumeração de **Gödel**, aplicado à computação, como descrita por **Hermes**:

Supondo que tenhamos que representar - "pressionar a tecla **A** e de **enter**- por três números naturais, 11 para "pressionar tecla", 1 para "A", e 13 para "Enter". Então para codificar - "pressionar tecla "A"e de "Enter- combinamos os números 11, 1 e 13, de forma a compor um outro número natural. Este outro natural é o número criado por Gödel.

Assim, se $W\ G = 2^{11}x3^{1}x5^{13} = (2048)x(3)x(1220703125) = 7.500.000.000.000$

O três símbolos que foram, individualmente, codificados por 11, 1 e 13 são codificados como um único inteiro G, onde 2, 3 e 5 são os três primeiros números **primos**. Esta codificação usa diretamente o **Teorema Fundamental da Aritmética**: "Qualquer número natural é representado por um único produto de números primos". E também, o **Teorema dos Infinitos Números Primos**: "A quantidade de números primos

é infinita".

Formalizando, se tomarmos os número naturais x_1,x_2, ... ,x_n, o número de Gödel será dado por:

$$G = \times i = 1n(p_i)^i = p_1^{x_1}.p_2^{x_2}.....p_n^{x_n}$$

em que p_i são os primeiros números primos.

Neste sentido, pode-se ignorar tudo o que existe de hardware e de software dentro do computador e se concentrar em três grandes números para representar as sequências de bits: um para a entrada, outro para representar um programa de computador, e um terceiro para a saída.

De uma forma geral, uma numeração de **Gödel** é uma função matemática que atribui a cada *símbolo* e *fórmula bem formada* de alguma linguagem formal um único número natural, chamado seu **número de Gödel**.

A numeração de **Gödel** pode ser interpretada como uma codificação em que um número é atribuído a cada símbolo da notação matemática, após o qual uma sequência de números naturais pode representar uma seqüência de caracteres. Estas sequências de números naturais podem voltar a ser representadas por um único número natural, facilitando a sua manipulação nas teorias formais da aritmética.

15.4 Gödel e as Funcões Recursivas

Como em Zach (2006), grande parte da Ciência da Computação teórica mais geral, tem suas raízes, historicamente, bem como conceitualmente, no campo da lógica, e por isso, muitos dos resultados de **Gödel** também são importantes no campo do valor teórico para Ciência da Computação. No perído de 1933-1935, **Gödel** introduziu as funções recursivas primitivas. **Gödel** (1934) definiu as funções recursivas gerais, a partir das ideias de **Herbrand**. **Gödel** não se preocupou com a noção de efetivamente computável, mas somente com a definição de função recursiva, como as *funções recursivas primitivas.*

Gödel visitou a University of Princeton no período acadêmico de 1933/34 e deu uma série de palestras, entre Fevereiro e Maio de 1934, nas quais estavam participando **Church**, **Kleene** e **Rosser**. Ao fim de suas palestras em Princeton, **Gödel** introduziu a noção de função recursiva geral. Essa noção foi baseada em uma sugestão de **Herbrand** em uma carta a **Gödel**, de 7 de Abril, 1931 (Gödel, 2003b, 14-21). Nestas palestras, **Gödel** (1934, 368-369), definiu as funções recursivas gerais como aquelas que podem ser calculadas usando um conjunto específico de regras de substituição de um conjunto de equações de definição, e para as quais o resultado do cálculo é unicamente determinada.

Para uma discussão sobre a conexão entre as noções de **Gödel** e de **Herbrand**, veja Sieg 2005. **Gödel** não foi o primeiro a propor a definição de recursividade geral, como uma explicação da noção informal de "efetivamente computável", mas apenas como uma explicação da noção de "função recursiva". Em 1931, **Gödel** tinha introduzido as funções recursivas primitivas (embora ele as chamou, em seguida, apenas "funções recursivas"). Já era conhecido desde meados da década de 1920 (Hilbert, 1926; Ackermann, 1928) que existiam funções recursivas não-primitivas, que podiam ser definidas pela dupla recursão, e no início de 1930, **Péter** (1934, 1935) estudou essas funções recursivas em mais detalhes.

15.5 Bibliografia e Fonte de Consulta

Kurt Friedrich Gödel - ⟨https://pt.wikipedia.org/wiki/Kurt_G\unhbox\voidb@x\bgroup\accent127o\penalty\@M\hskip\z@skip\egroupdel⟩

Cleuzio Fonseca Filho (2007) - Historia da Computação: o Caminho do Pensamento e da Tecnologia, EDPUCRS.

Matheus Silva (Março de 2008) - Sobre o trabalho de Gôdel - *Prosa clara e rigor conceitual*, em ⟨http://criticanarede.com/log_godel.html⟩, acessado em 03 de Julho de 2015.

Ackermann, Wilhelm. 1928. Zum Hilbertschen Aufbau der reellen Zahlen. Mathematische Annalen 99: 118-133.

Barendregt, Henk. 1997. The impact of the lambda calculus in logic and computer science. The Bulletin of Symbolic Logic 3(2): 181-215.

Buss, Samuel R. 1994. On Gödel's theorems on lengths of proofs I: Number of lines and speedups for arithmetic. Journal of Symbolic Logic 39: 737-756.

Buss, Samuel R. 1995. On Gödel's theorems on lengths of proofs II: Lower bounds for recognizing k symbol provability. In Feasible Mathematics II, eds. P. Clote and J. Remmel, 57-90. Basel: Birkhäuser.

Hilbert, Gödel e Turing - ⟨http://www.philocomp.net/home/hilbert.htm⟩

Gödels Incompleteness Theorems - A Brief Introduction, em ⟨http://math.mind-crafts.com/godels_incompleteness_theorems.php⟩

James D. Stein - Como a Matemática Explica o Mundo, O poder dos números no cotidiano, Campus, Segunda Edição, Parte II-A Caixa de Ferramentas Incompletas, Cap.7 (Até a Lógica tem Limites, p.132).

15.6 Referências - Leitura Recomendada

Ernest Nagel, James R. Newman. A Prova de Gödel. Tradução de Gita K. Guinsburg. São Paulo: Editora Perspectiva, 2001, 100 pp.

Gödel, Kurt. 1929. Uber die Vollständigkeit des Logikkalküls. Dissertation, Üniversität Wien. Reprinted and translated in (Gödel, 1986, 60-101).

Gödel, Kurt. 1930. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. Monatshefte für Mathematik und Physik 37: 349-360. Reprinted and translated in (Gödel, 1986, 102-123).

Gödel, Kurt. 1930. Einige metamathematische Resultate über Entscheidungsdefinitheit und Widerspruchsfreiheit. Anzeiger der Akademie der Wissenschaften in Wien 67: 214-215. Reprinted and translated in (Gödel, 1986,140-143).

Gödel, Kurt. 1931. Uber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatshefte für Mathematik und Physik 38:173-198. Reprinted and translated in (Gödel, 1986, 144-195).

Gödel, Kurt. 1932. Ein Spezialfall des Entscheidungsproblem der theoretischen Logik. Ergebnisse eines mathematischen Kolloquiums 2: 27-28. Reprinted and translated in (Gödel, 1986, 130-235).

Gödel, Kurt. 1933. Zum Entscheidungsproblem des logischen Funktionenkalküls. Monatshefte für Mathematik und Physik 40: 433-443. Reprinted and translated in (Gödel, 1986, 306-327).

Gödel, Kurt. 1934. On undecidable propositions of formal mathematical systems. Lecture notes by Stephen C. Kleene and J. Barkely Rosser, Princeton University. Reprinted in (Gödel, 1986, 338-371).

Gödel, Kurt. 1936. Uber die Länge von Beweisen. Ergebnisse eines mathematisches Kolloquiums 7: 23-24. Reprinted and translated in (Gödel, 1986,394-399).

Gödel, Kurt. 1946. Remarks before the Princeton bicentennial conference on problems in mathematics. In Collected Works, eds. Solomon Feferman et al., vol. 2, 144-153. Oxford: Oxford University Press.

Gödel, Kurt. 1986. Collected Works, vol. 1, eds. Solomon Feferman et al. Oxford: Oxford University Press.

Gödel, Kurt. 2003a. Collected Works, vol. 4, eds. Solomon Feferman et al. Oxford: Oxford University Press.

Gödel, Kurt. 2003b. Collected Works, vol. 5, eds. Solomon Feferman et al. Oxford: Oxford University Press.

CAPÍTULO 16

Dos Fundamentos da Matemática aos Sistemas Formais

Denomina-se *fundamentos da matemática* a uma área de estudo que abrange tanto problemas da filosofia da matemática, como da lógica e da matemática. Ela teve a sua origem nas últimas décadas do século XIX e desenvolveu-se durante as primeiras décadas do século XX, como uma resposta à crise dos fundamentos gerada pelos *paradoxos*, a partir da Teoria dos Conjuntos de Cantor.

O surgimento de paradoxos deveu-se a resposta à teoria de **Cantor** dos ordinais transfinitos, **Burali-Forti** anuncia que nessa teoria pode ser derivada uma contradição, posteriormente denominada paradoxo de **Burali-Forti**. Em 1902, **Bertrand Russell** escreve uma carta para **Frege** na qual anuncia que no sistema das leis fundamentais da aritmética pode ser derivada uma contradição, hoje conhecida como *paradoxo de Russell*, mas certas fontes afirmam que já era conhecida com anteriormente por **Ernst Zermelo**, pertencente ao círculo de **Hilbert**. Esses paradoxos, mais outros enunciados posteriormente, geram uma crise de fundamentos (em alemão: *Grundlagenkrisis*), na qual são questionados os métodos e a lógica utilizada pela matemática.

As respostas à crise de fundamentos desenvolveram-se em diferentes direções, formando-se as correntes filsóficas principais denominadas como segue. Neste capítulo são apresentadas as correntes filosóficas da matemática, que em algum sentido beneficiou a ciência da computação. Nos fundamentos da matemática como explicados em Costa (2008), são divididas em *Logicismo*, *Intuicionismo* e *Formalismo*. Em Janos (2009), são citadas as correntes do **platonismo**, **formalismo** e **construtivismo** (ramificado do Intuicionismo).

16.1 O Platonismo

Platonismo, na filosofia da matemática, é a ideia de que os objetos matemáticos existem, independentemente dos matemáticos, sendo imutáveis e eternos. Na corrente platonista, estamos falando de coisas como números, triângulos, entre outras, que conhecemos bem. Mas também falamos de conjuntos ou algo que não conhecemos ainda. O *platonismo* **encara uma ideia matemática como uma descoberta e não como algo inventado pelo homem**. Exemplos são: (a) o número e e π são números descobertos na natureza, e não inventados pelos matemáticos. Os matemáticos os descobriram. (b) O teorema de Pitágoras não foi inventado, mas decoberto por Pitágoras. Segundo Janos (2009), 65% dos matemáticos são platonistas.

16.2 O Logicismo

Em outro sentido, **Gottlob Frege** afirma que a matemática deve fortalecer as suas bases lógicas, colocando claramente sua posição no livro Fundamentos da aritmética, e depois nas Leis fundamentais da aritmética, onde começa com um desenvolvimento da lógica matemática para passar á matemática, como maneira de justificar a unificação de ambas.

O **logicismo** é a tese de que a matemática, ou uma parte dela, deve reduzir-se à lógica, ou a uma parte da lógica. **Gottlob Frege** foi um dos primeiros lógicos a pensar assim, e ainda no século XIX, em 1884, **Frege** funda o logicismo. Essa escola tenta estabelecer a base da matemática através da lógica, defendendo que toda a matemática poderia ser derivada a partir da lógica, ou seja, a matemática seria na verdade uma lógica disfarçada.

Em 1902, o *logicismo* é contestado com a descoberta do paradoxo de **Russell**. Utilizando o princípio criado anteriormente por **Frege**, **Russell** pensou na seguinte classe de entidades: $R = \{X \| X \notin X\}$, ou seja, R é o conjunto de todos os conjuntos que não são membros deles próprios. Se R não é membro dele mesmo, então, pela própria definição de R, ele teria que conter ele mesmo. R também não pode ser membro dele mesmo, pois entraria em contradição com sua própria definição. Por isso, a existência de R é um paradoxo. Como R foi criado a partir do princípio utilizado por **Frege**, este não pode estar correto. O próprio **Russell** tentou resolver esse problema, criando uma teoria para definir quando uma entidade matemática podesse definir classes. Entretanto, a partir dessa nova teoria, **Russell** não conseguiu derivar os princípios básicos da aritmética, sem ter que apelar para princípios da matemática, e não da lógica. **Russell** aderiu ao pressuposto de **Frege** da unidade entre a lógica e a matemática e escreveu, junto com **Whitehead**, o monumental texto dos *Principia Mathematica*, na qual são desenvolvidas de uma maneira contínua, a lógica e a matemática. Esse aprofundamento das ideias de **Frege** como resposta à crise constitui a base da tendência logicista.

16.3 A Teoria dos Tipos de Russell

A *teoria dos tipos* é o ramo da matemática que se preocupa com a classificação de entidades (elementos de conjuntos) em conjuntos chamados *tipos*.

A teoria dos tipos moderna foi criada, em parte em resposta ao *Paradoxo de Russell*, publicado em *Principia Mathematica*, dos filósofos e matemáticos britânicos **Bertrand Arthur William Russell** (1872-1970) e **Alfred North Whitehead** (1861-1947).

A resposta ao paradoxo veio do próprio **Bertarnd Russell**, com a introdução de sua **teoria dos tipos**. Embora primeiro introduzido por **Russell** em 1903 nos *Princípios*, sua *teoria dos tipos* encontra sua expressão madura em seu artigo *Mathematical Logic como base na Teoria dos Tipos* de 1908, e na obra monumental que ele escreveu, chamada *Principia Mathematica* (1910 , 1912, 1913), com co-autoria de **Alfred North Whitehead** (1861-1947). Sua idéia básica era que a referência a coleções problemáticas (como o conjunto de todos os conjuntos que não são membros de si mesmos que caracterizou o paradoxo sobre a teoria dos conjuntos de Cantor) poderiam ser evitados, organizando todas as sentenças em uma hierarquia, começando com frases sobre os *membros* no nível mais baixo, sentenças sobre *conjuntos de membros* no próximo nível mais baixo, sentenças sobre *conjuntos de conjuntos de membros* no próximo nível mais baixo, e assim por diante. Deste ponto de vista, segue-se que é possível, se referir a uma *coleção de objetos* para os quais uma determinada condição vale, se esses estão todos ao mesmo nível ou do mesmo "*tipo*".

Surge então, a ideia de *tipos* e a *teoria dos tipos*, que veio ser utilizada na ciência da computação, no sentido de se organizar espaço de dados em programas de computador. No último capitulo sobre Visáo Abstrata de Dados no volume II, o leitor verá que a *teoria dos tipos* deu origem às *classes* de objetos, e que se pode programar um computador segundo o paradigma da orientação a objetos. Em teoria dos conjuntos, uma *coleção* (também chamada de *classe*) é "quase"um conjunto, ou seja, classes tem várias propriedades em comum com conjuntos, mas não são, necessariamente, conjuntos. A ideia de uma coleção tem a ver com a definição de um multiconjunto (Bag Theory).

16.4 O Pré-Intuicionismo

Antes do *Intuicionismo*, um pequeno grupo de matemáticos não eram adeptos as ideias do logicismo no final do século XIX. Esse grupo, liderados por **Poincaré**, **Borel** e **Lebesgue**, formaram a escola pré-intuicionista Brouwer (2011). Essa escola não aceitava que os números naturais, o princípio da indução completa e qualquer entidade construída a partir deles, que fossem geradas puramente da lógica e da linguagem. Apesar desse pensamento romper com o logicismo nesses pontos, os pré-intuicionistas não foram muito além. Por exemplo, no caso dos reais, essa escola

não chegou a tentar procurar uma origem que fosse independente da lógica e da linguagem, como fizerampara os números naturais Brouwer (2011).

Além disso, ao contrário do que se verá no *intuicionismo*, grande parte dos pré-intuicionistas não chegavam a rejeitar o princípio do terceiro excluído, fato criticado por **Brouwer**. Entretanto, esse não foi o caso do matemático **Leopold Kronecker**, o qual também pode ser considerado um pré-Intuicionista. **Kronecker** não compartilhava da mesma visão queos outros adeptos dessa escola tinham sobre os números naturais. Mesmo assim, **Kronecker** ainda é considerado um pré-intuicionista, pois não aceitava provas *não construtivas*, como a construção dos reais feita por *Dedekind*. Dessa forma, ele já criticava a lei do terceiro excluído (essa é uma lei da lógica que diz que para qualquer sentença P, é válido P ou $\neg P$), antes mesmo dos trabalhos de **Brouwer**. Por agora, é importante notar que a rejeição desse princípio foi uma grande crítica à matemática clássica, pois, naquela época, diversos teoremas importantes tinham sido provados o utilizando como um argumento essencial.

