UNIVERSIDADE FEDERAL DE SANTA CATARINA

CAMILA CECILIA CASTRO

CRIPTOGRAFIA RSA

Blumenau

2019

Camila Cecilia Castro

CRIPTOGRAFIA RSA

Trabalho de Conclusão de Curso submetido ao Curso de Licenciatura em Matemática da Universidade Federal de Santa Catarina para a obtenção do Grau de Licenciada em Matemática.

Orientador: Prof. Dr. Felipe Vieira

Blumenau

2019

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

Arquivo compilado às 20:37h do dia 16 de dezembro de 2019.

Camila Cecilia Castro
Criptografia RSA : / Camila Cecilia Castro; Orientador, Prof. Dr. Felipe Vieira; , - Blumenau, 20:37, 16 de dezembro de 2019.
69 p.

Trabalho de Conclusão de Curso - Universidade Federal de Santa Catarina, Departamento de Matemática (MAT), Centro de Blumenau, Curso de Licenciatura em Matemática.

Inclui referências

1. Álgebra. 2. Criptografia RSA. 3. Números Primos. 4. Congruência. I. Prof. Dr. Felipe Vieira II. III. Curso de Licenciatura em Matemática IV. Criptografia RSA

CDU 02:141:005.7

Camila Cecilia Castro

CRIPTOGRAFIA RSA

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciada em Matemática, e aprovado em sua forma final pelo Curso de Licenciatura em Matemática do Departamento de Matemática (MAT), Centro de Blumenau da Universidade Federal de Santa Catarina.

Blumenau, 16 de dezembro de 2019.

Prof. Dr. André Vanderlinde da Silva
Coordenador do Curso de Licenciatura em Matemática

Banca Examinadora:

Prof. Dr. Felipe Vieira
Orientador
Universidade Federal de Santa Catarina – UFSC

Profª. Drª. Naiara Vergian de Paulo Costa
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. Rafael Aleixo de Carvalho
Universidade Federal de Santa Catarina – UFSC

Este trabalho é dedicado à pessoa mais importante da minha vida.

AGRADECIMENTOS

A primeira pessoa a quem eu agradeço imensamente é a pessoa a quem eu devo a minha vida. Aquela que me criou sozinha, me educou, me ensinou tudo que eu sei até hoje. E se eu estou onde estou, conquistando tudo que eu conquisto, é graças a ela, a mulher mais forte que eu conheço e que eu tanto amo: mãe.

A segunda pessoa a quem eu agradeço é meu padrasto, que sempre me ajudou como pode. Cuida do meu maior tesouro e demonstra todo o carinho e amor que ele tem por mim, do jeitinho dele. Obrigada!

Professor Dr. Felipe Vieira, que desde o começo do curso me deu várias oportunidade para crescer como profissional, como estudante, como pessoa. Obrigada por ter me dado todo o suporte necessário nesses quatro anos e meio de curso, e por aceitar o convite de me orientar. Muito obrigada!

Professora Dra. Louise Reips, por ter me dado todo o apoio, e toda ajuda. Por todas as conversas, para que eu conseguisse chegar até o fim. Muito obrigada!

Fernanda Gonçalves Amaro, Bryan Aoliabe Siqueira e Cleison dos Santos Ramthun, obrigada por dividirem comigo os momentos de felicidade e algumas muitas vezes de desespero. As conquistas, os choros, as madrugadas, o dia a dia. Sem vocês nada disso seria possível. Obrigada!

Por fim, agradeço aos demais professores, familiares e amigos, por toda energia positiva e por cada palavra amiga. Muito Obrigada!

"Quando tiver que escolher entre estar certo e ser gentil, escolha ser gentil."

R. J. Palacio

RESUMO

O presente trabalho de conclusão de curso trata sobre a Criptografia RSA e como ela funciona. Inicialmente, aborda toda a parte teórica, como os números primos, fatoração e congruência, para por fim, entender como e porque a criptografia funciona.

Palavras-chaves: Criptografia RSA. Números Primos. Congruência.

ABSTRACT

This work presents the RSA Cryptography. First, we introduce the prime numbers, fatoration, congruences and then, we study the RSA Cryptography, showing why it works.

Keywords: Cryptography RSA. Prime Numbers. Congruence.

LISTA DE SÍMBOLOS

$mdc(a, b)$	Máximo Divisor Comum de a e b.
$a\|b$	a divide b.
$M(n)$	Números de Mersenne.
$F(n)$	Números de Fermat.
$p^{\#}$	Produto de todos os primos menores e iguais a p.
$\sim$	Relação de equivalência.
$\in$	Pertence.
$\bar{x}$	Conjunto das classes de equivalência de x.
$\subseteq$	Contido.
$\neq$	Diferente.
$\equiv$	Congruente.
$\mathbb{Z}_n$	Conjunto dos inteiros módulo n.
$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{Q}$	Conjunto dos números racionais.

SUMÁRIO

1 INTRODUÇÃO

O presente Trabalho de Conclusão de Curso traz toda a parte teórica que está por trás da Criptografia RSA. Essa criptografia foi desenvolvida em 1978 por R.L Rivest, A. Shamir e L. Adlemann, em Massachussets, e tem esse nome, RSA, justamente por conta das iniciais dos sobrenomes de cada um deles.

A Criptografia RSA é conhecida por ter seu código de codificação público, o que chamamos de chave pública. Teoricamente, a ideia do RSA é muito simples: dados dois parâmetros p e q primos distintos e grandes, utilizamos $n = p \cdot q$ para codificar, e para decodificar precisamos conhecer p e q. A segurança do RSA, vai estar justamente no fato de ser difícil fatorar um número grande, pois ainda não temos métodos avançados que nos ajudem a realizar esse tipo de operação.

No Capítulo 2, entenderemos dois algoritmos que serão fundamentais para entender todo o processo da criptografia: o algoritmo da divisão e o algoritmo de Euclides.

No Capítulo 3, veremos diferentes fórmulas e jeitos de fatorar alguns números e verificar que realmente nenhum deles é suficiente para quebrar a Criptografia RSA, bem como, iniciaremos vendo alguns resultados importantes sobre os Números Primos.

No Capítulo 4, estudaremos maneiras de encontrar Números Primos, seja por meio de fórmulas, de crivos. E vamos verificar também que até hoje, não temos uma fórmula mágica que fornecerá todos os números primos.

No Capítulo 5, revisaremos toda a parte sobre a aritmética modular, principalmente, a relação de congruência. Esse capítulo é um dos principais, se não o mais importante, para que possamos entender todo o processo de codificação e decodificação.

E por fim, o Capítulo 6, é a união do estudo de todos os capítulos anteriores, onde veremos passo a passo, como é realizada a codificação de mensagens e a decodificação. E o mais importante

de todos, o porquê de a Criptografia RSA, realmente funcionar.

2 INTRODUÇÃO À CRIPTOGRAFIA RSA

2.1 ALGORITMOS FUNDAMENTAIS

Primeiramente, precisamos analisar dois algoritmos que serão fundamentais no estudo introdutório da Criptografia. Ambos algoritmos são datados de 300 a.C na Grécia Antiga, e foram enunciados no livro *Os Elementos* de Euclides [3].

Um algoritmo é um conjunto de instruções que auxilia na conclusão de objetivos, ou seja, um algoritmo é uma receita que seleciona determinados ingredientes e o transforma em um determinado produto. É esperado de um algoritmo, que ele acabe em um tempo finito, que seja curto, e que o resultado seja compatível com o esperado.

Ou seja, o algoritmo pode ser enunciado como um teorema: dado um x, existe uma maneira (o próprio algoritmo) de produzir o y, onde x faz o papel de elemento de entrada do algoritmo e o y o elemento de saída do algoritmo.

2.1.1 Algoritmo de Divisão

Estamos interessados na divisão de um número inteiro positivo por outro também positivo, ou seja, a divisão com resto. Dessa forma, precisamos encontrar o quociente e o resto dessa divisão. Por exemplo:

$$\begin{array}{r|l} 1\,2\,3\,4 & 2\,8 \\ \cline{2-2} -\,1\,1\,2 & 4\,4 \\ \cline{1-1} 1\,1\,4 & \\ -\,1\,1\,2 & \\ \cline{1-1} 2 & \end{array}$$

Na divisão anterior de 1234 por 28, encontramos o quociente 44 e o resto 2. Portanto, utilizando a linguagem de algoritmo, temos

como elementos de entrada o dividendo e o divisor, nesse caso, 1234 e 28, respectivamente. E como elementos de saída, o quociente e o resto, nesse caso 44 e 2, respectivamente.