Em desacordo com as posições anteriores, **L. E. J. Brouwer** afirma que a matemática chegou a paradoxos por ter-se afastado das intuições claras e dos métodos construtivos bem definidos, de modo que os métodos da lógica clássica que pode ser aplicada sem problemas a objetos concretos e em situações empíricas, são extrapolados de maneira abusiva quando aplicados na matemática. Em particular, rejeita o princípio de terceiro excluído e as demonstrações de existência de um objeto matemático que não são construtivas. Assim, Brouwer deu origem à corrente *intuicionista*, depois ramificada para constituir a corrente denominada *construtivista*.

16.5 O Intuicionismo

O *intuicionismo* nasceu em 1907, com a tese de doutorado com título "*On The Foundations of Mathematics*", escrita pelo matemático holandês **Luitzen Egbertus Jan Brouwer** (1881-1966).

O *logicismo* procurou achar uma base para a matemática através da lógica, se utilizando da forma clássica de pensar (ou seja, a forma utilizada durante o século XIX). Por sua vez, o *intuicionismo* tinha uma ideia bem contrária a essa forma de pensar, pois rejeitava que a matemática era um produto derivado da lógica. Para **Brouwer**, os princípios básicos da matemática (os axiomas) eram resultado da intuição, daí o nome pelo qual a escola é conhecida. Além disso, **os objetos da matemática só podem existir quando fossem criados a partir da produção da mente humana**, rejeitando, então, a visão *platonista*, de que objetos matemáticos são descobertos e, não criados pelo homem. **Para a corrente intuicionista, apenas existe em matemática, o que for construído, efetivamente criado pelo homem. As entidades matemáticas não são descobertas pelo matemático, mas criações suas.** Com base nessa visão, **Brouwer** considerava a matemática independente até mesmo da linguagem. Essa filosofia também criticava fortemente a

Figura 83 – Brouwer - *On The Foundations of Mathematics* que originou o intuicionismo.

Fonte: en.wikipedia.org.

matemática clássica, não aceitando provas que não fossem construtivas, ou seja, era uma filosofia construtiva (construtivismo). Esses primeiros trabalhos com ênfase nos fundamentos da matemática ficaram conhecidos como o "primeiro ato"do *intuicionismo* Ferreiros (2008).

Em 1918, **Brouwer** passa a desenvolver uma *teoria dos conjuntos* que é independente da *Lei do Terceiro Excluído*, rompendo com as teorias mais aceitas até então, a de **Cantor** e de **Zermelo**. Esse trabalho no desenvolvimento de uma *teoria intuicionista dos conjuntos* é chamado de "segundo ato"do intuicionismo Ferreiros (2008).

Como foi visto anteriormente, foi possível construir os reais a partir dos racionais utilizando a teoria dos conjuntos de **Cantor** a partir do método criado por **Dedekind**, mas essa construção não é aceita pelo intuicionismo, já que é não-construtiva. Além disso, o próprio axioma da escolha não é aceito do ponto de vista do construtivismo, pois apenas impõe a existência de uma escolha, mas não explicita qual é essa escolha. O maior problema surge do fato de que a análise clássica é muito dependente tanto da construção dos reais como do axioma da escolha. Por isso, foi rejeitada pelo intuicionismo e, então, desenvolver uma teoria intuicionista dos conjuntos foi a forma encontrada por **Brouwer** para resolver esse problema. Mais detalhes sobre essa teoria e como ela chega nos reais de forma construtiva pode ser vista no ótimo trabalho em Ramos (2013).

Com o desenvolvimento da nova teoria intuicionista dos conjuntos, a comunidade matemática ficou dividida durante a década de 20. De um lado, os defensores da matemática clássica, liderados por **Hilbert**, de outro, os críticos liderados por **Brouwer**.

Na matemática, existem proposições que já são, a princípio, consideradas verdadeiras,

as quais são chamadas de *axiomas*. Excluindo os axiomas, qualquer outra proposição matemática precisa ser provada para ser considerada verdadeira. Dessa forma, um argumento matemático que demonstra de forma rigorosa que determinada proposição é verdadeira é chamado de prova. Porém, nem todas as formas de provas são aceitas por todos os matemáticos, sendo esse o caso dos intuicionistas. Um ponto fundamental do *intuicionismo* é que é uma escola não-clássica, ou seja, a única forma de prova aceita é a *prova construtiva*. Dado uma proposição, esse tipo de prova procura apresentar um exemplo que mostre que a proposição é verdadeira ou pode, ainda, fornecer um *algoritmo* que construa tal exemplo Weisstein (2013). Vale ressaltar que, por essa definição, a *matemática construtiva* é independente do próprio intuicionismo, sendo encontrados diversos exemplos de provas construtivas na matemática clássica.

16.6 O Construtivismo

No seção anterior, foi mostrada uma forma de matemática construtiva através das ideias do intuicionismo. O construtivismo, porém, não se limitou apenas a essa escola da matemática. A década dos anos 30 foi marcada por avanços na **teoria da computação** através dos trabalhos de **Alonzo Church** e **Alan Turing**. Esses trabalhos também foram de grande importância para o surgimento e desenvolvimento da *teoria da recursão*. Com isso, surgiu uma nova área da matemática chamada *matemática recursiva*. Essa área, assim como as demais áreas da matemática clássica, utilizava a lógica clássica.

Na década de 1940, o matemático **Andrei Andreyevich Markov**, na Figura 84, desenvolveu uma versão construtiva da matemática recursiva. Basicamente, **Markov** desenvolveu a *matemática recursiva* substituindo a lógica clássica pela lógica intuicionista Bridges (2013).

Figura 84 – Andrew Markov - A versão construtiva da matemática recursiva.

Fonte: apometriacuritiba.spaceblog.com.br.

Markov também criou a *cadeia de Markov*, um caso particular de processo es-

tocástico com estados discretos e apresenta a propriedade Markoviana, chamada assim em homenagem ao matemático **Andrei Andreyevich Markov**. A representação gráfica de uma cadeia de Markov é similar a de um autômato finito acrescentado de probabilidades em seus estados e transições.

Mesmo com o surgimento da *matemática construtiva recursiva*, o progresso do construtivismo foi lento durante a década de 1950 e durante metade da década de 1960. O principal motivo foi que em algumas áreas o construtivismo deixou a teoria extremamente complexa. Com isso, a comunidade matemática foi aos poucos perdendo o interesse. Entretanto, em 1967, o interesse foi renovado com o importante trabalho *Foundations of Constructive Analysis* (1967), do matemático **Errett Bishop** Bishop (1972). Por meio deste trabalho, ele conseguiu desenvolver de forma construtiva, grande parte da análise matemática do século XX, como em Bridges (2013). O trabalho de **Bishop** resultou em uma nova forma de construtivismo, conhecida como *construtivismo de Bishop*.

Figura 85 – Errett Bishop - Os fundamentos da análise construtivista.

Fonte: www-groups.dcs.st-and.ac.uk.

Bishop se interessou em questões fundamentais da matemática por volta de 1964, quando ele estava no Miller Institute. Ele escreveu *Foundations of Constructive Analysis*, que teve como objetivo mostrar que um tratamento construtivo da análise era viável.

Bishop decidiu refinar a forma de indicar que uma prova é não-construtiva. Para isso, utilizou os chamados *princípios da omnisciência*. Qualquer instância do princípio do terceiro excluído não pode ser provada por esse construtivismo. Assim, **Bishop** resolveu trabalhar particularmente em cima de uma dessas instâncias, a qual é chamada de *princípio da omnisciência* Lietz (2005). Esse princípio diz que, dado um conjunto A, ou todos os elementos de A tem uma propriedade P ou existe um elemento de A com a propriedade $\neg P$.

B. van Rootselaar, revisando o texto de **Bishop**, escreveu: -

"*A inspiração foi feita a partir de ideias de **Brouwer** modificados de modo a obter uma peça de matemática, que podusse ser considerada como construtiva e ao mesmo tempo se remontasse à matemática clássica, tanto quanto possível. O raciocínio subjacente à teoria é principalmente intuicionista, evitando o uso da negação. No entanto, uma boa dose do intuicionismo de **Brouwer** é rejeitado, notavelmente as suas noções de sequências de livre escolha, spreads (um conceito proposto por Brouwer) e o bar theorem (**Brouwer**). O princípio da não-construtivo de raciocínio clássico "Ou todos os elementos de A tem a propriedade P ou existe um elemento de A com propriedade não P"(o chamado princípio da onisciência) tem de ser evitado. Isso geralmente é feito restringindo as noções de tal forma que nem o princípio é trivialmente satisfeita ou não é necessário o apelo ao princípio.*"

Ao mesmo tempo em que **Bishop** escrevia a publicação citada anteriormente, um outro nome importante para o construtivismo, **Martin-Löf**, também estava trabalhando em uma publicação relacionada à análise construtiva. Ele começou a escrever a publicação *Notes on Constructive Analysis* em 1966, terminando em 1968. Como até a data de publicação ele nunca teve acesso ao trabalho de Bishop, a teoria utilizada nesse trabalho foi a da matemática construtiva recursiva e não o construtivismo de Bishop Bridges (2013). Apesar dessa publicação marcar o início dos trabalhos de **Martin-Löf** na matemática construtiva, a contribuição mais importante dele foi a criação e desenvolvimento de uma *teoria intuicionista dos tipos*. Essa teoria, além de uma importância teórica, já que serve como um fundamento para o *construtivismo de Bishop* Bridges (2013), tem uma grande *importância prática para a computação*.

16.7 Teoria Intuicionista dos tipos de Martin-Löf

Per Erik Rutger Martin-Löf (1942-...) é um lógico, filósofo, estatístico e matemático sueco, na Figura 86. É internacionalmente reconhecido por seu trabalho sobre os fundamentos da probabilidade, estatística, lógica matemática e ciência da computação.

Os avanços no construtivismo decorrentes do trabalho de **Bishop** permitiram que, em 1971, o matemático **Martin-Löf**desenvolvesse a chamada *teoria intuicionista dos tipos*. Entre as formas de construtivismo mostradas até aqui, a **teoria dos tipos é a que deixa mais evidente a relação entre o construtivismo e a computação**. O objetivo desse tópico será limitado a fazer uma introdução simples do que significa a teoria dos tipos e mostrar alguns dos seus usos na computação. Isso deve-se ao fato que é uma teoria bastante complexa, seria necessário um artigo inteiro para explicá-la de forma satisfatória.

Figura 86 – Martin Löf - A teoria intuicionista dos tipos.

Fonte: michaelt.github.io.

Para entender melhor a teoria dos tipos , pode-se pensar na teoria dos conjuntos. Na teoria dos conjuntos, o conceito principal é o conjunto e a partir dele, a teoria vai sendo construída. De forma semelhante funciona a teoria dos tipos, mas sendo o principal conceito os tipos. O próprio **Martin-Löf** falou algumas palavras que ajudam entender as ideias por trás dessa teoria. De acordo com ele, devemos pensar acerca de objetos matemáticos e construções. Todo objeto matemático seria de um certo tipo e sempre seria dado junto comesse determinado tipo. O tipo é definido descrevendo o que deve-se fazer para construir umobjeto desse tipo. Assim, um tipo seria bem-definido quando se sabe o que significa se ter um objeto desse tipo Bridges (2013).

Com essas palavras, **Martin-löf** acaba definindo informalmente o que é um tipo . Além disso, ele vai mais além, dando um exemplo. O exemplo é que o motivo das funções $\mathbb{N} \to \mathbb{N}$ serem um tipo, não é porque é sabido a existência de alguma função numérica em particular, como por exemplo, as funções recursivas primitivas (soma, multiplicação, ...), mas sim porque a noção de uma função numérica é bem entendida em geral Bridges (2013). Nessa introdução abreviada das ideias de **Martin-Löf**, já fica evidente a relação entre a **teoria dos tipos** e a **computação**. A forma que essa teoria interpreta os objetos matemáticos é semelhante a muitas linguagens funcionais, sendo um bom exemplo *Haskell*.

Em *Haskell*, todos os dados são associados a um certo tipo. Porém, o que deixa essa linguagem mais similar ainda, é que qualquer função ou expressão da linguagem também tem um tipo associado. Por causa dessas semelhanças, algumas linguagens funcionais mais recentes, como as linguagens *Epigram* e *Agda*, basearam-se diretamente na teoria de **Martin-Löf** (teoria dos tipos com l[ogica intuicionista). Além disso, uma outra grande importância é a relação entre essa teoria e o isomorfismo de *Curry-Howard*. De forma resumida, esse isomorfismo estabelece a equivalência entre programas e provas matemáticas. Isso é visto de forma bem clara na teoria de **Martin-Löf**, pois do jeito que ela é desenvolvida, facilita a extração de programas

a partir das provas Bridges (2013). É por isso que os conceitos da teoria dos tipos são bastante usados para desenvolver programas que tem como objetivo servir de assistente para provas.

16.7.1 O Construtivismo de Bishop

O *intuicionismo* de **Brouwer** teve sucesso na crítica da matemática clássica. Também é inegável a influência dessa escola para o desenvolvimento do *construtivismo*. Entretanto, **Brouwer** utilizou os novos conceitos do intuicionismo para a negação da matemática clássica. Por causa disso, ele acabou não se concentrando na relevância matemática que esses conceitos teriam para a matemática construtiva Lietz (2005). Além disso, com os trabalhos do segundo ato do intuicionismo, **Brouwer** focou no desenvolvimento de conceitos que não foram muito bem aceitos por boa parte da comunidade matemática. Diante disso, pode-se dizer que os trabalhos de **Brouwer** não foram tão importantes para o desenvolvimento do construtivismo e seus conceitos quanto foram para a negação da matemática clássica.

Até a metade da década de 1960, o *construtivismo* ainda estava intimamente ligado ao *intuicionismo*. Ora, até essa década, a única versão alternativa do *construtivismo* era a matemática construtiva recursiva de **Markov**. Entretanto, essa teoria, por sua vez, também estava fortemente associada ao *intuicionismo* , pois utilizava a lógica intuicionista. Como grande parte da comunidade matemática dessa época eram matemáticos clássicos, era natural que uma teoria que dependesse de uma outra que negava a matemática clássica não fosse popular. Diante desse contexto, era necessário surgir algum matemático que, de alguma forma, conseguisse encaixar o construtivismo na matemática clássica. Esse foi o papel que o matemático clássico **Ernett Bishop** assumiu ao desenvolver sua versão do *construtivismo*. No desenvolvimento de sua *teoria de construtivismo*, **Bishop** procurou não cometer o mesmo erro que **Brouwer**. Ou seja, não focou em negar resultados, mas sim, em construí-los.

16.7.2 Relações entre formas de construtivismo e a matemática clássica

Para melhor ilustrar as relações entre as diversas formas de construtivismo e a matemática clássica, pode-se utilizar a Figura 87. Considere **CLASS** como o conjunto que representa a **matemática clássica**, **INT** representa o **intuicionismo**, **BCM** a **matemática construtiva de Bishop** e **CRM** a **matemática construtiva recursiva de Markov**.

Por volta do final do século XIX e início do século XX, depois de muitas controvérsias na matemática, foram feitas muitas tentativas para revelar o valor de verdade das matemáticas. Seguindo a ideia de **Leibniz**, a necessidade de maior rigor foi percebida e estabelecida, através da iniciativa de **David Hilbert**. Ele tentava desenvolver uma formulação consistente e completa da matemática. A posição filosófica de **Hilbert** a respeito dos fundamentos da matemática é chamada de *formalismo*. Ele pretendeu

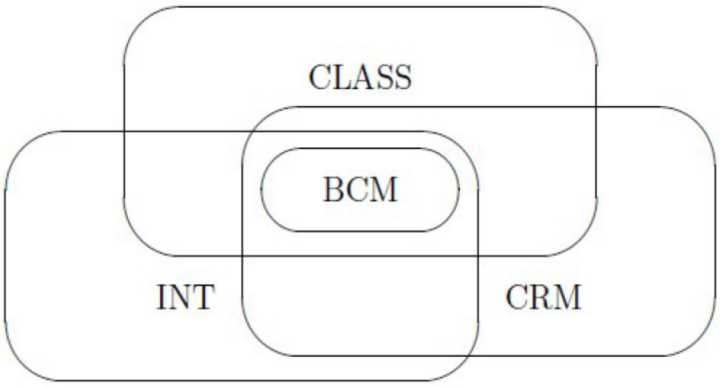


Figura 87 – A relação entre a matemática clássica e os diferentes tipos de construtivismo.