Generalizando o algoritmo da divisão, temos que a *entrada* do algoritmo são os dois inteiros positivos a e b e a *saída* são os outros dois inteiros q e r, que estão relacionados da seguinte forma:

$$a = b \cdot q + r \qquad \text{e} \qquad 0 \leq r < b.$$

Onde a chamamos de dividendo, b de divisor, q de quociente e r é o resto da divisão. Assim, temos o seguinte teorema:

Teorema 2.1 (Algoritmo da Divisão Euclidiana)**.** *Sejam a e b inteiros positivos. Existem números inteiros q e r tais que*

$$a = b \cdot q + r \qquad e \qquad 0 \leq r < b.$$

Além disso, os valores de q e r que satisfazem as relações acima, são únicos.

Demonstração. Por hipótese temos que $a > 0$. Então se $a < b$ é só tomarmos $q = 0$ e $r = a$. Se $a = b$, então teremos que $q = 1$ e $r = 0$. Então, vamos assumir que $0 < b < a$, assim, $a - b \cdot q$ é um número inteiro, maior ou igual a zero. Vamos considerar um conjunto formado por esses elementos. Logo, pelo Princípio da Boa Ordem (Proposição 3.3), temos que esse conjunto admite um menor elemento, chamaremos de r, $r = a - b \cdot q$, para algum $q \geq 0$, além disso $r < b$, pois se não

$$r = a - b \cdot q \geq b \Rightarrow a - b(q + 1) \geq 0. \tag{2.1}$$

Porém, como $b > 0$

$$a - b(q + 1) < a - b \cdot q. \tag{2.2}$$

Das duas desigualdades, podemos tirar que

$$0 \leq a - b(q + 1) < a - b \cdot q.$$

O que é um absurdo, já que $r = a - b \cdot q$ e, por hipótese, que é o menor elemento não negativo do conjunto. Portanto, para quaisquer a e b existe uma divisão Euclidiana.

Para provar que é única, vamos considerar a e b dois inteiros positivos, e vamos supor que existem: q, q',r, r' tais que

$$a = b \cdot q + r \qquad \text{e} \qquad 0 \leq r < b,$$

e

$$a = b \cdot q' + r' \qquad \text{e} \qquad 0 \leq r' < b.$$

Mostraremos que $q = q'$ e que $r = r'$. Como r e r' são inteiros, um dos dois vai ser maior ou igual ao outro. Vamos supor sem perda de generalidade, que $r \geq r'$. Subtraindo as duas equações acima, temos:

$$a - a = b \cdot q + r - (b \cdot q' + r')$$

$$\Rightarrow a - a = b \cdot q + r - b \cdot q' - r'$$

$$\Rightarrow 0 - b \cdot q + b \cdot q' = r - r'$$

$$\Rightarrow b \cdot (q' - q) = r - r'.$$

Sabemos que tanto r quanto r' são menores que b, como supomos também que $r \geq r'$, então temos $0 \leq r - r' < b$, e como $r - r' = b \cdot (q' - q)$, podemos concluir que:

$$0 \leq b \cdot (q' - q) < b.$$

Mas b é um inteiro positivo, então, podemos dividir ambos os lados da desigualdade por b. Assim, ficamos com $0 \leq q' - q < 1$. Como $q' - q$ é um inteiro positivo, então o resultado dessa subtração só pode ser 0, ou seja, $q' - q = 0$, portanto, $q = q'$. Logo, se os quocientes são iguais, os restos também serão. Então, $r' = r$.

■

Antes de continuar, vamos a uma definição muito importante, que aparecerá algumas vezes no decorrer do texto.

Definição 2.1. Sejam a e b números naturais quaisquer. Diremos que a divide b quando existir um número natural t de modo que $b = a \cdot t$.

Utilizamos a notação a|b, para indicar que a divide b.

2.1.2 Algoritmo Euclidiano

O algoritmo Euclidiano facilita o cálculo do máximo divisor comum entre dois números inteiros. Dados dois inteiros positivos a e b, o *máximo divisor comum* entre a e b é o maior inteiro positivo d que é divisor de a e também é divisor de b. Se d for o máximo divisor comum de a e b, escrevemos

$$mdc(a, b) = d$$

Caso o $mdc(a, b) = 1$ dizemos que a e b são *primos entre si*.

Quando os números inteiros são "pequenos" temos como encontrar rapidamente o máximo divisor comum entre eles, através da listagem de seus divisores. Agora, já se torna impraticável esse método se o número for um pouco maior. Felizmente, temos o algoritmo de Euclides que pode nos ajudar nessa busca.

Consideremos a e b novamente, inteiros e positivos, e que $a \geq b$. O algoritmo de Euclides calcula o máximo divisor comum entre a e b da seguinte maneira: primeiro ele divide a por b, obtendo o resto r_1. Se $r_1 \neq 0$. Dividimos b por r_1, achando o resto r_2. Se $r_2 \neq 0$. Dividimos r_1 por r_2, obtendo r_3, e assim por diante, até encontrar o último resto que seja *diferente de zero*. Desta sequência de divisões, esse número será o máximo divisor comum entre a e b.

Para entender melhor esse processo, vamos considerar os inteiros positivos 1234 e 54 e encontrar o máximo divisor comum entre eles, utilizando o método do algoritmo de Euclides. Primeiramente,

então, dividimos 1234 por 54:

$$\begin{array}{r|l} 1\,2\,3\,4 & 5\,4 \\ \cline{2-2} -\,1\,0\,8 & 2\,2 \\ \cline{1-1} 1\,5\,4 & \\ -\,1\,0\,8 & \\ \cline{1-1} 4\,6 & \end{array}$$

O $r_1 = 46$ é diferente de zero. Então, vamos agora dividir b por r_1:

$$\begin{array}{r|l} 5\,4 & 4\,6 \\ \cline{2-2} -\,4\,6 & 1 \\ \cline{1-1} 8 & \end{array}$$

Assim, $r_2 = 8$ que é diferente de zero. Então, continuamos dividindo r_1 por r_2:

$$\begin{array}{r|l} 4\,6 & 8 \\ \cline{2-2} -\,4\,0 & 5 \\ \cline{1-1} 6 & \end{array}$$

Logo, $r_3 = 6$ que é diferente de zero. Então, dividimos r_2 por r_3:

$$\begin{array}{r|l} 8 & 6 \\ \cline{2-2} -\,6 & 1 \\ \cline{1-1} 2 & \end{array}$$

Assim, $r_4 = 2$ que é diferente de zero, Então, dividimos r_3 por r_4:

$$\begin{array}{r|l} 6 & 2 \\ \cline{2-2} -\,6 & 3 \\ \cline{1-1} 0 & \end{array}$$

Como chegamos a um resto $r_5 = 0$ paramos a conta. Assim, o último resto diferente de zero da sequência, que é o $r_4 = 2$, é o $mdc(1234, 54)$. Portanto, tudo que precisa ser feito são sucessivas divisões. Vamos provar agora duas coisas muito importantes. A primeira delas é o porquê este algoritmo ser efetivo. Ou seja, como

temos a certeza de que realizando essas divisões, realmente chegaremos ao máximo divisor comum. E o segundo, é verificar se as divisões sempre chegam a um resto zero ou o algoritmo continua sem fim.

Verificaremos primeiramente a segunda questão. Considere a e b inteiros, positivos com $a \geq b$. Digamos que para encontrar o máximo divisor comum realizamos as seguintes divisões:

$$\begin{gathered} a = bq_1 + r_1 \text{ e } 0 \leq r_1 < b \\ b = r_1q_2 + r_2 \text{ e } 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3 \text{ e } 0 \leq r_3 < r_2 \\ r_2 = r_3q_4 + r_4 \text{ e } 0 \leq r_4 < r_3 \\ \vdots \quad \vdots \end{gathered}$$

Vamos analisar o que está acontecendo com os restos. O resto seguinte é sempre menor que o anterior, e todos eles são maiores ou iguais a zero, ou seja:

$$b > r_1 > r_2 > r_3 > r_4 > ... \geq 0. \tag{2.3}$$

Assim, como entre b e 0 existe uma quantidade finita de inteiros positivos, essa sequência não pode ser infinita. Portanto, como o cálculo só para quando encontramos um resto igual a zero, isso nos dá garantia de que o algoritmo sempre irá parar.

Para realizar a prova do porquê de realmente o algoritmo de Euclides funcionar, vamos primeiramente analisar o lema a seguir.

Lema 2.2. *Sejam a e b números inteiros positivos. Suponhamos que existam inteiros g e s tais que $a = b \cdot g + s$. Então $mdc(a, b) = mdc(b, s)$.*

Demonstração. Queremos provar que, se $a = b \cdot g + s$, então temos que $mdc(a, b) = mdc(b, s)$. Vamos definir $d_1 = mdc(a, b)$ e $d_2 = mdc(b, s)$ e basta provar então que $d_1 = d_2$. Para isso, vamos verificar que $d_1 \leq d_2$ e que $d_2 \leq d_1$. Se ambas forem verdadeiras, chegaremos a igualdade que queremos.

Como $d_1 = mdc(a, b)$, pela definição de máximo divisor comum, temos que d_1 divide a e d_1 divide b. Então, pela Definição 2.1 existem u e v naturais de modo que $a = d_1 \cdot u$ e $b = d_1 \cdot v$. Se substituirmos a e b na equação da hipótese, $a = b \cdot g + s$, teremos:

$$a = b \cdot g + s$$

$$\Rightarrow d_1 \cdot u = d_1 \cdot v \cdot g + s$$

$$\Rightarrow d_1 \cdot u - d_1 \cdot v \cdot g = s$$

$$\Rightarrow d_1 \cdot (u - v \cdot g) = s.$$

Isso significa que d_1 divide s. Mas d_1 divide b. Assim, d_1 é divisor comum de b e s, mas o maior divisor comum entre b e s é d_2. Logo, $d_1 \leq d_2$.

De maneira análoga, vamos provar que $d_2 \leq d_1$. Como $d_2 = mdc(b, s)$, então, d_2 divide b e d_2 divide s. Assim, existem c e f naturais, de modo que $b = d_2 \cdot c$ e $s = d_2 \cdot f$. Substituindo em $a = b \cdot g + s$, temos:

$$a = b \cdot g + s$$

$$\Rightarrow a = d_2 \cdot c \cdot g + d_2 \cdot f$$

$$\Rightarrow a = d_2(c \cdot g + f).$$

Assim, d_2 divide a, mas d_2 divide b. Assim, d_2 é divisor comum de a e b. Como d_1 é o maior dos divisores de a e b, temos $d_2 \leq d_1$.

Portanto, como provamos que $d_1 \leq d_2$ e $d_2 \leq d_1$, concluímos que $d_1 = d_2$, como queríamos provar.

■

Vamos utilizar o lema anterior para provar que a sequência de divisões realmente resulta no máximo divisor comum.

Aplicaremos então, o algoritmo de Euclides a a e b e vamos supor que o resto zero acontece após n divisões. Assim temos:

$$a = b \cdot q_1 + r_1 \text{ e } 0 \leq r_1 < b$$

$$
\begin{gathered}
b = r_1 \cdot q_2 + r_2 \text{ e } 0 \leq r_2 < r_1 \\
r_1 = r_2 \cdot q_3 + r_3 \text{ e } 0 \leq r_3 < r_2 \\
r_2 = r_3 \cdot q_4 + r_4 \text{ e } 0 \leq r_4 < r_3 \\
\vdots \\
r_{n-4} = r_{n-3} \cdot q_{n-2} + r_{n-2} \text{ e } 0 \leq r_{n-2} < r_{n-3} \\
r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} \text{ e } 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1} \cdot q_n \text{ e } r_n = 0
\end{gathered}
$$

Na última divisão, temos que r_{n-1} divide r_{n-2}. Logo, o maior divisor comum entre os dois é r_{n-1}, ou seja, $mdc(r_{n-2}, r_{n-1}) = r_{n-1}$.

Vamos aplicar o lema, nas linhas das divisões para ver o que acontece. Começando pela penúltima linha, temos que:

$$mdc(r_{n-3}, r_{n-2}) = mdc(r_{n-2}, r_{n-1})$$

e como $mdc(r_{n-2}, r_{n-1}) = r_{n-1}$, então

$$mdc(r_{n-3}, r_{n-2}) = r_{n-1}$$

Aplicando na antepenúltima linha, temos:

$$mdc(r_{n-4}, r_{n-3}) = mdc(r_{n-3}, r_{n-2})$$

E daí:

$$mdc(r_{n-4}, r_{n-3}) = r_{n-1}.$$

Se continuarmos com esse procedimento, vamos chegar que $mdc(a, b) = r_{n-1}$, como queríamos provar.

3 FATORAÇÃO

Todo número inteiro pode ser escrito como um produto de números primos. Saber que essa decomposição existe será muito importante para a descoberta de propriedades interessantes sobre números inteiros. Porém, muitas vezes, encontrar a decomposição de um número inteiro pode ser um processo demorado e árduo.

3.1 TEOREMA DA FATORAÇÃO ÚNICA

Há muito tempo, na Grécia Antiga, o filósofo grego Demócrito denominou as partículas pequenas de uma matéria de **átomo**. Do grego *a*: não; *tomo*: divisão, porque naquela época se acreditava mesmo que o átomo não era divisível.

Na aritmética, essa ideia também existe e também vem de muito tempo atrás, só que em vez dos átomos, temos os *Números Primos*. Por volta de 500 a.C a 300 a.C, os pitagóricos se interessaram muito pelas propriedades desses números. Afinal, eles são responsáveis por gerar todos os números inteiros, exceto o 0 e o ± 1.

Os gregos classificavam os números em primeiro (ou indecomponíveis) e secundários (ou compostos). Os números compostos são secundários por serem formados a partir dos primos. Os romanos, algum tempo depois, apenas traduziram literalmente a palavra grega para primeiro, que em latim é *primus*. É daí que vêm a origem do nome: *Números Primos*.

E é com a decomposição de inteiros primos que trabalharemos nesse capítulo. Por isso, é interessante que recordemos a definição de números primos.

Definição 3.1. Um número inteiro p é primo se $p \neq \pm 1$ e $p \neq 0$ e os únicos divisores de p são ± 1 e $\pm p$.

Portanto 2, 11, 13 e -5 são primos, pois todos eles possuem apenas o ± 1 e eles mesmos (com seus opostos) como divisores. Já 35 não é um número primo, pois $35 = 7 \cdot 5$. Chamamos estes números, que são diferentes de 0 e ± 1 e que não são primos de, *números compostos*. Portanto, 35 é um *número composto*.

Pela definição de números primos, sabemos que os números ± 1 não são primos, e também não são compostos.

O principal teorema deste capítulo é muito conhecido como o *Teorema Fundamental da Aritmética*. O principal matemático a enunciá-lo foi Carl Friedrich Gauss (1777-1855) em um dos seus mais famosos livros: *Disquisitiones Arithmeticae*, o que não significa que esse resultado não tenha vindo da Grécia Antiga, por meio de outros matemáticos. Sua origem é dada a Gauss, somente por ele ter desenvolvido a aritmética como uma ciência sistemática (Hardy & Wright, 1994).

Teorema 3.1 (Teorema Fundamental da Aritmética em $\mathbb{N}$)**.** *Dado um inteiro positivo $n \neq 1$, podemos sempre escrevê-lo, de modo único, na forma*

$$n = p_1^{e_1} \ ... \ p_k^{e_k},$$

onde $1 < p_1 < p_2 < p_3 < ... < p_k$ são números primos e $e_1, ..., e_k$ são inteiros positivos.

Chamamos os expoentes da fatoração $e_1, ..., e_k$ de *multiplicidades*. Assim, a multiplicidade de p_1 na fatoração do número n é e_1, ou seja, a multiplicidade de p_1 é o maior expoente e_1 tal que $p_1^{e_1}$ divide n. Quando fatoramos um número n qualquer, temos k fatores primos, e se somarmos as multiplicidades $e_1 + ... + e_k$ saberemos a quantidade total de fatores primos, sejam eles distintos ou não, que n possui.

Analisando o teorema, podemos tirar duas informações muito importantes: a primeira, é que podemos escrever todo número inteiro como o produto de potências de números primos. E a se-

gunda informação, é que só há uma alternativa possível de primos e expoentes para a fatoração. Portanto, teremos que provar que a fatoração existe e que ela é única.