Fonte: Ph.D Thesis de Peter Lietz, "From constructive mathematics to computable analysis via the realizability interpretation".

reduzir o infinito a um sistema formal livre de contradições, cuja validade pudesse ser provada por meios finitários Carnielli e Epstein (2005) com um pequeno número de símbolos. Surgiu então a parceria entre a Lógica e a Matemática, chamada de lógica simbólica. Um sistema infinito de fórmulas definidas de modo finito, como será mostrado neste livro no capítulo 17.

Por causa da iniciativa de **Hilbert**, as matemáticas de hoje repousam inteiramente numa base axiomática. Fundamentam-se num sistema de símbolos sem relação direta com a realidade (não considera-se a semântica desses simbolos) e submetida as suas próprias regras, cuja característica dominante é uma completa submissão à lógica, também simbolizada e formalizada Omnes (1996). Por exemplo, como mostrado no capítulo 14, a aritmética se preocupa com as operações sobre os números naturais, mas na visão formalista, as custas de seus axiomas aritméticos (envolvendo operações aritméticas), mas para se provar propriedades sobre esses números e operações, precisa-se da lógica, com seus axiomas lógicos.

O importante nas matemáticas é construir provas, e os axiomas da lógica em que essas se fundamentam são supostamente os mais fundamentais. Os axiomas são considerados absolutamente gerais, conhecidos por intuição ou por tê-los extraídos da acumulução dos fatos. A corrente *formalista* então, se baseia na concepção *logicista* desenvolvida por **Bertrand Russel** e **Whitehead**, que, por sua vez, se esteia no *método axiomático* e, as vezes, é esquematizada dizendo-se que a matemática se reduz à lógica Omnes (1996). Mas, para os formalistas as matemáticas são inteiramente redutíveis à manipulação de símbolos. Assim, em meados do século XX, a axiomática tal como fora formulada por **Hilbert** e codificada pelos livros de **Bourbaki**, torna-se dominante e, também, muito relevante na concepção dos sistemas formais em que a ciência da computação se fundamenta. As matemáticas não nos interessam, aqui, por si mesmas, mas sim, por seus significados para as áreas da ciência da computação.

Hilbert, que no seu livro sobre os fundamentos da geometria (1899) reduziu a consistência dos axiomas da geometria aos da aritmética, estava muito interessado na consistência dos axiomas da aritmética. Uma questão originada naquela altura pelo debate sobre a **construtividade** e pelas aparentes contradições nos fundamentos. Com este propósito concebeu um método chamado *formalismo*: a redução das matemáticas a um "jogo" finito, com um sistema infinito de fórmulas definidas de modo finito. Além disto, as regras do "jogo" deveriam ser *consistentes*, isto é livre de contradições. Esta questão conduziu a uma área do pensamento chamada de *metamatemática* ou **teoria da demonstração**, uma ciência a um nível onde as matemáticas formalizadas podiam ser estudadas, os cículos viciosos evitados e as inconsistências eliminadas Struik (1987).

16.8 A Metamatemática

A **metamatemática**, um termo criado por **Jacques Herbrand**(1908-1931, 23 anos) em 1930, é a linguagem que trata do rigor matemático, sobre conceitos como o de *axioma*, *regra de inferência*, *demonstração formal ou dedução*, de *completude*,*consistência* e outros recursos envolvidas na construção de teorias da lógica e da própria matemática. A Teoria da Prova é inerente à metamatemática.

Herbrand foi um matemático francês que trabalhou com Lógica matemática. Ele submeteu seu principal estudo sobre da *teoria da prova* e *funções recursivas* gerais, no seu trabalho intitulado "*On the Consistency of Arithmetic*"(Sobre a Consistência da Aritmética) no início de 1931. A Figura 88 mostra uma foto de Herbrand aos 23 anos, pouco antes de sua morte trágica, ao praticar alpinismo numa montanha na França. As ideias de **Herbrand** sobre funções recursivas vieram a contribuir definitivamente na Ciência da Computação. **Gödel**, **Church**, **Kleene**, **Rosser** e **Turing** prosseguiram suas ideias.

Figura 88 – Jacques Herbrand - Sobre a consistência da aritmática.

Fonte: http://pt.wikipedia.org/wiki/Jacques_Herbrand.

Enquanto o ensaio de **Herbrand** intitulado "*Sobre sentenças formalmente indecidíveis do Principia Mathematica e sistemas relacionados I*" estava sendo examinado, **Gödel** anunciou a impossibilidade de formalizar a prova de consistência de uma teoria suficientemente forte dentro dessa própria teoria.

Herbrand estudou o ensaio de **Gödel** e escreveu um apêndice para o seu próprio estudo, explicando porque o resultado de **Gödel** não contradizia o seu. Mas, em julho de 1931, **Herbrand**, acidentalmente, faleceu e, seu trabalho "*On the Consistency of Arithmetic*" foi publicado após sua morte.

David Hilbert, **Kurt Gödel**, **Jacques Herbrand** e **Alfred Tarski** (1901-1983), um lógico, matemático e filósofo polonês, foram os idealizadores da **metamatemática**. **Tarski** migrou para os Estados Unidos e tornou-se cidadão naturalizado e foi professor de matemática da Universidade da Califórnia em Berkeley, de 1942 até sua morte. **Tarski** escreveu, dentre outras áreas, sobre topologia, geometria, teoria da mensuração, axiomatização da álgebra e geometria, fundamentação da semântica, lógica matemática, teoria dos conjuntos, metamatemática, e, especialmente, sobre teoria dos modelos, teoria semântica da *verdade*, álgebra abstrata e lógica algébrica. Seu trabalho possui grande relevância filosófica. Juntamente com **Aristóteles**, **Frege** e **Gödel**, é considerado um dos maiores lógicos da história. Na filosofia, ganha destaque especialmente por suas caracterizações matemáticas dos conceitos de *verdade*, constante lógica (*true*) e consequência lógica para sentenças de linguagens formalizadas classicamente. Na matemática, sua fama deve-se principalmente a seus trabalhos sobre teoria dos conjuntos, teoria dos modelos e álgebra.

Figura 89 – Alfred Tarski: Filosofia, Lógica e Matemática.

Fonte: dokumente.unibw.de.

Caracterizando a metamatemática, enquanto trata dos axiomas, a metamatemática não é parte específica da matemática. Ela é a linguagem com que se fala da matemática, sem ser a própria matemática. É apenas uma aplicação de axiomas gerais a casos particulares da matemática.

Hilbert não participa da ideia de unificar a lógica e a matemática, mas considera que a formalização da lógica que culmina na obra de **Frege** é uma parte importante de uma outra resposta. **Hilbert** propõe a formalização e axiomatização das diferentes áreas da matemática, para assim poder dar uma demonstração da consistência de essas teorias, ou seja, de que não é possível a derivação de contradições nelas, constituindo a base do Programa de Hilbert e o início da corrente formalista. A corrente formalista foi continuada por figuras como **Paul Bernays**, **Stephen Kleene**, **Haskell B. Curry**, **Ernst Zermelo** e **John von Neumann**.

Paul Isaac Bernays (1888-1977) foi um matemático suíço. Contribuiu significativamente com a lógica matemática, teoria axiomática dos conjuntos e filosofia da matemática. Foi um assistente e grande colaborador de **David Hilbert**.

Haskell B. Curry (1900-1982) foi um matemático e lógico estadunidense, conhecido por seu trabalho na lógica combinatória. O paradoxo de **Curry** é um paradoxo que ocorre na teoria dos conjuntos ingênua, e permite a derivação de uma sentença arbitrária de uma sentença auto-referente e algumas regras de dedução lógica aparentemente inócuas. É assim denominado em referência a **Haskell Curry**. Seu interesse por lógica matemática começou quando ele conheceu *Principia Mathematica*, de **Alfred North Whitehead** e **Bertrand Russell**. Ainda em Harvard, **Curry** começou um Ph.D. em matemática. Enquanto dirigido por **George Birkhoff** para trabalhar em equações diferenciais, seu interesse continuava na lógica. Em 1927, enquanto era instrutor na Universidade de Princeton, se mudou para a Universidade de Göttingen, onde pôde trabalhar com **Paul Bernays**. **Curry** foi supervisionado por **David Hilbert** e trabalhou com **Bernays**, recebendo o grau de Ph.D. em 1930 com uma obra sobre lógica combinatória.

Haskell dá nome a uma linguagem de programação puramente funcional, de propósito geral, nomeada em homenagem ao lógico **Haskell Curry**. Como uma linguagem funcional, a estrutura de controle primária é a função.

Haskell é a linguagem funcional sobre a qual mais se realizam pesquisas atualmente. Muito utilizada no meio acadêmico. É uma linguagem nova, elaborada em 1987, derivada de outras linguagens funcionais. Ela se baseia em um estilo de programação em que se enfatiza mais o que deve ser feito (*what*) em detrimento de como deve ser feito (*how*). É uma linguagem que possui foco no alcance de soluções para problemas matemáticos, clareza, e de fácil manutenção nos códigos, e possui uma variedade de aplicações.

Figura 90 – Haskell Curry - Ele dá nome a uma linguagem de programação funcional, muito ensinada e utilizada nos tempos de hoje.

Fonte: https://www.google.com.br/?gws_rd=ssl#q=Haskell+B.+Curry.

16.9 O Reordenamento pela Axiomática

Como apontado em Omnes (1996), o período de reordenamento das matemáticas pela axiomática, estende-se de 1850 a 1950. Neste período podemos citar grandes nomes, como **Hermann Grassmann** (1809-1877), quem desenvolveu a álgebra linear; **Karl Weierstrass** (1815-1897), que forneceu as bases da teoria das funções analíticas, base da implementação de funções em bibliotecas de linguagens de programação; **Richard Dedekind**(1831-1916) com a teoria dos anéis (polinômios); **Georg Cantor** (1845-1918) com as ideias da teoria dos conjuntos; **Gottlog Frege** (1848-1925) com a ideia do *Cálculo dos Predicados*; **Giuseppe Peano** (1858-1932), com a caracterização dos números naturais e os princípios de indução matemática usadas em muitas provas da computação teórica; **David Hilbert** (1862-1943), quem touxe à luz, nas origens da ciência da computação, sobre a ideia de problemas decidíveis (decidibilidade) na teoria da computabilidade; **Alfred Whitehead** (1861-1947) e **Bertrand Russel** (1872-1970), sobre os fundamentos da matemática, e que juntamente com **Bertrand Russell**, escreveu *Principia Mathematica*, livro que foi classificado pela *Modern Library* como o vigésimo terceiro de uma lista dos cem mais importantes livros do século XX; **Kurt Gödel** (1906-1978), que mostrou a inconsistência da "consistência"proposta por **Hilbert**.

Seguindo a proposta de **Hilbert**, **Zermelo** propõe em 1908 um sistema de axiomas para fundamentar a teoria de conjuntos, evitando os paradoxos conhecidos, como os de **Cantor**, **Burali-Forti** e **Russell**. Com contribuições posteriores, essa teoria deu lugar à Teoria de Conjuntos de Zermelo-Fraenkel com o axioma da escolha, ZFC, na qual pode ser formalizada a maior parte da matemática atual. Essa teoria é geralmente formalizada na lógica de primeira ordem com igualdade e tem como único símbolo não lógico não definido, a relação de pertinência.

Todos estes mencionados nesta seção, sem podermos entrar em todas as suas contri-

buições, nem nos esquecermos que outros nomes participaram dele. De certa forma, a maior parte desse movimento foi finalmente formalizada, durante 30 anos (1939-1968), pela grupo de matemáticos franceses em sua maioria, que assinava pelo pseudônimo coletivo de *Nicholas Bourbaki*. A corrente formalista terminou por influenciar a aparição da ciência da computação.

16.10 Métodos Construtivos e Métodos Axiomáticos na Computação

Vislumbrando as caraterísticas da matemática apontadas, podemos verificar o estreito laço entre o que caracteriza as matemáticas e o que caracteriza a construção de sistemas da computação, pois tais características dizem bem repeito à criação dos sistemas, quanto as formas com que um cientista da computação pode construir um sistema, seguindo a ideia de um *método construtivo* ou de um *método axiomático*. Ambos os métodos podem ser utilizados quando se começa a construir um sistema de computação, especificando o seu comportamento (que precisa ser validado) ou suas propriedades (que precisam ser verificadas). Em ambas as abordagens podemos nos valer dos formalismos apropriados a cada um dos métodos. Existem duas formas importantes para a ciência da computação, de seguir os métodos de construção da matemática Janos (2009):

- A primeira, defende os **métodos construtivos** (**construtivismo**). Para esses a ideia é de que somente existe na matemática, aquilo que efetivamente pode ser construído de forma finita. Do ponto de vista da construção de um sistema de computação, os métodos construtivos são aqueles que descrevem um modelo abstrato, através de uma especificação, dizendo como o sistema deve se comportar. Com os métodos construtivos podemos construir especificações mais detalhadas, que descrevem outras especificações mais simples, visualizando-se o sistema sendo especificado em níveis de abstração. Como então, estar seguro de que o comportamento do nível mais detalhado corresponde ao comportamento do nível mais simplificado? Constroí-se o sistema contendo niveis de abstração dos mais altos para os mais baixos, os níveis ser validados, fazendo a validação do mais detalhado contra o mais simplificado. O leitor pode conhecer, como exemplo, o método construtivo como está em Milner (1989), que apresenta a linguagem de especificacão algébrica de um *Calculus of Communicating Systems* (CCS), e ensina métodos de validação no sentido aqui imaginado.

- A segunda corrente, diz respeito aos **métodos axiomáticos** ou **orientados à propriedade**, também chamada de (**formalismo**). Esses defendem que não existem objetos matemáticos, são requeridos pelas lógicas, onde existem axiomas, definições (termos, símbolos funcionais e símbolos predicativos), teoremas, fórmulas, que podem ser usados diretamente para afirmar propriedades dos objetos matemáticos. Em termos matemáticos, por exemplo, para os formalistas não existe, *a priori*, um conjunto de números naturais, o que fazemos é criá-lo

através de um conjunto de axiomas. Da mesma forma, do ponto da construção de uma sistema de computação, os métodos axiomáticos são aqueles que afirmam quais propriedades o sistema deve possuir. O importante nesses métodos é expressar as propriedades requeridas de forma precisa e inteligível. O leitor pode entender métodos axiomáticos em Vasconcelos (1989), que descreve vários exemplos de aplicações de *lógicas temporais* na especificação de propriedades de sistemas de computação.

A idéia de considerar **a matemática como um sistema formal** empolgava os matemáticos do século XIX. Os resultados obtidos naquela época, precedentes à invenção do computador, é que o computador seria um sistema lógico, e portanto, seria um sistema formal. O que acabou por se concretizar nos tempos atuais. O **formalismo** e o**construtivismo**, acabaram sendo as duas correntes filosóficas usadas para se construir, em suas etapas iniciais, os sistemas de computação.

16.11 Bibliografia e Fonte de Consulta

Newton da Costa - Introdução aos Fundamentos da Matemática, Editora Hucitec, 2008.

Set Theory and Foundations of Mathematics - http://www.settheory.net/

Frege, Gottlob - Die Grundlagen der Arithmetik: eine logisch-mathematische Untersuchung über den Begriff der Zahl. Breslau: W. Koebner, 1884.

Frege, Gottlob - Grundgesetze der Arithmetik. Jena: Hermann Pohle, 1893-1903.

ZERMELO, Ernst. (1908). "Untersuchungen über die Grundlagen der Mengenlehre. I"(em alemão). Mathematische Annalen 65 (2): 261?281. Reimpresso com tradução ao inglês em Zermelo 2010, pp. 188?229, e tradução ao inglês em van Heijenoort 1967, pp. 199?215.

ZERMELO, Ernst. Collected Works - Gesammelte Werke (em alemão e inglês). Heidelberg: Springer, 2010. vol. I. ISBN 978-3-540-79383-0

FRAENKEL, Abraham A.; BAR-HILLEL, Yehoshua. Foundations of Set Theory. Amsterdam: North Holland (Elsevier), 1958.