Antes de começarmos a prova, se olharmos para o enunciado do teorema, conseguiremos entender por que o ± 1 não é considerado primo pela definição. Vamos lá. Se considerássemos 1 número primo, então 7 e $1^2 \cdot 7$ seriam duas formas de fatorar o número 7, logo, não poderíamos falar sobre unicidade de uma fatoração.

A existência do Teorema Fundamental da Aritmética significa que, dado um inteiro $n \geq 2$, podemos escrevê-lo como produto de primos. Assim, para demonstrar a existência vamos utilizar um algoritmo, que tem como entrada n, e que tem como saída seus fatores primos e os respectivos expoentes.

O algoritmo mais simples, para determinar um fator de um inteiro dado, é o seguinte: consideremos n como entrada e dividimos n por todos os inteiros de 2 a $n-1$. Se algum destes inteiros dividir n, então teremos achado um fator de n. Além disso, o menor fator que encontrarmos dessa maneira, deve ser primo.

Mas, por que o menor dos fatores será um número primo? Seja f um inteiro tal que $2 \leq f \leq n-1$. Vamos supor que f é o menor fator de n e que f' é um fator (maior que 1) de f. Pela definição de divisibilidade, existem inteiros a e b tais que

$$n = f \cdot a \text{ e } f = f' \cdot b$$

Se substituirmos f na primeira igualdade, ficaremos com, $n = f' \cdot ab$, assim f' também é fator de n. Mas, por hipótese, temos que f é o menor fator de n. Portanto, concluímos que $f \leq f'$. Mas, f' é fator de f, o que só pode acontecer se $f' \leq f$. Assim, das duas desigualdades temos que $f = f'$. Portanto, o único fator de f que é maior que 1 é o próprio f. Logo, f é primo.

O algoritmo começa a procura de divisores de n a partir do número 2. Sobre o algoritmo, ainda temos que fazer uma observação, pois, se começarmos a realizar as operações, quando devemos parar? Bem, como um número inteiro não contém divisores maiores que o

próprio número, não precisamos passar de $n-1$. Melhor ainda, não precisamos procurar divisores maiores que $\sqrt{n}$. Como o algoritmo encontra o menor divisor de n maior que 1, basta que provemos que ele será obrigatoriamente menor ou igual a $\sqrt{n}$. Porém, se temos n primo, então o menor divisor maior que 1, é o próprio n. Temos que verificar então, que se n é composto e se $f > 1$ é o menor divisor, então $f \leq \sqrt{n}$.

Proposição 3.2. *Se n é um número composto, e $f > 1$ é seu menor divisor, então $f \leq \sqrt{n}$.*

Demonstração. Queremos provar que, dados n um número composto e $f > 1$ o seu menor divisor, então f será menor ou igual a $\sqrt{n}$. Por hipótese temos que f é o menor divisor de n, ou seja, existe p inteiro positivo de modo que, $n = f \cdot p$. A partir disso, podemos entender que p também é divisor de n. Mas, por hipótese, temos que f é o menor divisor de n maior que 1. Então, $f \leq p$. Se multiplicarmos ambos os lados da desigualdade por f, temos

$$f \leq p \Rightarrow f \cdot f \leq f \cdot p.$$

Como $f \cdot p = n$, substituímos na desigualdade, ficando com $f^2 \leq n$. Se tirarmos a raiz quadrada em ambos os lados, teremos que, $\sqrt[2]{f^2} \leq \sqrt{n} \Rightarrow f \leq \sqrt{n}$, como queríamos provar.

■

Basicamente então, vimos que o algoritmo deve procurar um número que é divisor de n, começando por 2 até $\sqrt{n}$. Se o divisor for um número composto, teremos certeza que encontramos seu menor divisor por esse método, além disso, teremos garantia de que n é primo. Agora, se utilizarmos esse método, e não conseguirmos nenhum divisor do número, significa que o próprio número é primo. Assim, basta aplicar esse algoritmo sucessivas vezes e teremos a fatoração de um dado número.

3.2 PROPRIEDADE FUNDAMENTAL DOS PRIMOS

Proposição 3.3 (Princípio da Boa Ordem)**.** *Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.*

Teorema 3.4 (Teorema de Bézout)**.** *Dados a e b inteiros positivos, existem inteiros α e β tais que:*

$$a \cdot \alpha + b \cdot \beta = mdc(a, b)$$

O Teorema de Bézout é facilmente demonstrado utilizando o Princípio da Boa Ordem, para isso, basta demonstrar que existe um menor elemento no conjunto formado pelos elementos do tipo $a \cdot \alpha + b \cdot \beta$, e que esse elemento é exatamente o $mdc(a, b)$. O Princípio da Boa Ordem está demonstrado em [4] (página 16). E a demonstração completa do Teorema de Bézout, é facilmente encontrada em [1].

Antes de provar que a fatoração de números primos é única, precisamos estudar uma propriedade muito importante e fundamental dos Números Primos. Para isso, vamos provar antes uma proposição e um lema.

Proposição 3.5. *Se $a|m$ e $a|n$ então, $a|(m + n)$.*

Demonstração. Queremos provar que se a divide m e a divide n, então a vai dividir a soma $m + n$. Por hipótese, temos que $a|m$ e $a|n$, por definição, existem t e k naturais, de modo que $m = t \cdot a$ e $n = k \cdot a$. Assim, temos que:

$$m + n = t \cdot a + k \cdot a = (t + k) \cdot a. \tag{3.1}$$

Mas, como t e k são números naturais, então $z = t + k$ também é um número natural, já que a soma de dois números naturais é um número natural.
Portanto, por (3.1) temos que $m + n = z \cdot a$. Por definição, isso significa que $a|(m + n)$.

■

Lema 3.6. *Sejam a, b e c inteiros positivos e suponhamos que a e b são primos entre si.*

(1) Se $b|(a \cdot c)$ então $b|c$.
(2) Se $a|c$ e $b|c$ então $(a \cdot b)|c$.

Demonstração. Temos por hipótese que a e b são primos entre si, ou seja, que o $mcd(a, b) = 1$. Pelo Teorema de Bézout:

$$\alpha \cdot a + \beta \cdot b = 1$$

Para provar (1), vamos considerar c um número inteiro positivo, e multipliquemos em ambos os lados da igualdade o c, assim:

$$c \cdot (\alpha \cdot a + \beta \cdot b) = c \cdot 1$$

Utilizando a propriedade distributiva, obtemos:

$$\alpha \cdot ac + \beta \cdot bc = c$$

É visível que $\beta \cdot bc$ é divisível por b. Pela hipótese de (1), temos que b divide ac. Portanto a parcela $\alpha \cdot ac$ também é divisível por b. Assim, como b divide cada uma das parcelas, pela Proposição 3.5, b dividirá a soma. Por consequência, b dividirá c.

Agora, para provar (2), usaremos o que acabamos de provar para (1). Por hipótese, temos que a divide c, logo: $c = a \cdot t$, para algum inteiro t. Na mesma hipótese, temos que b também divide c, e como a e b são primos entre si, do item (1), temos que b tem que dividir t. Logo, podemos escrever como $t = b \cdot k$, para algum k inteiro. Assim, temos as seguintes igualdades:

$$c = at = a(bk) = (ab)k$$

Portanto, ab divide c, como queríamos demonstrar.

■

Podemos agora demonstrar a propriedade mais importante dos números primos, conhecida como Propriedade Fundamental dos

Números Primos. Esta propriedade é muito importante e é conhecida desde a Grécia Antiga. Sendo que, se encontra em um dos livros mais traduzidos do mundo, e lido pelas mentes mais brilhantes já conhecidas, *Os Elementos* [3] de Euclides, no livro VII, Proposição 30.

Teorema 3.7 (Propriedade Fundamental dos Primos)**.** *Sejam p um número primo e a e c inteiros positivos. Se p divide o produto ac então p divide a ou p divide c.*

Demonstração. Queremos provar que se p divide o produto ac então, p vai dividir a ou p vai dividir c.

Se p dividir a, temos a propriedade fundamental demonstrada.

Vamos ver o caso em que p não divide a. Então p e a são primos entre si. Logo, $mdc(p, a) = 1$. Assim, como p e a são primos entre si e como p divide ac por hipótese, utilizando o lema anterior, temos então que p divide c.

Portanto, a Propriedade Fundamental dos Números Primos está provada.