Curry, Haskell (1934), "Functionality in Combinatory Logic", Proceedings of the National Academy of Sciences, 20, pp. 584-590

Curry, Haskell B.; Feys, Robert (1958), Combinatory Logic Vol. I, Amsterdam: North-Holland, with 2 sections by William Craig.

16.12 Referências - Leitura Recomendada

Brouwer, L.E.J. (1976). "On the significance of the principle of excluded middle in mathematics, especially in function theory". Em van Heijenoort, Jean. A Source Book in Mathematical Logic, 1879-1931. Cambridge MA. pp. 334-345. ISBN 0-674-32449-8.

HEIJENOORT, Jean van. From Frege to Gödel: a source book in mathematical logic, 1879?1931 (em inglês). Cambridge, Massachusetts: Harvard University Press, 1967.

Surgimento dos paradoxos - https://pt.wikipedia.org/wiki/Fundamentos_da_matemática#vanHeijenoort1967fregetogodel, p. 104-112, p. 124-125.

David Hilbert: The Foundations of Mathematics (1927)

Kurt Gödel: The modern development of the foundations of mathematics in the light of philosophy (1961)

Solomon Feferman: The development of programs for the foundations of mathematics in the first third of the 20th century

Stephen G. Simpson: What is Foundations of Mathematics?

Stephen G. Simpson: Logic and Mathematics Set Theory and Foundations of Mathematics

CAPÍTULO 17

Os Sistemas Formais na Ciência da Computação

Os sistemas formais da matemática e da lógica embasam matemática e logicamente a ciência da computação. Há forte associação entre estas ciências, de modo que os sistemas formais da **Álgebra**, da **Lógica** e do **Cálculo**, alicerçam, matematicamente, a ciência da computação. Os formalismos da matemática e da lógica, e como surgem na ciência da computação, precisam ser explicados. O capítulo diz respeito ao que os formalistas da escola de **Hilbert** estabeleceram. Come;amos com uma breve história que recapitula o conteúdo dos capítulos anteriores.

17.1 Breve História dos Sistemas Axiomáticos

O site de **Fernando Vieira Costa Júnior** nos proporciona uma breve história do surgimento da ideia do método axiomático de se realizar provas. Desde os tempos dos períodos paleolítico e neolítico que o homem, ainda caçador-coletor, migra de um lugar para o outro em busca de alimento e melhores condições de vida. A partir do período neolítico, já se utiliza de sistemas de contagens primitivos, como para contagem de rebanhos. No entanto, podemos afirmar que a Matemática só começou a surgir há 6000 a.C., depois da agricultura. Há 4000 a.C., os egípcios utilizavam o rio Nilo a seu favor, construindo plantações nas proximidades ou fazendo irrigações. Surge um problema. Em época de cheia do rio, as águas destruíam as marcações das terras, gerando grande confusão entre seus proprietários. Ver o capítulo 2.

Como solução para este problema, os egípcios passaram a medir a terra de forma a saber qual era a medida exata do terreno de cada um. Este é considerado o fundamento da Geometria (geo: terra, metria: medir). Dessa forma, os agrimensores (funcionários dos faraós que tinham a tarefa de medir a terra) desenvolveram formas de calcular áreas de triângulos e retângulos. Estes e outros conhecimentos possibilitaram, posteriormente, a construção das pirâmides e outros monumentos egípcios. Ver o capítulo 2.

Embora os egípcios já tivessem um grande estoque de conhecimento geométrico, somente na Grécia, no século IV a.C., foram feitas as primeiras demonstrações de teoremas. **Talles de Mileto** (625 a.C.-545 a.C.) é considerado o instituidor da geometria na Grécia. Este, assim como **Pitágoras de Samos** (570 a.C-495 a.C.) e outros geômetras antigos, realizaram várias demonstrações e descobriram muitos outros teoremas. No século III a.C., **Euclides** percebe um problema: haviam muitos teoremas demonstrados, mas existiam outros muitos aceitos sem uma devida demonstração. Alguns destes geravam dúvidas, fazendo com que houvesse a necessidade de revisar o estoque de teoremas aceitos sem demonstração. Ver o capítulo 2.

Como solução para este problema, **Euclides** pensou em reduzir a quantidade de sentenças aceitas sem demonstração a algumas poucas, claras e intuitivamente evidentes (menos uma que deu problema depois). A estas, ele deu o nome de *axiomas* (sentenças matemáticas gerais) e postulados (sentenças geométricas). Hoje consideramos *axiomas* e *postulados* como sendo a mesma coisa. A partir de quatro axiomas e cinco postulados, **Euclides** conseguiu demonstrar uma gama enorme de teoremas da geometria. Ficou assim instituído o conceito de *Sistema Axiomático*. A matemática utilizou deste método para desenvolver-se por mais de 2000 anos. Na realidade, por esse período a validade deste método sequer foi questionada. Ver o capítulo 2.

Os estudos de **Aristóteles** (384 a.C-322 a.C.), além de outros gregos, foram de suma importância para o desenvolvimento da Lógica, disciplina que fundamenta o pensamento das disciplinas dedutivas atuais. Vale lembrar que os trabalhos lógicos de **Aristóteles**, como a *Teoria do Silogismo*, derão a ele o título de pai da Lógica. De fato, as demonstrações futuras, pós-**Euclides**, levam em consideração conceitos da *Lógica Aristotélica* (ou **Lógica Clássica**). Porém, mesmo 2000 anos depois, uma demonstração ainda consistia numa atividade intelectual que objetivava convencer o próprio indivíduo e outras pessoas da verdade da sentença em discussão TARSKI (2007). Não haviam limites bem definidos para a argumentação. O processo de prova de teoremas ainda estava envolto pela tentativa de persuasão. Assim como a geometria grega pré-euclidiana tratava das verdades geométricas, o exigido numa demonstração, até aqui, era que o argumento fosse intuitivamente evidente. Aqui vale a pena rever os capítulos 2 e 7.

Nesse ponto, era cada vez mais discutido na academia que esse processo de argumentação necessitava de uma análise mais profunda. Surge o período das grandes controvérsias na Matemática (ver as correntes filosóficas destas controvérsias da Matemática no capítulo 16), tarefa levada a cabo por lógicos e não lógicos, a começar por **Gottlob Frege** (1848-1925). A análise desta forma de argumentação culminou na instituição da noção de *demonstração formal*. Similarmente à atitude de **Euclides** frente à grande quantidade de sentenças geométricas intuitivamente aceitas, as formas de argumentação, ou melhor, as formas de afirmação de novas sentenças (as regras de inferência) deveriam sofrer uma redução a algumas poucas regras de inferência primitivas, das quais deveriam derivar todas as demais. Uma linguagem para a matemática foi completamente formulada. Os sistemas axiomáticos passaram a

ser **Sistemas Formais**, ou seja, a validade de suas sentenças e inferências estão diretamente ligadas à forma (no sentido estrutural) com que se apresentam.

Para que um sistema seja um **Sistema Formal**, ele deve: (a) ter um alfabeto, que deverá conter todos os caracteres utilizados na linguagem a ser formalizada; (b) conter um conjunto de regras de formação, que permitirão decidir se uma sequência de caracteres da linguagem forma uma sentença dela; (c) conter um conjunto de axiomas, isto é, um conjunto de sentenças bem formadas aceitas (afirmadas) sem demonstração; (d) conter um conjunto de regras de inferência primitivas (ou regras de transformação primitivas), que permitirão obter (derivar) novas sentenças a partir dos axiomas ou de sentenças já obtidas anteriormente. Foi o que **Hilbert** defendeu: a corrente filosófica chamada de **Formalismo**. Ver no capítulo 14.

A partir de um sistema formal, pode-se demonstrar formalmente todas (ou quase todas) as sentenças verdadeiras desse sistema. Essa noção permite transpassar o problema da argumentação, pois não se pode argumentar para além das regras de inferências primitivas, ou das regras de inferência que são derivadas das primitivas, o que põe um limite às possibilidade de afirmação de novas sentenças. As demonstrações passam a ser demonstrações formais. Ver o capítulo 15.

Finalmente, uma demonstração, influenciada pela corrente filsófica chamada **Logicismo** (ver o capítulo 16) é uma sequência finita de sentenças, onde as primeiras são os axiomas (ou sentenças primitivas) do sistema, depois, todas as sentenças posteriores da sequência, podem ser obtidas a partir das sentenças anteriores, ou através da aplicação de algumas regras de inferência primitiva, ou de alguma regras de inferência demonstrada a partir das regras primitivas, e a última sentença da sequência corresponde ao que se chama *teorema*.

A partir do reordenamento do método axiomático (ver no capítulo 16), a corrente filosófica formalista consegue enorme influência, para a Matemática moderna e que contribui para alicerçar a **Ciência da Computação**, objetivo deste capítulo. Esses moldes ficaram como a base de toda a Matemática desenvolvida dos tempos de **Hilbert** em diante. O problema das demonstrações foi resolvido, sem deixar espaço para persuasão dos períodos tão remotos. O que vem nas seções posteriores diz respeito aos Sistemas Formais como vistos na Ciência da Computação.

Desde os seus começos, a Álgebra se preocupou sempre com a procura de métodos gerais e rigorosos. Assim por exemplo, R.J. Gillings em (*Mathematics in the times of the Pharaohs*) comentando os métodos que os egípcios usavam para lidar com a resolução de equações diz - Os estudiosos da história e filosofia da ciência do século vinte, ao considerar as contribuições dos antigos Egípcios, se inclinam para atitude moderna de que um argumento ou prova lógica deve ser simbólico para ser considerado rigoroso.

17.2 O que são Sistemas Formais

Formal se refere a forma. Portanto, sistemas formais são sistemas de manipulação de formas, sem a preocupação do que estas formas significam no mundo real Barreto (2000).

- A essência de um sistema formal é, portanto, sua **sintaxe**.
- Inclui-se ainda o estudo , de maneira abstrata, utilizado para se poder descrever as semânticas das linguagens de programação.

Conforme Barreto (2000), o primeiro registro que se tem de um sistema formal são os trabalhos de Euclides (300 a.C). Esses trabalhos organizaram e sistematizaram todo o conhecimento da época com relação à geometria euclidiana e são conhecidos sob o nome **Os Elementos**. No trabalho de **Euclides**, pela primeira vez, a apresentação é feita através de definições, axiomas, postulados, teoremas, corolários, e demonstrações. É neste trabalho que se encontram as raízes dos conceitos de uso atual.

Criadores dos Sistemas Formais Atuais - René Descartes (1596-1650) e de Leibniz (1646-1716) sôbre e alfabetos completaram o arcabouço básico de sistemas formais. **Frege** (1848-1925), **Peano** (1858-1932), **Whitehead** (1861-1947) e **Bertran Russel** (1872-1970) e finalmente **Wittgenstein** (1889-1951) criaram a formalização, como se costuma apresentar nos dias de hoje. **Kurt Gödel** enunciou teoremas dando os limites dos sistemas formais.

17.3 Construção de um Sistema Formal

Como descrito por em Barreto (2000), na construção de um sistema formal deve-se concentrar atenção no modo como se trabalha. Linguagens naturais (aquelas usadas entre seres humanos para se comunicarem) possuem ambiguidades que impedem o seu uso para este propósito. Portanto, torna-se necessário, dar um passo na direção de evitar estas ambiguidades, o que é realizado aplicando uma linguagem constituída por um conjunto bem definido de e de , permitindo a construção de novos objetos a partir daqueles que se dispõe.

Definição (**Alfabeto e Cadeias Finitas**)

- Um alfabeto é um conjunto finito de símbolos, denotado por letras gregas maiúsculas. Exemplos: Φ ou Σ.
- Costuma-sa ainda com relação a alfabetos, usar os seguintes símbolos:
  1. O conjunto de todas as cadeias (em inglês, *strings*) finitas formadas com os elementos do alfabeto Φ é denotado por Φ^*.
  2. A cadeia vazia, ou seja, aquela que tem 0 elementos é denotada por ϵ.

3. O conjunto $\Phi^* - \epsilon$, isto é, o conjunto de todas as cadeias finitas a partir do alfabeto Φ, excluida a cadeia vazia, será denotado por Φ^+.
4. O comprimento de uma cadeia é o número de elementos da mesma. O da cadeia μ denota-se $\rho(\mu)$ ou $|\mu|$.

Regra de Derivação

Seja o alfabeto Φ e seja $n \in \mathbb{N}$ um número natural. Uma **regra de derivação** é uma função:

$$F : \Phi^{*^n} \rightarrow \Phi^*$$

Exemplo Barreto (2000): Sejam os dois elementos de $\Phi^* = \{..., (xy), (car'), ...\}$, uma será:

$F : ((xy)(car')) \rightarrow (car'(xy))$, que também se escreve na forma de regras como:

$\frac{(xy)(car')}{(car'(xy))}$

Definição (Uma Linguagem)

Seja um alfabeto de símbolos Φ e o conjunto de objetos sintáticos (cadeias de símbolos) relativo a este alfabeto, onde um cadeia é uma sequência finita de símbolos de Φ. Uma linguagem é um subconjunto L de Φ^*, isto é, $L \subseteq \Phi^*$.

Quando é preciso explicitar o , denota-se, L_Φ ou $L(\Phi)$.

Exemplo (Uma linguagem Imperativa $\mathcal{L}_1$) Barreto (2000)

As linguagens imperativas são orientadas a ações, onde a computação é vista como uma sequência de instruções que manipulam valores de variáveis. O fundamento da programação imperativa é o conceito de máquina de Turing, que nada mais é que uma abstração matemática que corresponde ao conjunto de funções computáveis. A sua criação foi influenciada pela arquitetura de computadores **John von Neumann**, onde programas e dados são armazenados na mesma memória. Os operandos das expressões são passados da memória para a CPU e o resultado da expressão é passado de volta para uma célula da memória. São caracterizadas por três conceitos: Variáveis, Atribuição e Repetição.

$\Phi = \{;\ ,\ begin, end, if, then, else, while, do, E, \alpha, \beta\}$

Usando esta linguagem $\mathcal{L}_1$ podemos escrever um exemplo de programa de computador Barreto (2000), como descrito a seguir:

begin

while E_1 do C_1 ; C_2 end;

end;

if begin then while E_1 else do C_2;

begin

If E_1 then C_1; C_2 else C_3; C_4 end;

end;

Definicão (**Sistema Formal**)

Sistemas formais costumam ser representados por letras gregas maiúsculas, como por exemplo: Γ, Π, Σ, Ω, Ξ ou Ψ. Aqui nós usamos Ψ.

Um sistema formal Ψ é um par constituído por objetos sintáticos de uma linguagem Φ e um **sistema dedutivo**, consistindo de um conjunto D chamado, genericamente, de **regras de derivação**. É denotado por $\Psi =< \Phi, D >$, onde Φ é uma linguagem e D é um *sistema dedutivo*, um conjunto de regras de derivação que deriva regras. **Regras de derivação** são funções $F : \Phi^{*^n} \rightarrow \Phi^*$.

Definições Interessantes

O que é formalmente um *cálculo*? Este conceito nunca é explicado a contento, principalmente para um real e completo entendimento de alunos iniciantes. Informalmente, o sistema dedutivo de um sistema formal é o que vem a ser chamado de um **cálculo**.

Em função de um sistema dedutivo ser um cálculo, é necessário se entender o que vem a ser um *sistema dedutivo* e é importante, agora, o leitor entender o que vem a ser uma **inferência** ou *dedução*.

Definição (**Inferência ou Dedução**):

Seja um sistema dedutivo de um sistema formal e uma sequência de objetos sintáticos $O = (o_1, o_2, o_3, \ldots, os)$. Neste contexto, tem-se que, os objetos obtidos sucessivamente pela aplicação das regras de derivação $R = (r_1, r_2, r_3, \ldots, r_{s-1})$ de um sistema formal formam:

- R : uma **inferência** ou **dedução**;

- *O* : sequência de **passos da dedução**;
- *os* : a **conclusão** da dedução.

17.4 O que é uma Lógica

Uma lógica é um *sistema formal* que possui uma **linguagem** sobre a qual objetos sintáticos são gerados.

Para a Lógica Proposicional, a mais básica de todas as lógicas, mas que influiu na concepção do que viria a ser o computador digital, pode-se estudar a lógica consistindo de Manna (1985) Filho (2002):

Proposição é um termo usado em lógica para descrever o conteúdo de sentenças. Uma sentença é um conteúdo que pode ser tomado como verdadeiro ou falso. Diferentes sentenças podem expressar a mesma proposição quando têm o mesmo significado. Por exemplo, "A neve é branca." e "Snow is white." são sentenças diferentes, mas ambas dizem a mesma coisa, a saber, que a neve é branca. Logo, expressam a mesma proposição. Outro exemplo de sentença que expressa a mesma proposição que as anteriores é "A precipitação de pequenos cristais de água congelada é branca", pois "precipitação de pequenos cristais de água congelada" é a definição de "neve". O conceito de sentença tem sentido semântico. O termo proposição é indicado quando se considera o caso mais abstrato, pois de uma proposição pode-se ter algumas sentenças de mesmo significado. Uma proposição é um tipo genérico para um conjunto de sentenças de mesmo significado. O que é o mesmo que dizer que uma sentença é um caso particular de uma proposição. Tanto faz, proposição ou sentença, ambas tem valor semântico verdade ou falso. Sentenças podem ser construídas a partir de proposições, por aplicação de conectivos lógicos.

- A linguagem, que define proposições abstratas, que no caso da Lógica Proposicional, são chamadas de **proposições**. A linguagem consiste dos símbolos de veracidade (**verdade** e **falso**) e dos *símbolos proposicionais abstratos*.
- conectivos lógicos sobre proposições: **not**, **and**, **or**, **if-then** (condicional), **inf-and-only-if** (bicondicional), **if-then-else**.
- Interpretação e o significado de uma sentença (a semântica da linguagem): verdade ou falso.
- Propriedades de proposições:
  - *válidas*,
  - *satisfatíveis*,
  - *contraditórias*,
  - *implicação*,

  - *equivalência*,
  - *consistência de um conjunto de sentenças*.

- Tabelas-verdade: método para determinar se uma sentença é válida.
- Árvores semânticas: um outro método para testar a validade de uma sentença.
- Prova de falsificação: uma método alternativo para testar a validade de uma sentença.
- Classes de sentenças válidas.
- Substituição de sentenças por sub-sentenças nos esquemas de sentenças válidas.
- Interpretação estendida: uma interpretação atribui valores (true ou falso) à proposições e estabalece a semântica.
- Conjunto de sentenças que implicam outra, também conhecido por consequência lógica.
- Equivalência lógica: proposições que são esquivalentes em termos da lógica (se-e-somente-se).
- Problemas que podem ser solucionados por lógica proposicional.

A Lógica dos Predicados **estende** a Lógica Proposicional. Pode-se estudar a Lógica dos Predicados em Manna (1985) ou explicada num livro mais básico como em Filho (2002). Numa forma bem mais rigorosa temos a obra em Loeckx e Sieber (1987):

- A linguagem, que define símbolos, , proposições e sentenças. A linguagem consiste dos símbolos de veracidade ou falsidade (*verdade* e *falso*), os símbolos-constantes, os símbolos-variáveis. Os e os que formam o conjuntos dos *símbolos abstratos*. Com estes se pode escrever as proposições e sentenças desta lógica.
- Definição dos *termos*: as expressões que denotam objetos da lógica, dadas por constantes, variáveis e funções.
- Definição das *proposições*: as expressões que relacionam objetos, tais como os *predicados*.
- Definição de *sentenças* em função das *proposições* e *operadores lógicos* sobre proposições.
- Definição das *expressões* da lógica em função das *sentenças* ou *termos*.
- Variáveis livres e ligadas: aqui aparecem os quantificadores $\exists$ e $\forall$.
- O significado de uma sentença (a semântica da linguagem): verdade ou falso.
- Interpretações.

- Regras e propriedades semânticas.
- Interpretações estendidas.
- Validade de sentenças fechadas (sentenças logicamnete válidas).
- Estabelecendo a não-validade.
- Conceitos adicionais: sentenças fechadas, satisfatíveis, contraditórias ou consistentes.
- Fecho universal e existencial.
- Prova de falsificação: uma método alternativo para testar a validade de uma sentença.
- Esquemas de sentenças válidas: classes de sentenças válidas.
- Modelos e consequência lógica: (implicação lógica) conjunto de sentenças que implicam outra, também conhecido por consequência lógica, que determinam o *Teorema da Dedução*.
- Equivalência lógica: proposições que são esquivalentes em termos da lógica (se-e-somente-se).
- Substituição de sentenças equivalentes.
- Esquemas válidos com substituição.
- Problemas que podem ser solucionados por lógica dos predicados.

A partir destas duas lógicas, a ciência da computação pode se valer de outras lógicas construídas de expressividade maior com relação as características computacionais nos sistemas de computação concorrentes ou distribuídos, como são os casos das lógicas temporais que podem ser construídas a partir da Lógica Proposicional e da Lógica dos Predicados. O leitor pode obter um trabalho muito bem explicado sobre lógica temporal em Vasconcelos (1989).

O sistema dedutivo de uma lógica

Além da linguagem da lógica, como se pode derivar (deduzir, numa lógica dedutiva) uma *sentença* a partir de um conjunto de sentenças ?

A partir do conceito de *interpretação*, um *modelo* e de **consequência lógica**, pode-se estabelecer a conexão entre o conceito de consequência lógica e o símbolo de implicação lógica ($\Rightarrow$), algumas vezes denotado por $\supset$, culminando com o *Teorema da Dedução*, com as *variáveis livres* trazidas sob controle.

Teorema da Dedução

O que é uma dedução Seja W um conjunto de sentenças e v_1, v_2 sentenças da Lógica dos Predicados. Então as seguintes duas implicações ocorrem:

1. $W \models v_1 \supset v_2$ implica $W \cup \{v_1\} \models v_2$
2. $W \cup \{v_1\} \models v_2$ implica $W \models \bar{v_1} \supset v_2$

onde, se v_1 é qualquer fórmula e sejam $x_1, x_2, ..., x_n$ todas as variáveis livres que ocorrem em v_1, então $\bar{v_1}$ denota a fórmula fechada como $(\forall\, x_1, \ldots, x_n).v_1$.

Em particular, quando $W = \{w_1, \ldots, w_n\}$ for finito, este teorema pode ser usado para reduzir o conceito de consequência lógica à aquele de validade lógica:

$\{w_1, \ldots, w_n\} \models v$ se, e somente se, $\models \bar{w_1} \supset \ldots \supset \bar{w_n} \supset v$

Neste caso, dizemos que v é um teorema deduzido (derivado) de W. Note que o conceito de consequência lógica envolve a semântica das sentenças da Lógica dos Predicados. Vejamos que o conceito de *consequência lógica* é que define o que vem a ser uma *teoria*. O conjunto das sentenças válidas logicamente da Lógica dos Predicados é particularmente interessante porque consiste de sentenças que sempre ocorrem, isto é, elas ocorrem em toda a teoria.

17.5 O que é uma Teoria

Uma teoria é um sistema formal. *Teoria* é o conhecimento descritivo puramente racional. Também pode ser entendido como forma de pensar e entender algum fenômeno a partir da observação. O termo é aplicado a diversas áreas do conhecimento, sendo que em cada área possui uma definição específica.

Em ciência, a definição de teoria científica difere bastante da acepção de teoria em senso comum: o de simples especulação. A palavra teoria é usada, no dia-a-dia, sempre de forma inadequada, como um abuso de linguagem, em situações de inexistência de partes práticas. Mas, na realidade, uma teoria é um sistema formal. O conceito moderno de teoria científica estabelece-se, entre outros, como uma resposta ao problema da demarcação entre o que é efetivamente científico e o que não o é.

Da Lógica dos Predicados (primeira ordem, pois quantifica variáveis), temos que o conjunto de fórmulas logicamente válidas é, particularmente de muito interesse, porque consiste de fórmulas que sempre ocorrem, ou seja, ocorrem em toda teoria de primeira ordem. Um cálculo é um modo de obter as fórmulas logicamente válidas em uma maneira puramente sintática. De fato, o método é mais geral e produz as consequências lógicas de qualquer conjunto de fórmulas. Na Lógica dos Predicados, a

definição não-construtiva da semântica não provê nenhuma indicação para um modo mecânico poder distinguir fórmulas válidas de fórmulas inválidas. Mas, nem tudo é perfeito. Embora, o conjunto de **fórmulas logicamente válidas** possam ser gerado em um modo mecanizado, num cálculo, esse conjunto de fórmulas logicamente válidas não é um conjunto **decidível**. Assim, não existe nenhum procedimento efetivo, para o qual seja dada uma fórmula da Lógica dos Predicados e esse possa decidir se ela é logicamente válida ou não.

O Cálculo da Lógica dos Predicados (chamado de Cálculo dos Predicados) é um cálculo **consistente** - tudo que pode ser provado é verdadeiro, e **completo** - tudo que é verdadeiro pode ser provado, para o conjunto de todas das fórmulas logicamente válidas. Dado que essas fórmulas são universalmente válidas, elas são bem gerais para revelar sobre aplicações específicas, como por exemplo, na Teoria dos Grupos, na Teoria do Números ou na Teoria do Inteiros não Negativos.

A questão surge, então, sobre a existência de um **cálculo** para uma tal **teoria** específica, e além disso, sobre a *decidibilidade* de uma tal teoria.

Definição: (O que é uma **Teoria de Primeira Ordem**)

Antes, precisamos definir o que vem a ser um **modelo** e o que é **consequência lógica**.

Definição: (**Modelo**)

O que é um modelo. Seja $W \subseteq WFF_B$. Uma interpretação é chamada um de W se, e somente se, toda fórmula w de W é válida para tal interpretação.

Definição: (**Consequência Lógica**)

O que é uma consequência lógica. Seja um conjunto de fórmulas $W \subseteq WFF_B$ de fórmulas da Lógica dos Predicados. Uma fórmula $w \in WFF_B$ é chamada uma consequência lógica de W, denotado $W \models w$ se, e somente se, w é válida para todo modelo de W.

Seja o **conjunto de fórmulas bem-formadas** da Lógica dos Predicados sobre uma base $B = (F, P)$, onde F é o conjunto de símbolos funcionais e P o conjunto dos símbolos predicativos da Lógica. Um subconjunto não vazio T de fórmulas bem-formadas (sentenças) é chamado de uma **teoria** sobre a base B, quando as seguintes duas condições ocorrrem:

1. (*Consistência*) Existe pelo menos um *modelo* para T.

2. (*Fechamento sobre consequência lógica*) Todas as consequêcias lógicas de T estão em T.

Note que, por definição, uma contém pelo menos todas as fórmulas logicamente válidas da Lógica dos Predicados, que é definida como sendo uma lógica de primeira ordem.

Se $W \subseteq WFF_B$ é um conjunto de fórmulas que tem ao menos um modelo, então o conjunto $CL(W)$ de todas as consequências lógicas de W é uma teoria. Esta propriedade provê um modo conveniente para se criar uma teoria: toma-se um conjunto de fórmulas com um *modelo* e forma-se o fecho de T sob consequência lógica.

17.5.1 A Construção de uma Teoria

A formalização de uma teoria divide-se em três etapas fundamentais. Na primeira etapa, inicialmente situa-se em um universo do discurso e escolhe-se uma linguagem simbólica ou formal para expressar as sentenças da teoria sobre tal universo. Na segunda etapa organiza-se as assertivas da teoria, dedutivamente, isto é, escolhe-se algumas assertivas como axiomas a partir dos quais outras assertivas podem ser gradativamente deduzidas. Nesta etapa, também exprime-se as propriedades dos termos do Universo de Discurso através de novos axiomas até que o significado desses termos não precise mais ser usados nas deduções. Na última etapa explicita-se o significado dos termos ordinários (fora do universo do discurso) e os princípios usados para decidir quando uma assertiva é consequência lógica de outras. O resultado destas etapas é uma teoria em que se abstraiu inteiramente o conteúdo semântico ou significados dos termos, restando apenas a sua sintaxe ou forma. A teoria estará completamente formalizada.

O universo de discurso em questão e a linguagem simbólica (formal) que descreve princípios lógicos adotados, diz respeito e é parte intrínseca à teoria. A segunda da parte dos axiomas, pode ser até separada e usada novamente em outros contextos. Um sistema formal consiste exatamente de uma linguagem formal e de uma abstração adequada aos princípios lógicos usados para decidir quando uma assertiva é consequência lógica de outras.

Definição (**O que é uma Teoria**)

O que vem a ser uma teoria? Seguimos a definição dada em Manna (1985). Uma **teoria** consiste de uma **linguagem** e um conjunto de **axiomas**. Uma excelente linguagem de uma teoria é a *linguagem da lógica de primeira ordem*, na qual nos restringimos aos *termos* constantes, os símbolos funcionais, e os símbolos predicativos, e a um vocabulário específico, o qual é um subconjunto particular dos símbolos permitidos na Lógica dos Predicados em geral.

Definição (**Vocabulário de uma teoria**)

O vocabulário de uma teoria é:

- Um subconjunto particular c_1, c_2, c_3, ... das constantes da lógica dos predicados.
- Um subconjunto particular f_1, f_2, f_3, ... dos símbolos funcionais da lógica dos predicados.
- Um subconjunto particular p_1, p_2, p_3, ... dss símbolos predicativos da lógica dos predicados.

Cada um dos três subconjuntos podendo ser finito ou infinito, vazio ou não-vazio.

Os termos, sentenças e expressões de uma teoria são aqueles termos, sentenças e expressões da lógica dos predicados, cujas constantes, símbolos funcionais e símbolos predicativos, todos pertencem ao vocabulário da teoria.

Definição (**Axiomas de uma teoria**)

Os **axiomas** de uma teoria são um conjunto de sentenças fechadas $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$, ... da teoria. Dizemos então, que a teoria é definida pelos seus axiomas. Note que não requeremos que um dado conjunto de axiomas seja finito.

Exemplo (**Teoria da Família**)

Suponha que nós gostaríamos de definir uma teoria dos relacionamentos em família. Na interpretação "familia"$\mathcal{I}$, nós temos em mente o domínio de um conjunto de pessoas, e intuitivamente podemos dizer:

$f(x)$ é o pai de x

$g(x)$ é a mãe de x

$p(x, y)$ significa y é um "parent" de x, significando que ("x foi gerado por y")

$q(x, y)$ significa y é um avô de x

$r(x, y)$ significa y é uma avó de x

Mais precisamente, $p_{\mathcal{I}}(d, e)$ ocorre se e é um "parent"de d, e assim por diante.

Assim, o vocabulário de uma teoria consiste dos simbolos funcionais f e g, dos símbolos predicativos p, q e r, e nenhum síbolo constante, neste caso.

Os axiomas da teoria são as seguintes conjuntos de sentenças fechadas:

$\mathcal{F}_1 : (\forall\ x)\ p(x, f(x))$, significando que (O pai de todo mundo é seu ou sua "parent".)

$\mathcal{F}_2 : (\forall\ x)\ p(x, g(x))$, significando que (A mãe de todo mundo é seu ou sua "parent".)

$\mathcal{F}_3 : (\forall\ x)$ e $(\forall\, y)\ \ [if\ (p, x)\ then\ q(x, f(y))]$, significando que (O pai de um parent é seu ou sua avô.)

$\mathcal{F}_4 : (\forall\ x)$ e $(\forall\, y)\ \ [if\ (p, x)\ then\ r(x, g(y))]$, significando que (A mãe de um parent é seu ou sua avó.)

Seja considerar o relacionamento entre os axiomas de uma teoria e a interpretação específica que temos em mente.

Definição (**modelo**, **validade**, **consistência**)

Uma interpretação $\mathcal{I}$ é um **modelo** para uma teoria, se cada axioma $\mathcal{A}_i$ é verdadeira sob $\mathcal{I}$.

Uma sentença fechada $\mathcal{S}$ de uma teoria é **válida** na teoria, se $\mathcal{S}$ é verdadeira para todo modelo da teoria.

Uma sentença $\mathcal{S}$ implica uma sentença $\mathcal{T}$ na teoria, se sempre que $\mathcal{S}$ é verdadeira sob um modelo para a teoria, $\mathcal{T}$ é também verdadeira sob o modelo.

Duas sentenças $\mathcal{S}$ e $\mathcal{T}$ são equivalentes na teoria, se $\mathcal{S}$ e $\mathcal{T}$ tem o mesmo valor-verdade sob todo modelo para a teoria.

Uma teoria é **consistente**, se existe pelo menos um modelo para a teoria.

Como consequência imediata desta definição, temos que todo axioma para uma teoria é válido na teoria. Também, se a teoria é inconsistente, ela não tem nenhum modelo, e, portanto, toda sentença é "vacuamente"válida na teoria.