■

Uma aplicação da Propriedade Fundamental dos Primos é que, dado p primo, então $\sqrt[k]{p}$ é um número irracional, onde $k \in \mathbb{N}$ e é maior que 1 e $p > 0$ se k for par. Para provar esse caso, utilizaremos o método da *redução ao absurdo* ou também conhecido como *demonstração por contradição.*

Sabemos que os números irracionais são aqueles que não podem ser obtidos pela divisão de dois números inteiros, ou seja, números que não podem ser escritos na forma de fração.

Proposição 3.8. *Se p for primo, então $\sqrt[k]{p}$ será um número irracional, para todo $k \in \mathbb{N}$ e maior que 1 e $p > 0$ se k for par.*

Demonstração. Queremos provar que $\sqrt[k]{p}$ é um número irracional para qualquer k pertencente aos naturais. Vamos supor, então, que $\sqrt[k]{p}$ pode ser escrito como uma fração, e vamos tentar encontrar algum absurdo. Se conseguirmos, então significa que nossa hipótese é falsa. Portanto, $\sqrt[k]{p}$ é irracional.

Se $\sqrt[k]{p}$ pode ser escrito como uma fração, então existem a e b inteiros positivos, de modo que:

$$\sqrt[k]{p} = \frac{a}{b}.$$

Além disso, vamos supor que a fração está na sua forma reduzida. Ou seja, que $mdc(a, b) = 1$. Elevamos ambos os lados da equação anterior à k e obtemos

$$(\sqrt[k]{p})^k = \frac{a^k}{b^k} \Rightarrow p = \frac{a^k}{b^k}.$$

Multiplicando em ambos os lados por b^k

$$b^k \cdot p = b^k \cdot \frac{a^k}{b^k} \Rightarrow b^k \cdot p = a^k.$$

Logo, p divide a^k. Pela *Propriedade Fundamental dos Primos* temos que: p divide a, ou seja, existe um inteiro c tal que $a = p \cdot c$. Substituindo a na equação anterior,

$$b^k \cdot p = (p \cdot c)^k \Rightarrow b^k \cdot p = p^k \cdot c^k.$$

Para $k > 1$, pela lei do cancelamento da multiplicação, podemos cancelar p em ambos os lados, assim:

$$b^k = p^{k-1} \cdot c^k.$$

Podemos concluir da equação que resultou, que p divide b^k. Utilizando novamente a *Propriedade Fundamental dos Primos*, temos que p divide b. O que é um absurdo, pois, se realmente p divide a e p divide b, então o $mdc(a, b)$ não é 1. Portanto, $\sqrt[k]{p}$ é irracional, como queríamos demonstrar.

■

Teorema 3.9. *A fatoração de um número inteiro é única.*

Demonstração. Queremos demonstrar que a fatoração é única. Para isso, vamos supor então que existe um número inteiro que admite mais de uma fatoração. Vamos chamar esse inteiro de n e vamos supor que n seja o *menor* inteiro positivo entre os que admitem duas fatorações distintas. Pelo teorema, podemos escrever:

$$n = p_1^{e_1} \cdots p_k^{e_k} = q_1^{r^1} \cdots q_s^{r_s} \tag{3.2}$$

onde $p_1 < ... < p_k$ e $q_1 < ... < q_s$ são primos e $e_1, ..., e_k$ e $r_1, ..., r_s$ são inteiros positivos. Porém, estamos supondo que essas duas fatorações sejam diferentes. Isto pode acontecer por dois motivos: os primos da direita podem não ser os mesmos que os da esquerda, ou caso sejam os mesmos, podem ter multiplicidades diferentes. Vamos analisar cada situação.

Analisando a fatoração da esquerda, p_1 é um primo que divide n. Porém se olharmos para a fatoração da direita, $n = q_1^{r^1} ... q_s^{r_s}$. A *Propriedade Fundamental dos Primos* garante que p_1 deve dividir um dos fatores do produto que esta à direita, mas um primo só pode dividir outro se eles forem iguais. Então, p_1 tem que ser um dos primos $q_1, q_2, ...$ ou q_s. Sem perda de generalidade, digamos que $p_1 = q_j$, onde $1 \leq j \leq s$.

Substituindo q_j por p_1

$$\begin{aligned} n = p_1^{e_1} \cdots p_k^{e_k} &= q_1^{r^1} \cdots q_s^{r_s} \\ &= q_1^{r_1} \cdots p_1^{r_j} \cdots q_s^{r_s} \end{aligned}$$

Pela lei do cancelamento na multiplicação, podemos cancelar p_1 em ambos os lados. Assim:

$$\frac{n}{p_1} = m = p_1^{e_1 - 1} \cdots p_k^{e_k} = q_1^{r_1} \cdots p_1^{r_j - 1} \cdots q_s^{r_s} \tag{3.3}$$

que é um novo número menor que n. Porém, m tem duas fatorações, como mostra a equação (3.3). Essas equações foram obtidas da fatoração de (3.2) que são diferentes por hipótese. Portanto, as fatorações de m em (3.3) são necessariamente distinta.
Portanto, temos um número m que é menor que n que apresenta

duas fatorações distintas. O que é um absurdo. Pois, já assumimos que n era o menor inteiro positivo que apresentava duas fatorações diferentes. Portanto, concluímos que a fatoração é única.

■

4 NÚMEROS PRIMOS

A segurança da Criptografia RSA depende da dificuldade da fatoração e detecção de números primos. Nesse capítulo vamos ver alguns métodos e fórmulas para encontrar alguns números primos. Inicialmente, discutiremos três dessas:

- Fórmulas polinomiais;
- Fórmulas exponenciais;
- Fórmulas fatoriais.

Além das fórmulas, veremos um método muito antigo de gerar todos os números primos positivos até um dado $n \in \mathbb{N}$, chamado *Crivo de Eratóstenes*, que, de fato, gera todos os números primos positivos até um dado $n \in \mathbb{N}$, porém de forma muito lenta.

4.1 FÓRMULAS POLINOMIAIS

Quando pensamos em fórmulas, o jeito mais simples que temos são as fórmulas polinomiais. Vamos considerar uma função polinomial do tipo:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0,$$

onde os coeficientes $a_n, a_{n-1}, ..., a_1, a_0$ são números inteiros com $a_n \neq 0$, e que satisfazem a seguinte condição

$$f(m) \text{ é primo para todo inteiro positivo } m.$$

Para ficar mais claro, vamos analisar o que acontece com o seguinte exemplo: $f(x) = x^2 + 1$. Faremos então, uma tabela com inteiros

positivos x e seus respectivos valores de $f(x)$. Assim temos:

x	$f(x)$
1	2
2	5
3	10
4	17
5	26
6	37
7	50
8	65
9	82
10	101

Podemos observar que quando x é um número ímpar, então o seu $f(x)$ é um número par. Ou seja, para x ímpar diferente de 1, encontramos sempre números compostos para $f(x)$, pois são múltiplos de 2.

Assim, só há a possibilidade de gerar números primos quando $x > 1$ e quando x é um número par. Porém, observe na tabela que $f(8) = 65$, e 65 é um número composto. Ou seja, esse polinômio em questão não nos fornece uma fórmula para números primos.

Teorema 4.1. *Dado uma função polinomial f(x) com coeficientes inteiros, existe uma infinidade de inteiros positivos m tais que f(m) é um número composto.*

Demonstração. Queremos provar que existem infinitos inteiros positivos m onde $f(m)$ é um número composto. Para isso, vamos considerar apenas os casos em que o polinômio f tem grau dois.

Então, seja $f(x) = ax^2 + bx + c$ um polinômio onde os coeficientes a, b e c são números inteiros, com $a \neq 0$. Para que $f(x)$ seja sempre positivo para qualquer valor de x, vamos supor que $a, b, c > 0$, e separar em dois casos:

1º caso: Se $f(x)$ for um número composto para qualquer x inteiro

positivo, temos o teorema demonstrado. Vamos supor no segundo caso que existe um inteiro positivo m, que dê um número primo.