Na definição de uma teoria, nós temos em mente que a interpretação que nós temos em mente é um modelo para a teoria. Em geral, contudo, existem muitos modelos para uma teoria.

O conjunto de teoremas em uma teoria são as sentenças, as quais são consequências lógicas dos axiomas da teoria.

17.5.2 Teorias Especiais de Primeira Ordem

Teorias de primeira ordem são importantes, devido a consistência e a completude proporcionadas pela Lógica de Primeira Ordem.

- O conjunto de todas as fórmulas logicamente válidas da Lógica dos Predicados sobre qualquer base (neste caso, W é o conjunto vazio ϕ, isto é, temos: $\phi \models_{\mathrm{w}}$

ou $\models_{\mathrm{w}}$.

- Teoria das ordens parciais estritas.
- Teoria das relações de equivalência.

17.5.3 Teorias com Igualdade

A relação de igualdade é uma importante ferramenta que requer tratamento especial. Nós desejamos definir uma teoria de igualdade sob aqueles modelos em que um símbolo predicativo binário é atribuído a uma relação de igualdade sobre um domínio, isto é, a sentença $p(t_1, t_2)$ é verdade sob uma interpretação $\mathcal{I}$, precisamente quando os termos t_1 e t_2 tem o mesmo valor sob $\mathcal{I}$.

As mais importantes teorias especiais para nós serão aquelas definidas em termos do princípio matemático da indução (que comportam igualdade). Este princípio é representado por um *esquema de axiomas* (um conjunto infinito de axiomas).

1 Teoria da Igualdade

2 Teoria das Ordens Parciais fracas

3 Teoria das Relações Associadas

4 Teoria dos Grupos

5 Teoria dos Pares

6 Teoria dos Inteiros não Negativos

7 Teoria das Strings (cadeias de símbolos de um alfabeto)

8 Teoria das Árvores (como estruturas de dados em computação)

9 Teoria das Listas (lista uma lista é uma estrutura de dados em computação)

10 Teoria dos Conjuntos

11 Teoria dos Multiconjuntos - Bag Theory

12 Teoria das Tuplas

As teorias do [1]-[5] são tidas como teorias onde se pode aplicar a *relação de igualdade*. As teorias do [6]-[12] são tidas como teorias onde se pode aplicar o *princípio de indução matemática*. Mais sobre teorias de primeira ordem, o leitor pode estudar em Manna (1985), obra que contém de início, a Lógica Proposicional, e em seguida A Lógica dos Predicados da mais simples à mais avançada.

17.6 O que é um Cálculo

Nesta seção, um método que provê um modo de obter as sentenças logicamente válidas em uma maneira puramente sintática. O método é mais geral e produz as consequências lógicas de qualquer conjunto de sentenças.

Para tal a lógica precisa de um sistema dedutivo, ou seja, deve-se contar com o que vem a ser chamado um **cálculo**, ou dizemos que existe um *cálculo* para a *lógica*. Esta foi a ideia dos formalistas da escola de Hilbert.

Além disso, porque a lógica é uma linguagem e se poder atribuir o significado (**semântica**) a objetos sintáticos, pode-se definir a noção de **validade** de uma sentença (uma fórmula bem-formada sintaticamente), isto é, verificar a validade de uma sentença da lógica, e a noção de **sentença logicamente válida**. Assim, o conceito de consequência lógica, pode ser estabelecido para um conjunto de sentenças (fórmulas bem formadas) da lógica, estabelecendo-se, assim, um *método de prova*.

Como mostrado em Loeckx e Sieber (1987), o **Cálculo de Predicados** é o sistema dedutivo da **Lógica dos Predicados**. Esta lógica é muito importante para a ciência da computação e, como já dissemos, estende a Lógica Proposicional, que é a primeira lógica a ser vista numa disciplina básica de ciência da computação, e que tem, também, o seu cálculo correspondente.

Definição (**O que é um Cálculo**) Loeckx e Sieber (1987)

O que é um cálculo? Seja SO algum conjunto de objetos sintáticos de uma linguagem. Um cálculo (também chamado de um sistema axiomático sobre SO é um par $C = (A, R)$, onde A é um conjunto finito de *esquemas de axiomas*, os quais são **subconjuntos decidíveis** de SO, e os elementos de um esquema de axioma são chamados *axiomas*. R é um conjunto finito de *regras de inferência*, as quais formam **subconjuntos decidíveis** de $SO^n \times SO$, $n \geq 1$.

Uma observação importante, neste momento, é que um **cálculo** é um **sistema dedutivo puramente sintático**, ou seja, seus objetos sintáticos são desprovidos de uma semântica formal.

Exemplo (**Esquema de Axioma**): Para um $SO = WFF_B$, o conjunto de *fórmulas bem-formadas* da Lógica dos Predicados, um *esquema de axioma* possível é:

$\{W \vee \neg W \mid W \in WFF_B\}$, onde W pode ser qualquer *fórmula bem-formada* da Lógica dos Predicados.

Se W for $(x = y)$, um axioma deste esquema, é por exemplo, $(x = y) \vee \neg(x = y)$. Um esquema de axiomas é uma *classe* de axiomas.

Definição (**Regra de Inferência**)

Uma regra de inferência, visualizada como uma relação **R**, pode ser definida na notação de conjunto por:

$\mathbf{R} = \{(s_1, ..., s_n, s) \in SO^n \times SO \mid \mathbf{P}\}$,

onde a propriedade **P** é uma propriedade decidível, geralmente alguma propriedade sintática, que ocorre para $s_1, ..., s_n, s$.

Ao invés desta notação uma regra de inferência é normalmente apresentada como:

$\mathbf{R}$: $\frac{s_1,....,s_n}{s}$, tal que P ocorre, para toda $s_1, ..., s_n, s$

$s_1, ..., s_n$ são chamadas de *premissas* e s, a *conclusão* da regra de inferência **R**.

Exemplos (**Regras de Inferência**)

Como mostrado em Loeckx e Sieber (1987), com $SO = WFF_B$ como o conjunto de fórmulas bem-formadas da Lógica dos Predicados, uma regra de inferência pode ser dada no seguinte exemplo:

$\mathbf{R}$: $\frac{w_1}{w_1 \vee w_2}$, para todo w_1 e w_2 pertencente a WFF_B, isto é, são sentenças, fórmulas bem-foermdas. Esta é um regra de inferência que representa a relação decidível:

$\mathbf{R} = \{((w_1), w_1 \vee w_2) \mid w_1, w_2 \in WFF_b\}$.

Um outro exemplo, de acordo com a definição formal de regra de inferência, é a seguinte regra:

$\mathbf{R}$: $\frac{\neg w_1, \neg w_2}{w_1 \wedge w_2}$, para todo w_1 e w_2 pertencente a WFF_B, que também é uma regra de inferência. Contudo, como uma regra de inferência para o Cálculo dos Predicados, ela violaria seu propósito intuitivo.

Um cálculo é também chamado de um sistema axiomático. Mas, o que vem a ser um **álgebra** ?

17.7 O que é uma Álgebra

Nesta seção, explicamos o que vem a ser um álgebra, no sentido formal. Interessante, é a *álgebra* que existe sobre o conjunto finito R de regras de inferência de um cálculo. Pode-se compor regras de derivação pela aplicação sucessiva de duas outras regras em R. Supondo que r_1 e r_2 são duas regras em R, e que "." é um operação sobre R, um outra regra r_3, não pertencente a R, pode ser uma composição de r_1 e r_2, ou seja:

$$r_1.r_2 = r_3$$

Esta composição de regras gera uma *nova regra* r_3, que não aparece no conjunto finito de regras de inferência da definição do cálculo.

Pode-se, também, até imaginarmos uma regra que nada faz, a regra identidade r_i, para funcionar como o elemento neutro desta álgebra.

A composição de regras de derivação é associativa, pois:

$r_1.(r_2.r_3) = (r_1.r_2).r_3$

Estes exemplos, mostram somente uma operação denotada por ".". Entretanto, um álgebra pode comportar outras operações.

O que garante a geração de novas regras de inferência é a noção de **morfismo**, que ocorre bastante na matemática contemporânea. Em muitos campos da matemática, **morfismo** se refere ao mapeamento de uma estrutura matemática (regras de derivação de um cálculo) para outra estrutura (a extensão do conjunto das regras de derivação), de forma que a estrutura é preservada, ou seja regras de derivação originam outras regras de derivação. Para a Teoria dos Conjuntos, morfismos são funções.

Definição: (**Álgebra**)

Uma **álgebra** é um **sistema formal**, constituindo-se de um conjunto qualquer munido de operações sobre esse conjunto, e mais a definição de um ou mais **elementos distinguidos**, também chamados de *elementos neutros*.

Esse elementos distinguidos (neutros), se operados com elementos desse conjunto, resulta no próprio elemento operado com um elemento neutro. A matemática define várias **estruturas algébricas** - álgebras específicas que tem utilidade nas várias áreas da ciência da computação. Dependendo da área que se vai estudar, pode existir uma álgebra mais apropriada para uma determinada área, do que outra. Uma álgebra é algo abstrato, também chamada de álgebra abstrata.

Álgebras são muito importantes, como sistemas formais-base, na construção de sistemas de computação ou na construção de ferramentas computacionais que servem para modelar sistemas de computação.

Exemplos de álgebras

Exemplo 1 - (Álgebra dos Conjuntos) - A teoria dos conjuntos nos proporciona uma álgebra bem esclarecedora. Imagine o conjuntos de todos os possíveis conjuntos, munido das operações entre conjuntos (união ($A \cup B$), interseção ($A \cap B$), diferença ($A - B$) , complemento ($\complement A$), ... Observe o elemento distinguido que é o conjunto

vazio $\varnothing$, funcionando como um elemento neutro nestas operações.

Exemplo 2 - (Álgebra das Proposições) - Considere o conjunto de todas as proposições possiveis, como na Lógica Proposicional, munido das operações ($\wedge$, $\vee$, $\rightarrow$, ...). O elemento neutro, distinguido, é uma proposição p operada com ela própria, como por exemplo, $p \wedge p \Leftrightarrow p$, $p \vee p \Leftrightarrow p$, $p \rightarrow p \Leftrightarrow p$, ...

Exemplo 3 - (Álgebra das Regras de Inferência) - As regras de inferência de um cálculo formam uma álgebra. Por eemplo, veja o caso das regras de inferência do Cálculo Proposicional em Janos (2009) ou em Filho (2002).

Exemplo 4 - (**Álgebra de Processos de Hoare**) - Em Hoare (1985), CSP - Communicationg Sequetial Processes proporciona uma álgebra de processos de computador (sistemas operacionais), com a definição de vários operadores sobre o conjunto de todos os processos possíveis. Operações como composição sequencial de processos $(P;\ Q)$, composição paralela de processos $(P \parallel Q)$, escolha não-determinística entre processos $(P \sqcap Q)$, *hiding* ou P sem C $(P \setminus C)$, intercalação entre processos $(P \parallel \parallel Q)$, e muitos outros operadores. Em CSP, existe um processo chamado STOP que nada faz e funciona como um elemento neutro da álgebra.

Exemplo 5 - (**Álgebra de Processos de Milner**) - Em Milner (1989), CCS - Calculus of Communicating Systems está construída uma álgebra de processos (Milner chama processos como agentes), com poucos operadores, como por exemplo, ocorrência de uma ação num agente E $(\alpha;\ E)$, escolha entre agentes $(E + F)$, composição paralela entre agentes $(E \| F)$, restrição de labels $(E \setminus L)$ e a composição sequencial $(E;\ F)$. Nesta álgebra um agente nulo, que nada faz é definido e simbolizado por O, e funciona como um elemento neutro da álgebra do CCS.

Exemplo 6 - (**Álgebra Relacional**) - Na álgebra criada por **E. F. Codd**, um modelo relacional representa o banco de dados como um conjunto de relações. Uma relação pode ser pensada como uma tabela de valores. Cada linha na tabela representa uma coleção de valores de dados relacionados, representada algebricamente pelo conceito de produto cartesiano entre os conjuntos de dados (tipos) contidos numa tabela. As operações básicas são União ($\bigcup$), Diferença ($-$), Produto Cartesiano ($\times$), Projeção ($\sqcap$), Seleção (σ), Interseção ($\bigcap$) e outras. Em ciências da computação, a álgebra relacional é uma derivação descendente da lógica de primeira ordem e da álgebra de conjuntos em relativa às operações sobre o conceito de relação sobre conjuntos de dados finitos, que auxilia o trabalho ao identificar os componentes de uma tupla por nome (chamado o atributo), o qual é chamado a relação na terminologia de banco de dados. A principal aplicação da álgebra relacional é sustentar a fundamentação teórica de banco de dados relacional, particularmente a linguagem de consulta aos bancos de dados relacionais.

Exemplo 7 - (**Álgebra da Teoria dos Grupos**)

Em matemática, um *grupo* é um conjunto de elementos associados a uma operação que combina dois elementos quaisquer para formar um terceiro. Para se qualificar como *grupo* o conjunto e a operação devem satisfazer algumas condições chamadas *axiomas de grupo*: *associatividade*, *elemento neutro* (o elemento distinguido) e *elementos inversos* (os simétricos dos elementos do grupo). *Grupos* estão por trás de muitas estruturas algébricas, como *corpos* e *espaços vetoriais*, e são uma importante ferramenta para o estudo de *simetrias*. A *teoria de grupos* é considerada uma área importante da matemática moderna, e tem aplicações em ciência da computação. Por exemplo, *grupos finitos* são utilizados na área de segurança computacional.

17.8 Problemas de Decisão

O *Entscheidungsproblem*, termo alemão para "*problema de decisão*", é atribuído a David Hilbert:

"*Em sua lista de 1900 dos 23 problemas mais importantes da Matemática, David Hilbert fez questões bastante precisas. Primeiro, era a matemática completa? ... Segundo, era a matemática consistente? ...*

Em 1900, Hilbert pediu em seu décimo problema: *Encontrar um processo para decidir se um sistema de equações com coeficientes inteiros tem uma solução inteira.*

E por terceiro, era a matemática *decidível*? O *Entscheidungsproblem* (problema de decisão, em alemão) foi um desafio posto por **David Hilbert** em 1928. **Hilbert** enuncia o Entescheidungsproblem assim:

O Entscheidungsproblem é resolvido quando conhecemos um procedimento que permite, para qualquer expressão lógica dada, decidir sua validade ou satisfatibilidade.

O *Entscheidungsproblem* pede por um procedimento efetivo (Hilbert chamava esse de processo) que receberá como entrada uma descrição de uma linguagem formal e um enunciado matemático na linguagem, e produzirá como saída "Verdadeiro"ou "Falso". Com isto ele quis dizer: existia um método definitivo que poderia, em princípio ser aplicado a qualquer asserção, e que garantiria a produção correta da decisão nos casos em que a asserção for verdadeira"Hodges (1970).

Em 1930 (embora publicado apenas em 1948), o lógico polonês **Alfred Tarski** demonstrou que: *Existe um algoritmo para testar a solubilidade, nos reais, de sistemas de equações polinomiais com coeficientes inteiros.*

Turing mostrou que o problema de se determinar se uma dada máquina de Turing pára ou não quando executa sobre uma dada entrada é indecidível. Esse ficou conhecido como o Problema da Parada. Trata-se de um problema matemático de decisão,

que não tem solução, daí o *Entscheidungsproblem*, que é o caso mais geral, também não ter solução.

Na *teoria da computabilidade* e na *teoria da complexidade computacional* um problema de decisão é uma questão sobre um *sistema formal* com uma resposta do tipo *sim-ou-não*. Um problema de decisão também pode ser formalizado como o problema de verificar se uma determinada cadeia de caracteres pertence ou não a um conjunto de cadeias de caracteres, também chamado de *linguagem formal*. Tradicionalmente, é comum definir-se o problema de decisão em termos do conjunto de entradas para as quais o problema retorna "sim". Nesse sentido, um problema de decisão é equivalente a uma *linguagem formal*.

Os problemas de decisão são problemas de determinar se um determinado elemento x de algum universo (conjunto) C, pertence ou não a um determinado conjunto (ou equivalentemente, se satisfaz uma determinada propriedade). Se existir um procedimento efetivo (que mais tarde, nos tempos de **Turing**, veio a ser chamado de algoritmo computacional) que receba como entrada um elemento x e retorne como saída "sim", caso x pertença ao conjunto C, ou "não", caso contrário, então diz-se que o problema de decisão para o conjunto C é *decidível*.

Definição (**Conjunto Decidível**)

Da teoria da computação teórica, um conjunto *decidível* significa dizer que existe um *procedimento efetivo* para o qual, dado um elemento potencial desse conjunto, o procedimento tem como resposta "sim"ou "não", de acordo, se é o elemento do conjunto ou não.

Um *problema de decisão* é chamado de *decidível* (*efetivamente solúvel*), se C é um *conjunto recursivo*. SC é um *conjunto recursivamente enumerável*, se existe um procedimento efetivo que reconhece elementos de C, dizendo "sim", mas que não pode terminar para elementos que não estão no conjunto C, ou pare com "não". Neste caso, o problema é chamado *parcialmente decidível*. Do contrário, o problema é chamado de *indecidível*.

Para tornar o significado de indecidível preciso, é necessário dispor de uma noção formal de algoritmo. Tal noção foi introduzida independentemente por **Alonzo Church** (1936) e **Alan Turing**. Em 1936 **Alan Turing** veio com uma definição precisa de máquinas de Turing. Isso viabilizou a definição exata da decidibilidade de problemas matemáticos, e, portanto, abrindo a possibilidade de se demonstrar que certos problemas são de fato indecidíveis.

Várias outras demonstrações de indecibilidade, inclusive a de **Emil Post** (1946) com relação ao problema da correspondência passaram a utilizar como referencial o Problema da Parada: *se esse problema for decidível então o Problema da Parada*

também o é, portanto ele não pode ser decidível. O problema da correspondência de **Post** é um problema de decisão indecidível que foi introduzido por **Emil Post** em 1946. O problema é mais simples que o problema da parada e o problema de decisão, e por isso ele é frequentemente usado em provas de indecidibilidade.

Problemas Indecidíveis na Computação - Citamos alguns problemas considerados indecidíveis na ciência da computação.

1. Determinar se dois programas são equivalentes.
2. Determinar se uma gramática livre-do-contexto é ambígüa.
3. Determinar se duas gramáticas livres-do-contexto são equivalentes.
4. Determinar se duas expressões do λ-cálculo são equivalentes.
5. Determinar se uma dada expressão do λ-cálculo tem forma normal.

Legado na Criptografia Moderna - A *decidibilidade* e a *parcialidade na decidibilidade*, deixaram um legado de problemas resolvidos, que surgiram na área de segurança computacional. Tais como:

1. Definição de: função unidirecional, função pseudoaleatória, indistinguibilidade.
2. Definição da noção de experimento, permitindo a definição matemática de: sigilo computacional, resistência à colisão e inforjabilidade existencial.
3. Provas de segurança relativa (por redução).

17.9 Lógica x Álgebra x Cálculo

Com as definições de lógica, álgebra e cálculo dadas, temos alguns exemplos de formalismos usados em ciëncia da computação:

- Lógica Proposicional + Álgebra Proposicional + Cálculo Proposicional, como em Filho (2002).
- Lógica dos Predicados + Cálculo dos Predicados, como em Loeckx e Sieber (1987).
- Logica dos Predicados + Álgebra de Processos, como em Hoare (1985).
- Álgebra de agentes + Cálculo de agentes (processos), como em Milner (1989).

17.10 Como Álgebras e Cálculos se relacionam com a Ciência da Computação

No que segue estão alguns exemplos das áreas da Ciência da Computação mais influenciadas pelas álgebras:

- Sistemas Operacionais: **Álgebras de Processos** servem para especificar e provar correção de sistemas.
- Bancos de Dados: **Álgebra Relacional** que serve para definir operações sobre um banco de dados.
- Segurança Computacional: a Teoria dos Grupos **Álgebra Abstrata** serve de embasamento teórico para a criação de algoritmos de criptografia na área da segurança da informação.
- Processamento de Imagem (anos 60), **Álgebra e Cálculo Vetorial** servem para construir ferramentas.
- Computação Gráfica (anos 80), **Álgebra e Cálculo Vetorial** serve para construir ferramentas e sistemas de computação gráfica.

17.11 Concluindo ...

Embora se tenha mostrado incapaz de se converter em fundamento conveniente da matemática (ver o capítulo 15), dentro dos moldes hilbertianos, o método axiomático é uma técnica de valor adotada na definição dos sistemas formais da computação.

Como em Filho (2007), **Turing** começou com uma descrição precisa de um *sistema formal*. Provou então, que os passos de um *sistema axiomático formal semelhante à lógica* e os estados da máquina imaginada por ele, perfaziam os "movimentos"(transições) em um *sistema formal automático* e, são equivalentes entre si. Um *sistema formal automático* é um dispositivo físico que manipula automaticamente os *símbolos de um sistema formal*, de acordo com as suas regras. Ele provou que *para qualquer sistema formal* existe uma máquina de Turing que pode ser programada para imitá-lo. Ou em outras palavras: para qualquer procedimento computacional bem definido, uma *Máquina de Turing Universal* é capaz de simular um processo mecânico que execute tais procedimentos. De um ponto de vista teórico, a importância da máquina de Turing está no fato de que ela representa um objeto matemático formal. Através dela, pela primeira vez, se deu uma boa definição do que significa computar algo. E isso levantou a questão sobre o que exatamente pode ser computado com tal dispositivo matemático.

Além do mais, a questão da *decidibilidade* iniciada com **Hilbert**, apesar de que não podemos ter todos os problemas decidíveis, podemos contar com problemas parcialmente decidíveis e, neste caso, existe um procedimento efetivo que pode responder

"sim", reponder "não", ou mesmo, "não parar". Enfim, todos estes conceitos estão todos subjacentes na tecnologia atual dos computadores digitais, cuja construção tornou-se possível pouco anos mais tarde da publicação de **Turing**, quando surgiram os primeiros projetos de computadores digitais.

17.12 Bibliografia e Fonte de Consulta

Jorge Muniz Barreto - Sistemas Formais, notas de aula, Dep. Informática e Estatística, 2000

Manna e Waldinger - The Logical Basis for Computing Programming - Volumes I (1985) e II (1990).

Jacques Loeckx e Kurt Sieber - The Foundations of Program Verification, 2 Ed. Wiley-Teubner Series in Computer Science, 1987.

Edgard de Alencar Filho - Introdução à Lógica Matemática, Ed. Nobel, 2002.

Marco A. Casanova, Fernando Giorno e Antonio Furtado - Programação em Lógica - V Escola de Computação, SBC, 1986.

Emil L. Post. (1946). "A variant of a recursively unsolvable problem". Bull. Amer. Math. Soc 52.

Michael Sipser. Introduction to the Theory of Computation. 2nd ed. [S.l.]: Thomson Course Technology, 2005. 199-205 p. ISBN 0-534-95097-3

Fernando Vieira Costa Júnior - https://logicaematematica.wordpress.com/2014/02/08/a-historia-dos-sistemas-axiomaticos-formais/

Alcorafado, P.; Duarte, A.; Wyllie, G. - Os Primeiros Escritos Lógicos de Gottlob Frege. São Paulo: IBFC Ramon Llull, 2012.

Costa Junior, Fernando V. - Minicurso de Lógica Matemática: Uma introdução à Lógica Matemática e uma aplicação do método da Dedução Natural a sistemas axiomáticos formais. Disponível em: ¡https://logicaematematica.wordpress.com/2014/02/04/minicu
de-logica-matematica/¿. Acesso em: 04 Fev. 2014.

Eves, Howard. - Introdução à História da Matemática. Traduzido por Hygino H. Domingues. 5 ed. Campinas: Editora da Unicamp, 2011.

Mortari, Cezar A. Introdução à Lógica. São Paulo: Editora UNESP, 2001.

Tarski, Alfred. A Concepção Semântica da Verdade. Tradução de Celso Braida

[et. al.]. MORTARI, Cezar A.; DUTRA, Luiz H. de A. (orgs.). São Paulo: Editora UNESP, 2007.

Geometria. In: Wikipedia, a enciclopédia livre. Flórida: Wikimedia Foundation, 2013. Disponível em: ¡http://pt.wikipedia.org/w/index.php?title=Geometria&oldid=37303472¿. Acesso em: 5 fev. 2014.

17.13 Referências - Leitura Recomendada

Michael Shermer. The borderlands of science: where sense meets nonsense. illustrated ed. [S.l.]: Oxford University Press US, 2001. 10-30,54,216,244-245 p. ISBN 0195143264, 9780195143263.

Gauch, Hugh G., Jr., Scientific Method in Practice (2003) 3-7.

Cover, J.A., Curd, Martin (Eds, 1998) Philosophy of Science: The Central Issues, 1-82.

Hodges, A., Alan Turing: The Enigma, Simon and Schuster, New York. Cf Chapter "The Spirit of Truth"for some more history that led to Turing's work. Hodges references a biography of David Hilbert: Constance Reid, Hilbert (George Allen & Unwin; Springer-Verlag, 1970). There are apparently more recent editions.

Kozen, D.C. (1997), Automata and Computability, Springer.

Hartley Rogers, Jr., The Theory of Recursive Functions and Effective Computability, MIT Press, ISBN 0-262-68052-1 (paperback), ISBN 0-07-053522-1.

Sipser, M. (1996), Introduction to the Theory of Computation, PWS Publishing Co.

Robert I. Soare (1987), Recursively Enumerable Sets and Degrees, Springer-Verlag, ISBN 0-387-15299-7.

Computabilidade: os limites da Computação - Regivan H. N. Santiago e Benjamín R. C. Bedregal.

Macintyre, A. (2011). "Undecidable and Decidable Problems in Mathematics: A survey and some reflections, for the centenary of Turing's birth". Talk given Tuesday, 17 May 2011 - 6:00pm, Barnard's Inn Hall, Gresham College, London, UK.

K. Ruohonen. (1983). "On some variants of Post's correspondence problem". Acta Informatica 19 (4): 357-367. Springer. DOI:10.1007/BF00290732.

R.J. Gillings - Mathematics in the times of the Pharaohs, Dover, New York, 1982.

Referências

ARP, R.; CAPLAN, A. *1001 Ideas That Changed the Way We Think*. Nova York: Simon and Schuster, 2013. P. 374. Citado na página 194.

ARP, R.; CAPLAN, A. *1001 Ideas That Changed the Way We Think. Nova Iorque: Simon and Schuster, 2013. pp. 374.* New York: Simon and Schuster, 2013. Pp. 374. Citado na página 136.

BARRETO, J. M. *Sistemas Formais*. CTC-UFSC, 2000. Mídia eletrônica. Notas de Curso de Teoria da Computação. Disponível em: ⟨http://www.inf.ufsc.br/~barreto/TC/formais.pdf⟩. Citado 2 vezes nas páginas 286 e 287.

BEN-ARI, M.; PNUELI, A.; MANNA, Z. The temporal logic of branching time. *Acta Informatica*, n. 20, p. 207–226, 1983. Citado na página 256.

BENATTI, K. *História da Algebra - Uma breve apresentacaoo*. 2015. Visitado em 23 de fevereiro de 2015. Disponível em: ⟨www.ebah.com.br/content/ABAAAenLEAI/historia-algebra⟩. Citado na página 127.

BERMAN, H. J. *Law and revolution: the formation of the Western legal tradition*. [S.l.]: Harvard University Press, 1983. ISBN 0-674-51776-8. Citado na página 135.

BISHOP, E. Foundations of constructive analysis. *Journal of Symbolic Logic*, v. 37, n. 4, p. 744–747, 1972. Disponível em: ⟨http://www.jstor.org/stable/2272421⟩. Citado na página 271.

BRIDGES, D. *Constructive Mathematics*. 2013. The Stanford Encyclopedia of Philosophy(Spring 2013 Edition), Edward N. Zalta(ed.),. Disponível em: ⟨http://plato.stanford.edu/archives/spr2013/entries/mathematics-constructive⟩. Citado 5 vezes nas páginas 270, 271, 272, 273 e 274.

BROUWER, L. E. J. *Brouwer's Cambridge Lectures On Intuitionism*. 1 ed.. ed. Cambridge: Cambridge University Press, 2011. P. 2-3. Citado 2 vezes nas páginas 267 e 268.

CARNIELLI, W.; EPSTEIN, R. *Computabilidade, Funcoes Computaveis, Logica e os Fundamentos da Matematica*. [S.l.]: Editora FAPESP, 2005. Citado 9 vezes nas páginas 8, 197, 235, 236, 240, 257, 259, 260 e 275.

CASANOVA, M. A.; GIORNO, F. A. C.; CASANOVA, F. A. C. G. A. L. F. M. A. *Programacao em Logica*. [S.l.]: SBC, 1986. Citado na página 155.

CERRI, C.; MONTEIRO, M. S. *História dos Números Complexos*. 2001. Visitado em 13 de março de 2015. Disponível em: ⟨http://www.ime.usp.br/~martha/caem/complexos.pdf⟩. Citado na página 62.

CONTADOR, P. R. M. *Matematica, uma breve historia*. Terceira edição. [S.l.]: Editora Livraria da Fisica, 2008. II. Citado na página 21.

COPI COHEN, C. I. *Copi, I., Cohen, C. Introduction to logic. 8 ed. New York: Macmillan Publishing Company, 1990. 569 p. p. 45–46. ISBN 0-02-946192-8*. [S.l.]: Macmillan Publishing Company, 1990. 569 p. p. 45–46, ISBN 0-02-946192-8. Citado na página 163.

COSTA, N. *Introducao aos Fundamentos da Matematica*. [S.l.]: Editora Ucitec, 2008. Citado 4 vezes nas páginas 7, 240, 241 e 265.

COULOURIS, G.; DOLLIMORE, J.; KINDBERG, T. *Sistemas Distribuidos: Conceitos e Projeto*. [S.l.]: Bookman, 2007. Citado 4 vezes nas páginas 189, 190, 191 e 193.

COX J. ROBERT; WILLARD, A. C. *Advances in Argumentation Theory and Research*. [S.l.]: Southern Illinois University Press, 1983. Citado na página 131.

CRATO, N. Alice e bob. *Expresso / Revista*, p. pp. 118–120, 22 de Setembro 2001. Citado na página 96.

DAVENPORT, H. *The Higher Arithmetic: An Introduction to the Theory of Numbers. 7ª ed. Cambridge, UK: Cambridge University Press, 1999. ISBN 0-521-63446-*. 7ª ed.. ed. Cambridge, UK: Cambridge University Press, 1999. Citado 2 vezes nas páginas 23 e 44.

DAVENPORT, H. J. H.; SIRET, Y.; TOURNIER, E. *Computer Algebra 298 p. ISBN 0-12-209232-8*. 2ª ed.. ed. Boston: Academic Press, 1993. 298 p. ISBN 0-12-209232-8. Citado na página 127.

DEO, N. *Graph Theory*. [S.l.]: Prentice Hall, 1974. (Series in Automatic Computation). Citado 3 vezes nas páginas 8, 210 e 211.

DUKE, R.; ROSE, G. *Formal Object-Oriented Specification Using Object-Z*. [S.l.]: McMillan, 2000. Citado na página 181.

EELS, W. C. *Number Systems of North American Indians*. [S.l.]: Amer, 1913. vol. 20. Pp. 263-272, 293-299, ver especialmente p. 293. Citado na página 35.

EMERSON, E. A.; SISTLA, A. P. Deciding full branching time logic. *Information and Control*, n. 61, p. 175–201, 1984. Citado na página 256.

FERREIROS, J. *The Crisis in the Foundations of Mathematics*. Princeton: Princeton University Press, 2008. (Princeton Companion to Mathematics). P. 1-14. Citado na página 269.

FILHO, C. F. *História da Computacao: O caminho do pensamento e da tecnologia*. 2007. Publicação Eletrônica. Disponível em: ⟨www.pucrs.br/edipucrs/online/historiadacomputacao.pdf⟩. Citado 4 vezes nas páginas 251, 252, 255 e 305.

FILHO, E. A. *Iniciacao a Logica Matematica*. [S.l.]: Nobel, 2002. Citado 6 vezes nas páginas 139, 145, 289, 290, 301 e 304.

FISHER, M.; M., D.; GABBAY, L. V. *Handbook of Temporal Reasoning in Artificial Intelligence*. [S.l.]: Elsevier, 2005. Citado na página 135.

GONICK, L. *Introdução Ilustrada à Computação. São Paulo*. São Paulo: Harper & Row do Brasil, 1984. 242 p. p. 34-35. Citado na página 35.