2º caso: Vamos supor então, que existe um inteiro positivo m, de modo que $f(m) = p$ é um primo positivo. Consideremos então, um h inteiro positivo qualquer. Assim:

$$f(m + hp) = a(m + hp)^2 + b(m + hp) + c.$$

Realizando o produto notável e colocando p em evidência, temos

$$f(m + hp) = (am^2 + bm + c) + p(2amh + aph^2 + bh).$$

Podemos perceber que toda a expressão que está no primeiro parênteses é igual a $f(m)$, que é igual a p. Assim, substituindo toda ela por p ficamos com

$$f(m + hp) = p \cdot (1 + 2amh + aph^2 + bh). \tag{4.1}$$

Portanto, o que podemos concluir é que, já que $f(m + hp)$ é p vezes algum inteiro, então ele é um número composto. Mas, precisamos ter certeza de que a expressão toda que está sendo multiplicada por p, não seja 1. Para isso, devemos encontrar e saber para quais valores de h a expressão seja maior que 1. Ou seja:

$$1 + 2amh + aph^2 + bh > 1.$$

Se subtrairmos 1 em ambos os lados:

$$2amh + aph^2 + bh > 0.$$

Por hipótese, temos que h é positivo. Então, as seguintes desigual-

dades são verdadeiras:

$$\begin{aligned} 2amh + aph^2 + bh &> 0 \\ \Leftrightarrow aph^2 + bh &> -2amh \\ \Leftrightarrow aph^2 &> -2amh - bh \\ \Leftrightarrow h \cdot (aph) &> h \cdot (-2am - b) \\ \Leftrightarrow h &> \frac{-2am - b}{ap} \\ \Leftrightarrow h &> \frac{-b - 2am}{ap}. \end{aligned}$$

Basicamente, o que mostramos é que se $f(x) = ax^2 + bx + c$ é um polinômio com coeficientes inteiros ($b > 0$) e $f(m) = p$ é primo. Então, $f(m+hp)$ será um número composto sempre que $h > \frac{(-b-2am)}{ap}$. Esse teorema consegue nos mostrar, que existem infinitos valores inteiros positivos x de modo que $f(x)$ seja um número composto.

■

Podemos demonstrar o mesmo teorema para um polinômio de qualquer grau. Porém, precisaríamos utilizar e envolver assuntos como somatório, cotas, binômio de Newton que não são o foco desse trabalho.

O que podemos concluir de tudo que vimos, é que não é promissor buscar uma fórmula polinomial que nos dê todos os números primos, pelo menos quando estivermos considerando polinômios em uma variável apenas. Há polinômios de grau mais elevado e com muitas variáveis, que fornecem números primos. Porém, por serem muito complicadas de se usar, acabam não sendo muito úteis.

4.2 FÓRMULAS EXPONENCIAIS: NÚMEROS DE MERSENNE E OS NÚMEROS DE FERMAT

Existem duas fórmulas exponenciais que foram muito estudadas por dois matemáticos do século XVII, Fermat e Mersenne. Ambas as fórmulas são de enorme importância para a história. São elas:

$$M(n) = 2^n - 1 \text{ e } F(n) = 2^{2^n} + 1,$$

onde n é um inteiro positivo. Chamamos os números da forma $M(n)$ de *Números de Mersenne*, e os da forma $F(n)$ de *Números de Fermat*.

Os números de Mersenne eram utilizados para encontrar os números primos, na Grécia antiga. Os números na forma $2^n - 1$ levaram seu nome, pois, Mersenne afirmou que os números nessa forma só seriam primos, quando n fosse os seguintes valores:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ e } 257;$$

e seriam compostos para os demais 44 primos de n, que são menores que 257. A primeira observação que podemos fazer é que todos os n da lista de Mersenne são números primos de fato, se algum n fosse composto $M(n)$ também seria um número composto.

Proposição 4.2. *Se n for um número composto então M(n) será um número composto.*

Demonstração. Vamos provar que isso realmente acontece, da seguinte maneira. Vamos considerar $n = r \cdot s$ um número composto, então

$$M(n) = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + ... + 2^r + 1)$$

Logo, se r divide n, então $M(r)$ divide $M(n)$.

■

Se olharmos na lista de números teremos que Mersenne indicou para n, o primo 11 não está incluso, de fato. Vamos calcular $M(11) = 2^{11} - 1 = 2048 - 1 = 2047$, e podemos escrever o 2047 como $23 \cdot 89$.

Anos depois, alguns matemáticos encontraram alguns erros na lista dada por Mersenne. Os números $61, 89$ e 107 são primos e não estão na lista. E a lista inclui os números 67 e 257 que são

compostos.

Os números de Fermat e sua história, se assemelham muito a de Mersenne. Basicamente, Fermat enunciou que para os seguintes valores de n:

$$3, 5, 17, 257, 65537$$

a forma $F(n) = 2^{2^n} + 1$ será um número primo.

Se compararmos os primos de Mersenne e de Fermat, é nítido que os números de Mersenne nos dão mais números primos que os de Fermat. Até o momento, só são conhecidos esses primos de Fermat. Como a fórmula de Fermat trabalha com exponencial de uma exponencial, é injusto acharmos que a fórmula de Fermat é pouco eficiente.

4.3 FÓRMULAS FATORIAIS

Suponhamos que p seja um primo positivo, primeiramente, por definição, $p^{\#}$ será o produto de todos os primos menores ou iguais ao próprio p. Por exemplo, vamos considerar $p = 5$ então, $p^{\#} = 5^{\#} = 2 \cdot 3 \cdot 5 = 30$, basicamente, um fatorial de primos. Mas por quê isso é importante? Observemos a tabela a seguir:

p	$p^{\#}$	$p^{\#} + 1$
2	2	3
3	6	7
5	30	31
7	210	211
11	2310	2311

Os números da terceira coluna claramente são primos. Porém, nem todo p primo, resultará em um primo. É o caso do $13^{\#}+1 = 30031 = 59 \cdot 509$, que é um número composto.

Proposição 4.3. *Não existe nenhum fator primo de $p^{\#} + 1$ menor ou igual a p.*

Demonstração. Vamos supor que existe um divisor primo $q \leq p$, que dividirá $p^{\#} + 1$. Ou seja, existe um inteiro positivo r de modo que $p^{\#} + 1 = q \cdot r$. Rearranjando a equação, temos $q \cdot r - p^{\#} = 1$. Como assumimos que $q \leq p$ então, q é um fator primo de $p^{\#}$. Então, q irá dividir $q \cdot r - p$ e q irá dividir 1, então $q = 1$, o que não é possível, pois q é um número primo. Portanto, independente se $p^{\#}$ é primo ou composto, o menor fator primo de $p^{\#} + 1$ terá que ser maior que o próprio p.

■

No que diz respeito a fórmula fatorial para encontrarmos primos, não temos muito sucesso, visto que conhecemos apenas 16 primos, por meio da fórmula fatorial, e o maior deles é quando $p = 24029$.

O verdadeiro motivo pelo qual vemos a fórmula fatorial, não é para encontrarmos números primos, mas sim, demonstrar que existem infinitos primos.

Teorema 4.4. *Existem infinitos números primos.*

Demonstração. Vamos supor que existem finitos primos. Assim, existirá um primo p que será maior que todos os outros. Vimos que dado um inteiro $p^{\#} + 1$ ele não pode ter divisores primos $\leq p$. Assim o número inteiro $p^{\#} + 1$ não terá fatores primos, o que é um absurdo, já que vimos que todo número inteiro pode ser fatorado em primos e que essa fatoração é única. Portanto, existem infinitos primos.

■

4.4 CRIVO DE ERATÓSTENES

Um dos métodos mais antigos para encontrar números primos é muito simples, porém trabalhoso, chamado *Crivo de Eratóstenes*. Eratóstenes foi uma matemático grego, nascido por volta de 284 a.C.. Foi muito bom em diversas áreas, mas nunca foi perfeito em nenhuma delas, e era muito julgado por isso. Antigamente, cha-

mavam o crivo de peneira, onde existiam vários números, e ao final de todo o processo só sobravam os números primos.

O objetivo do Crivo então é encontrar todos os primos até um dado $n \in \mathbb{N}$ e funciona da seguinte forma: dado um inteiro positivo n, listamos todos os ímpares de 3 a n. O primeiro número da lista é o 3, portanto riscamos todos os números de 3 em 3. Ou em outras palavras, riscamos todos os múltiplos de 3 maiores que ele. O passo seguinte é procurar o próximo número depois do 3 que não tenha sido riscado, que é 5. Assim, riscamos agora todos os múltiplos de 5 maiores que ele. E assim, até chegar em n. Por exemplo, vamos considerar $n = 40$. Listamos então os ímpares de 3 à 40:

$$3\ 5\ 7\ 9\ 11\ 13\ 15\ 17\ 19\ 21\ 23\ 25\ 27\ 29\ 31\ 33\ 35\ 37\ 39$$

Agora, riscamos todos os múltiplos de 3 maiores que ele, assim

$$3\ 5\ 7\ \not{9}\ 11\ 13\ \not{15}\ 17\ 19\ \not{21}\ 23\ 25\ \not{27}\ 29\ 31\ \not{33}\ 35\ 37\ \not{39}$$

Procuramos o próximo número, que é maior que 3, e não está riscado. Nesse caso é o 5. E riscamos todos os múltiplos de 5

$$3\ 5\ 7\ \not{9}\ 11\ 13\ \not{15}\ 17\ 19\ \not{21}\ 23\ \not{25}\ \not{27}\ 29\ 31\ \not{33}\ \not{35}\ 37\ \not{39}$$

Encontramos o próximo número que não está riscado. Nesse caso o 7, e repetimos o mesmo procedimento. Porém, não conseguiremos riscar nenhum múltiplo de 7. O mesmo vai acontecer com o 11, e com os demais até n. Portanto, os primos ímpares menores que 40, serão os números que não estão riscados:

$$3\ 5\ 7\ 11\ 13\ 17\ 19\ 23\ 29\ 31\ 37$$

O que podemos notar é que alguns números são riscados da lista mais de uma vez, e que a partir da terceira passagem, já tínhamos o crivo com os números primos prontos. Pela Proposição 3.2, basta que risquemos até $\sqrt{n}$. Assim, no exemplo anterior $6 < \sqrt{40} < 7$, então bastava apenas que cortássemos os múltiplos de 3 e de 5, e nada mais.

5 ARITMÉTICA MODULAR

Quando estamos falando da aritmética que todos conhecemos, $15 + 17$ sem sombra de dúvidas resulta em 32. Mas tem quem diga que dá 8, e pode provar que realmente dá 8. Vamos pensar no caso em que o número 15 represente 15 horas. Se somarmos mais 17 horas, serão 8 horas da manhã. Logo, nesse caso $15 + 17 = 8$. Agora que sabemos disso, podemos pensar em vários outros casos. Os anos, o mês, ou seja, qualquer fenômeno que tem um ciclo, ou seja, que é cíclico, é capaz de produzir esse tipo de aritmética.

A essa aritmética damos o nome de *Aritmética Modular*. Nesse capítulo, veremos como realizamos operações básicas, como soma, subtração, multiplicação, divisão e potenciação, com esse modelo de aritmética.

5.1 RELAÇÕES DE EQUIVALÊNCIA

Toda vez que realizamos uma comparação entre dois elementos de um conjunto qualquer, estamos definindo uma relação entre esses elementos. Por exemplo, $2 = 2$ e $4 \neq 6$ temos essas duas relações básicas para os números naturais, de igualdade e desigualdade. Outro exemplo bem prático e fora da matemática, é se considerarmos um conjunto de bolas coloridas. Uma relação que teremos para as bolas é *Ser de uma mesma cor*.

Considere X um conjunto onde está definida uma relação que é denotada por $\sim$. Sejam $x, y, z \in X$. Chamamos $\sim$ de *relação de equivalência* se são satisfeitas as seguintes propriedades:

(1) Propriedade Reflexiva: $x \sim x$
(2) Propriedade Simétrica: Se $x \sim y$ então $y \sim x$
(3) Propriedade Transitiva: Se $x \sim y$ e $y \sim z$ então $x \sim z$

A primeira propriedade pode ser averiguada nos números naturais, com a relação de igualdade. Todo número é igual a ele mesmo. Já a relação de estritamente menor nos inteiros não é reflexiva: -4 não é menor que -4.

Podemos perceber que mesmo a segunda propriedade não é satisfeita na relação de estritamente menor 2 é menor que 4, mas 4 não é menor que 2. Agora, se eu falar que João é irmão de Mateus, é verdade também que Mateus é irmão de João. Assim temos uma relação, onde a propriedade simétrica é válida.

Para a terceira propriedade temos mais relações que funcionam: a igualdade nos inteiros, estritamente menor, a relação de menor ou igual. Por exemplo, $-4 \leq -1$, $-1 \leq 5$ implica que $-4 \leq 5$. Agora, a relação de diferente nos inteiros não é transitiva, de fato, $5 \neq 7$ e $7 \neq 5$ mas não é verdade que $5 \neq 5$.

Utilizamos as relações de equivalência para classificar elementos de um conjunto, em subconjuntos que tenham propriedades semelhantes. Por exemplo, vamos olhar para o conjunto de bolas coloridas. Pela relação: ser de uma mesma cor. Chamamos cada conjunto de bolas de uma mesma cor de *classe de equivalência.*

Definição 5.1. Seja X um conjunto e $\sim$ uma relação de equivalência que está definida em X. Se $x \in X$ então, a classe de equivalência de x é o conjunto de elementos de X que são equivalentes a x pela relação $\sim$, ou seja:

$$\bar{x} = \{y \in X : x \sim y\}$$

Continuaremos utilizando o exemplo do conjunto das bolas coloridas, porque o entendimento é mais efetivo. Vamos supor que alguém disse que o subconjunto de bolas que temos nas mãos é uma classe de equivalência. Ora, para descobrir qual é a classe de equivalência, basta apenas checar a cor de uma das bolas. Assim, saberemos exatamente a qual classe de equivalência ela pertence. Ou seja, esse fato nos mostra que com apenas um só elemento, conseguimos identificar a classe inteira. Esse resultado é um dos mais importantes das classes de equivalência. E vamos provar a seguir que é verdadeira para qualquer que seja o conjunto.

Proposição 5.1. *Dado um conjunto X e uma relação de equivalência $\sim$, se y é um elemento da classe de x então $\bar{x} = \bar{y}$.*

Demonstração. Como queremos provar que dois conjuntos são iguais, precisamos mostrar que $\bar{x} \subseteq \bar{y}$ e que $\bar{y} \subseteq \bar{x}$.

$\bar{x} \subseteq \bar{y}$**:** Seja $z \in \bar{x}$. Como $y \in \bar{x}$, por definição $x \sim y$ e pela simetria, $y \sim x$. Por definição também, $x \sim z$. Pela transitividade, se $y \sim x$ e $x \sim z$ então $y \sim z$. Ou seja, $z \in \bar{y}$, Logo, $\bar{x} \subseteq \bar{y}$.

$\bar{y} \subseteq \bar{x}$**:** Seja $z \in \bar{y}$. Como $y \in \bar{x}$, por definição $x \sim y$. Também, $y \sim z$ e pela transitividade, se $x \sim y$ e $y \sim z$ então $x \sim z$. Ou seja, $z \in \bar{x}$, Logo, $\bar{y} \subseteq \bar{x}$.

Pelos casos acima, temos então que $\bar{x} = \bar{y}$, como queríamos provar. ■

Outras duas propriedades que são consequências importantes de um conjunto X com a relação de equivalência $\sim$ é que X é a união de todas as classes de equivalências, pois como cada elemento pertence a própria classe de equivalência, então todos os elementos do conjunto terão uma classe, e todas as classes formarão o conjunto. E a última propriedade, não menos importante, é que duas classes de equivalência diferentes não possuem elementos em comum. De fato, acabamos de provar que um elemento de uma classe é capaz de gerar toda a classe. Se tivessem pelo menos um elemento em comum, iriam gerar classes iguais e não diferentes.

5.1.1 Inteiros módulo n

Primeiramente, sem perda de generalidade, vamos escolher um inteiro n positivo, que ficará fixo. A partir daqui, analisaremos a congruência módulo n de todos os próximos desenvolvimentos.

Uma das relações de equivalência mais conhecidas no conjunto dos números inteiros, é a *congruência módulo n*. Basicamente, dois inteiros são equivalentes módulo n, quando a sua diferença for um múltiplo de n.

Definição 5.2 (Congruência módulo n)**.** Dois inteiros a e b são

congruentes módulo n se $a - b$ é um múltiplo de n. Escrevemos:

$$a \equiv b \pmod{n}.$$

Alguns exemplos com números deixam a ideia mais clara:

$10 \equiv 4 \pmod 3$, pois, $10 - 4 = 6$ que é múltiplo de 3
$14 \equiv 5 \pmod 3$, pois $14 - 5 = 9$ que é múltiplo de 3
$4 \equiv 7 \pmod 3$, pois $4 - 7 = -3$ que é múltiplo de 3.

Um dos casos especiais acontecem quando $n = 0$. Se $n = 0$ o único múltiplo de zero é o próprio zero. Portanto, para qualquer inteiro a e b, $a \equiv b \pmod 0$ é verdadeira quando $a = b$.