HAMILTON, A. G. *Logic for Mathematicians*. [S.l.]: Cambridge University Press, UK, 1978. ISBN 0-521-21838-1. Citado na página 154.

HAMILTON, A. G. *Logic for Mathematicians*. [S.l.]: [S.l.]: Cambridge University Press, 1980. ISBN 0-521-29291-3, faz uma abordagem moderna à lógica simbólica. Citado na página 135.

HAN ZHIYONG ZHOU, Y. W. J. Automatic verification for secrecy of cryptographic protocols in first-order logic. *International Journal of Distributed Sensor Networks*, Volume 5, n. Issue 1, p. 14–14, 2009. Citado na página 160.

HEATH, T. e. . . *The Thirteen Books of Euclid's Elements. 1.* (ed.) (1956) [1908]. [S.l.]: Dover Publications, 1908, 1956. 1 vol. ISBN 0-486-60088-2. Citado na página 32.

HEATH, T. L. *Euclid and the Traditions About Him , in Euclid, Elements (Thomas L. Heath, ed. 1908), 1:16, at Perseus Digital Library*. 1908. ed. [S.l.: s.n.], 1908. In Euclid, Elements (Thomas L. Heath), 1:16, at Perseus Digital Library. Citado na página 32.

HEATH, T. L. *A History of Greek Mathematics, 2 Vols. New York:ISBN 0-486-24073-8 / ISBN 0-486-24074-6*. New York: Dover Publications, 1981. 2 Vols. ISBN 0-486-24073-8 / ISBN 0-486-24074-6. Citado na página 32.

HERMES, H. *Enumerability, Decidability, Computability*. 2. ed.. ed. [S.l.]: Springer-Verlag, 1969. Citado na página 259.

HOARE, C. A. R. *Communicating Sequencial Process*. [S.l.]: Prentice Hall, 1985. (Series Editor). Citado 2 vezes nas páginas 301 e 304.

HODGES, A. *Alan Turing: The Enigma*. New York: Springer-Verlag, 1970. Cf Chapter "The Spirit of Truth"for some more history that led to Turing's work. Hodges references a biography of David Hilbert: Constance Reid; There are apparently more recent editions. Citado 2 vezes nas páginas 249 e 302.

IFRAH, G. *História Universal dos Algarismos: A Inteligência dos Homens Contada pelos Números e pelo Cálculo*. Rio de Janeiro: Nova Fronteira, 1997. vol. 1. 735 p. p. 162-180;346-354;404-409. 2 vol. Citado na página 35.

IFRAH, G. *OsNumeros - A Historia de uma Grande Invencao*. [S.l.]: Editora Globo, 2005. Traducao: Stella M. de Freitas Senra. Citado 3 vezes nas páginas 35, 36 e 37.

JANOS, M. *Matemática e Natureza*. [S.l.]: Editora Livraria da Fisica, 2009. ISBN 978-85-7861-038-8. Citado 21 vezes nas páginas 2, 8, 52, 53, 56, 57, 58, 61, 71, 73, 136, 139, 195, 208, 209, 214, 240, 265, 266, 280 e 301.

KARLSON, P. *A Magia dos Números*. Porto Alegre: [s.n.], 1961. Capítulo: Os Gregos. , 608 p. p. 80-154. Citado na página 33.

KNUUTTILA, S. *Reforging the great chain of being: Studies of the History of Modal Theories*. [S.l.]: Springer Science & Business, 1981. P.71. ISBN 90-277-1125-9. Citado na página 135.

KRAMER, S. *Timed Cryptographic Protocol Logic*. [S.l.], 2006. Citado na página 160.

LEI JUN LIU, J. X. X. Time-dependent cryptographic protocol logic and its formal semantics. *Journal of Software*, v. 22, n. (3), March 2011. Citado na página 160.

LEITE, G. G. *A CONSTRUÇÃO HISTÓRICA DOS SISTEMAS DE NUMERAÇÃO COMO RECURSO DIDÁTICO PARA O ENSINO FUNDAMENTAL I*. Dissertação (Mestrado) — Programa de Pós-Graduação em Matemática, Universidade Federal do Ceará,, 2014. Citado na página 27.

LIETZ, P. *From constructive mathematics to computable analysis via the realizability interpretation*. Tese (Tese de Doutorado) — TU Darmstad, Darmstadt, 2005. Pp 14-21. Citado 2 vezes nas páginas 271 e 274.

LOBUR, L. N. J. *Princípios Básicos de Arquitetura e Organização de Computadores*. [S.l.]: Bookman, 2006. ISBN 978-85-7780-766-6. p. 140. Citado na página 147.

LOECKX, J.; SIEBER, K. *The Foundations of Program Verification*. 2. ed. [S.l.]: John Wiley & Sons Ltd., B. G. Teubner, 1987. (Wiley-Teubner Series in Computer Science). Citado 8 vezes nas páginas 157, 181, 198, 256, 290, 298, 299 e 304.

MANNA, R. W. Z. *The LoLogic Basis for Computer Programming: Volume 1 - Deductive Reasoning*. [S.l.]: Addison Wesley, 1985. Vol 1. ISBN 0-201-18260-2. Citado 8 vezes nas páginas 139, 154, 157, 256, 289, 290, 294 e 297.

MCCARTHY, J. *A basis for a mathematical theory of computation. In Computer Programming and formal systems*. [S.l.]: North-Holland, 1963a. Citado na página 159.

MCKEON, R. *Aristótoles: The Basic Works*. [S.l.]: [S.l.]: Modern Library, 2001. Capítulo: Posterior Analytics. ISBN 0-375-75799-6. Citado na página 134.

MICHAELSON, G. *An Introduction to Functional ProgProgram through Lambda Calculus*. Segunda edição. [S.l.]: Addison Wesley, 1989. Primeira Edição, 1983. Citado 2 vezes nas páginas 181 e 198.

MILLES, C. P. *Breve Historia da algebra Abstrata*. [S.l.]: EPUSP, 1992. Citado 2 vezes nas páginas 107 e 110.

MILNER, R. *Communication and Concorrency*. [S.l.]: Prentice Hall, 1989. (Series Editor). Citado 3 vezes nas páginas 280, 301 e 304.

MONTEIRO, L. H. J. *Elementos de Álgebra*. [S.l.]: Ao Livro Técnico, 1969. (IMPA - Elementos de Matematica). Citado 11 vezes nas páginas 8, 44, 53, 54, 71, 73, 78, 87, 180, 181 e 205.

MORRIS, K. *Mathematics: The Loss of Certainty*. Oxford: Oxford University Press, 1980. Kline, Morris (1980). Mathematics: The Loss of Certainty. Oxford: Oxford University Press. ISBN 0-19-502754-X. ISBN 0-19-502754-X. Citado na página 33.

NACHBIN, L. *Introducao a Algebra*. [S.l.]: McGraw-Hill do Brasil, 1971. Citado na página 186.

NAGEL, E.; NEWMAN, J. R. *A Prova de Gödel*. [S.l.]: São Paulo: Editora Perspectiva, 2001. Citado 2 vezes nas páginas 257 e 259.

NIPKOW LAWRENCE C. PAULSON, M. W. T. *Isabelle HOL: A Proof Assistant for Higher-Order Logic*. [S.l.]: Springer-Verlag, 2014. Citado na página 162.

OLIVER, M. *História Ilustrada da Filosofia*. [S.l.]: [S.l.]: Manole,, 1998. P. 20. ISBN 978-85-204-0820-9. Citado na página 132.

OMNES, R. *Filosofia da Ciencia Contemporanea*. Sao Pulo: Editora da UNESP, 1996. Traduacao de Roberto Leal Ferreira, Titulo original: Philosophie de la Science Contemporaine. Citado 4 vezes nas páginas 2, 246, 275 e 279.

PROLO, P. *Aula de Teoria da Computabilidade de 19.08.2004, Prof Prolo*. Porto Alegre, 2004. Material de aula. Disponível em: ⟨https://www.inf.pucrs.br/~prolo/Disciplinas/07I/TComp590/aula19.08.04.pdf⟩. Citado 5 vezes nas páginas 220, 223, 224, 225 e 226.

RAMOS, A. F. *Matemática Construtiva e o Intuicionismo*. 2013. Trabalho de graduacao. Citado na página 269.

SA, I. P. Artimetica modular e algumas de suas aplicações. *Revista do Professor de Matematica*, Volumes 12 e 45, 2008. Ilydio Pereira de Sa Mestre em Educação Matematica, professor da UERJ, da Universidade Severino Sombra e do Colegio Pedro I, Rio de Janeiro. Disponível em: ⟨http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf⟩. Citado 3 vezes nas páginas 85, 89 e 91.

SCHEINERMAN, E. R. *Matemática Discreta - Uma Introdução*. [S.l.]: Cengage Learning Editores, 2003. ISBN 978-85-221-0291-4. p. 27. Citado na página 147.

SCHMIDT, D. A. *Denotational Semantics: a Methodology for Language Development*. [S.l.]: Wm. C. Brown Publishers, 1986. Citado na página 198.

SERRE, J.-P. *Serre, Jean-Pierre. A Course in Arithmetic New York*. New York: Springer, 1973. 115 p. ISBN 978-0-38790040-7. Citado na página 44.

SINGH, S. *O Livro dos Codigos*. São Paulo: Record, 2001. Citado na página 95.

SIPSER, M. *Introducao a Teoria da Computacao*. [S.l.]: Cengage Learning Editores, 2011. Citado 2 vezes nas páginas 8 e 256.

SMITH, D. E. *A Source Book in Mathematics*. [S.l.]: McGraw-Hill, 1929. Pages 20-34. Citado na página 113.

SPIVAK, M. *Calculus: Cálculo Infinitesimal*. Barcelona: Editorail Reverté sa, 1970. Vol. 2. Version española por Bartomé Frontera Marqués. Citado na página 56.

SPIVEY, J. M. *Understanding Z - A specification language and its formal semantics*. [S.l.]: Cambridge University Press, 1988. Citado na página 181.

SPIVEY, J. M. *The Z Notation*. [S.l.]: Prentice-Hall, 1989. Citado 3 vezes nas páginas 11, 181 e 214.

STALLINGS, W. *Criptografia e Seguranca de Redes: Principios e Praticas*. Ed. 4. [S.l.]: Pearson Education, 2008. Citado 3 vezes nas páginas 74, 81 e 97.

STANAT, D. F. M. D. F. *Discrete Mathematics in Computer Science*. Prentice-hall international editions. [S.l.]: Prentice-Hall, 1977. Citado na página 8.

STEIN, J. D. *Como a Matematica Explica o Mundo*. [S.l.]: Campus, 2008. Citado 4 vezes nas páginas 39, 40, 43 e 252.

STEWART, I. *Uma Historia da Simetria na Matematica*. [S.l.]: Zahar, 2012. Titulo original: WHY BEAUTY IS TRUTH,. Citado 2 vezes nas páginas 3 e 208.

STEWART, J. *Calculo*. 4 ed.. ed. [S.l.]: E Pioneira, 2002. Vol. I. Citado na página 194.

STOLYAR, A. A. *Introduction to Elementary Mathematical Logic*. New York: Dover Publications Inc., 1970. ISBN 0-486-64561. Citado na página 154.

STRUIK, D. J. *História Cincisa das Matemáticas*. [S.l.]: Gradiva, 1987. Citado 14 vezes nas páginas 2, 9, 11, 20, 21, 22, 26, 27, 28, 31, 32, 56, 101 e 276.

SUDKAMP, T. A. *Languages and Machines*. [S.l.]: Addison Wesley, 1988. Citado 10 vezes nas páginas 8, 216, 217, 218, 219, 220, 221, 222, 228 e 229.

SZALAS, A.; HOLENDERSKI, L. Incompleteness of first-order temporal logic with until. *Theoretical Computing Science*, n. 57, p. 317–325, 1988. Citado na página 256.

TERADA, R. *Seguranca de Dados*. [S.l.]: Editora Blucher, 2008. Citado na página 98.

TREMBLAY, R. M. J. P. *Discrete Mathematical Structures with Applications to Computer Science*. [S.l.]: McGraw-Hill, 1987. Citado na página 8.

VASCONCELOS. *O Tempo como Modelo*. Dissertação (Mestrado) — Program de P[os-Graduação em Sistemas de Computação - COPPE - UFRJ, 1989. Citado 3 vezes nas páginas 256, 281 e 291.

VIETE, F. *Opera Mathematica (Leiden, 1646; reprinted London, 1970)*. [S.l.]: Leiden, 1646. Citado na página 103.

WALLIS, J. *De algebra tractatus, historicus e practicus ... cum variis appendicibus ... Operum Mathematicorum volumen alterum*. 1693. P. 4. Disponível em: ⟨http://books.google.com.br/books?id=EuzpN1t5SOcC&pg=PP268⟩. Citado na página 101.

WEISSTEIN, E. W. *Constructive Proof*. 2013. Disponível em: ⟨http://mathworld.wolfram.com/ConstructiveProof.html⟩. Citado na página 270.

ZACH, R. *Kurt Gödel and Computability Theory*. 2006. Research supported by the Social Sciences and Humanities Research Council of Canada. Acessado em 12 de Outubro de 2015. Disponível em: ⟨http://people.ucalgary.ca/~rzach/static/cie-zach.pdf⟩. Citado 2 vezes nas páginas 11 e 261.

Índice

Este texto foi composto em Minion Pro, de Robert Slimbach, e Myriad Pro, de Robert Slimbach e Carol Twombly.

Este texto foi composto em fontes EBGaramond
(⟨http://www.ctan.org/tex-archive/fonts/ebgaramond⟩).

SÉRIE PENSAMENTO MATEMÁTICO @ CIÊNCIA COMPUTAÇÃO

Volume I: Dos Primórdios da Matemática aos Sistemas Formais da Computação

O presente volume foi idealizado no sentido de mostrar como as raízes da Ciência da Computação, a Matemática e a Lógica, influíram no desenvolvimento desta nossa ciência. Os grandes cientistas, da Matemática e da Lógica, avançaram no tempo, construindo a ciência que levou à construção do computador digital e o desenvolvimento da ciência computação. A evolução ocorreu promovida por mentes geniais, de matemáticos e lógicos, cada um deles baseando-se no trabalho dos que os antecederam. A partir de problemas matemáticos no início de século XX, as vezes até sem soluções, das primeiras ideias das funções recursivas, das controvérsias da matemática e das correntes filosóficas que nortearam os fundamentos da matemática, originou-se o embrião da ciência da computação. O texto aqui apresentado é uma coleção de ideias, algumas das quais, fascinaram os precursores desta ciência. Com o reordenamento da axiomática, chegou-se aos sistemas formais que sustentam a Ciência da Computação.

Este livro pretende servir de material de apoio às disciplinas de Matemática Discreta e Lógica, em cursos de graduação, e seu texto, seguindo o mais que possível a ordem cronológica da aparição das grandes ideias, tenta mostrar ao estudante, do ponto de vista histórico, como determinados conceitos derivados da Matemática e da Lógica, serviram para a construção da Ciência da Computação. Este primeiro trabalho faz a parte da organização da série Pensamento Matemático @ Ciência da Computação, inicialmente em dois volumes, baseando-se na exposição da evolução da Matemática e da Lógica, em termos dos grandes personagens, os verdadeiros donos das ideias, as vezes narrando fatos e suas ideias geniais, além de algumas escolas (como a de Hilbert), em vez de assuntos específicos. É uma tentativa de acrescentar este conhecimento histórico sobre as raízes da Ciência da Computação, proporcionando uma visão que outros livros, que tratam de temas específicos, não contemplam do ponto de vista histórico e conceitual.

Sobre o autor:

João Bosco M. Sobral é Bacharel em Matemática pelo Instituto de Matemática da UFRJ em 1973, M.Sc. pelo Programa de Sistemas e Computação da COPPE-UFRJ em 1977, e realizou seu doutorado no Programa de Engenharia Elétrica da COPPE-UFRJ em 1996. Como docente durante quase quatro décadas na ciência da computação da UFSC, ao participar nas disciplinas em cursos de graduação e mestrado em computação, teve a oportunidade de entender e vivenciar o elo existente entre a Matemática, a Lógica, e a Ciência da Computação. Agora, tenta disseminar o que aprendeu sobre o elo fascinante destas ciências, no sentido de motivar o leitor a ficar conectado com o mundo da Matemática e da Lógica, como ciências construtoras da Ciência da Computação passada e futura.

Agência Brasileira do ISBN
ISBN 978-85-902995-2-3
9 788590 299523