O outro caso especial, é quando $n = 1$. Por definição, todo número é múltiplo de 1, portanto, para quaisquer valor de a e b, $a \equiv b \pmod 1$ é válido.

Teorema 5.2. *Congruência módulo n é uma relação de equivalência.*

Demonstração. Queremos provar que a congruência módulo n é uma relação de equivalência. Para isso, precisamos mostrar que a congruência satisfaz a (1) reflexividade, (2) simetria e (3) transitividade. Vamos provar (1). Para isso, consideremos a um inteiro, se $a \equiv a \pmod n$. Por definição $a - a = 0$ é múltiplo de qualquer número inteiro, provando (1). Para provar (2), temos que se $a \equiv b \pmod n$. Então por definição $a - b$ é múltiplo de n. Mas $b - a = -(a - b)$, logo $b - a$ também é múltiplo de n. Ou seja, $b \equiv a \pmod n$, provando (2). Por fim, para provar (3), vamos supôr que $a \equiv b \pmod n$ e $b \equiv c \pmod n$, onde a, b, c são inteiros quaisquer. Da primeira congruência, temos que $a - b$ é múltiplo de n, e da segunda congruência, temos que $b - c$ é múltiplo de n. Se somarmos múltiplos de n, teremos um múltiplo de n, então:

$$(a - b) + (b - c) = a - b + b - c = a - c$$

é múltiplo de n, assim $a \equiv c \pmod{n}$.

Portanto, verificamos as três propriedades e concluímos que a congruência módulo n é uma relação de equivalência.

■

O conjunto que realmente vai nos interessar é o *conjunto dos inteiros módulo n*, denotado por $\mathbb{Z}_n$, $n > 1$.

Note que se $a \in \mathbb{Z}$, a classe de a será formada pelos $b \in \mathbb{Z}$ de modo que $b - a$ seja múltiplo de n. Em outras palavras, $b - a = k \cdot n$, para algum $k \in \mathbb{Z}$, ou seja:

$$\bar{a} = \{a + k \cdot n : k \in \mathbb{Z}\}.$$

Ora, se a é um inteiro qualquer, podemos dividi-lo por n, então

$$a = n \cdot q + r \text{ e } 0 \leq r \leq n - 1.$$

Assim, $a - r = n \cdot q$ é um múltiplo de n.

Proposição 5.3. *Um inteiro a qualquer é congruente módulo n ao resto da divisão r que vai de* 0 *a* $n - 1$.

$$a \equiv r \ (mod\ n).$$

Exemplo 5.1.1.

$$210 \equiv 2 \pmod{8}$$

$$210 = 26 \cdot 8 + 2$$

Em outras palavras, as classes $\bar{a}$ podem sempre ser tomadas com $0 \leq a \leq n - 1$. Assim,

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

Um jeito diferente de entender $\mathbb{Z}_n$ é: imagine uma folha e nela desenhada uma reta numérica horizontal, com números equidistantes. Agora, enrole o papel de modo a criar um círculo em que n fique em cima do 0. Como a reta é infinita, vamos enrolando mais vezes o papel. O que notaremos é que os pontos onde as coordenadas são múltiplos n estarão coincidindo no ponto zero, e em cada um dos outros pontos, estarão outros pontos que formarão as classes de equivalência, alguns exemplos são: $\mathbb{Z}_2, \mathbb{Z}_3$....

5.2 ARITMÉTICA MODULAR

Para entender como a operação soma é feita no $\mathbb{Z}_n$ vamos imaginar um relógio, que tem marcações de $\overline{0}$ até $\overline{n-1}$. Para realizar a soma de duas classes $\overline{a}$ e $\overline{b}$, colocamos o ponteiro no $\overline{a}$ e andamos $\overline{b}$ marcações no sentido horário.

Por exemplo, em $\mathbb{Z}_7$ vamos somar $\overline{5} + \overline{4}$. Colocamos o ponteiro no $\overline{5}$ e andamos $\overline{4}$ marcações no sentido horário. Repare que se movermos somente duas casas das $\overline{4}$, estamos no $\overline{0}$. Daí, andamos o restante das duas e estamos na casa $\overline{2}$. Assim $\overline{5} + \overline{4} = \overline{2}$.

Definição 5.3. Sejam $\overline{a}$ e $\overline{b}$ classes de equivalência de $\mathbb{Z}_n$ então,

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Vamos voltar e analisar o exemplo utilizado acima, conforme mostra a definição. Para somarmos $\overline{5}$ a $\overline{4}$, temos que somar os números inteiros 4 e 5. Assim $\overline{5} + \overline{4} = \overline{9}$. Opa, no exemplo anterior utilizando o relógio como forma de contagem, chegamos ao resultado $\overline{2}$ e utilizando a definição chegamos em $\overline{9}$. Como $9 = 7 \cdot 1 + 2$, então $9 \equiv 2 \pmod 7$. Ou seja, $\overline{9} = \overline{2}$.

Esse exemplo nos mostra uma coisa muito importante. Pela Definição 5.3 estamos somando classes que são subconjuntos de $\mathbb{Z}$, mas estamos utilizando elementos do subconjunto. Precisamos garantir que independente do elemento que escolhermos de cada subconjunto o resultado tem que ser o mesmo.

Voltemos ao exemplo anterior. Somamos $\bar{5}$ com $\bar{4}$ em $\mathbb{Z}_{\not 9}$, utilizando os elementos 5 da primeira classe e 4 da segunda classe. Sabemos que as seguintes igualdades são verdadeiras, $\bar{5} = \bar{12}$ e $\bar{4} = \bar{18}$. Assim, se somarmos as classes do 12 e do 18, temos que chegar em $\bar{2}$. De fato, $\bar{12} + \bar{18} = \bar{30}$, como $\bar{30} - \bar{2} = \bar{28}$ e é múltiplo de 7, então $\bar{28} = \bar{2}$.

Proposição 5.4. *Qualquer que sejam os representantes escolhidos para efetuar a soma de duas classes o resultado é a mesma classe de equivalência.*

Demonstração. Vamos supor que $\bar{a} = \bar{a'}$ e que $\bar{b} = \bar{b'}$, se $\bar{a} = \bar{a'}$ é equivalente dizermos que $a - a'$ é múltiplo de n, e do mesmo modo que $b - b'$ é múltiplo de n. Se somarmos os dois múltiplos, temos

$$(a - a') + (b - b') = (a + b) - (a' + b').$$

que também é múltiplo de n. Portanto, $\overline{a + b} = \overline{a' + b'}$, como queríamos demonstrar.

■

Vamos definir a diferença de classes mas não vamos mostrar que ela está bem definida, pois é muito análoga a soma de classes.

Definição 5.4. Sejam $\bar{a}$ e $\bar{b} \in \mathbb{Z}_n$, então $\bar{a} - \bar{b} = \overline{a - b}$.

Definição 5.5. Sejam $\bar{a}$ e $\bar{b} \in \mathbb{Z}_n$, então $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Do mesmo modo, vamos provar que independente dos representantes escolhidos, o produto das classes tem que ser a mesma.

Proposição 5.5. *Qualquer que sejam os representantes escolhidos para efetuar o produto de duas classes de equivalência, o resultado é a mesma classe de equivalência.*

Demonstração. Vamos supor que $\bar{a} = \bar{a'}$ e que $\bar{b} = \bar{b'}$. Como $\bar{a} = \bar{a'}$, temos que $a - a'$ é múltiplo de n, ou seja, $a = a' + r \cdot n$ para algum inteiro r, do mesmo modo se $\bar{b} = \bar{b'}$. Então, $b - b'$ é múltiplo de n, ou seja, $b = b' + s \cdot n$ para algum inteiro s. Multiplicando o que obtemos:

$$\begin{aligned} a \cdot b &= (a' + r \cdot n) \cdot (b' + s \cdot n) \\ &= a'b' + a' \cdot s \cdot n + b' \cdot r \cdot n + r \cdot s \cdot n^2 \\ &= a' \cdot b' + (a' \cdot s + b \cdot r + r \cdot s \cdot n) \cdot n \\ \Rightarrow a \cdot b - a' \cdot b' &= (a' \cdot s + b \cdot r + r \cdot s \cdot n) \cdot n. \end{aligned}$$

Logo, $a \cdot b - a' \cdot b'$ é múltiplo de n. Portanto, $\overline{a \cdot b} = \overline{a' \cdot b'}$.

■

Agora sabemos somar, subtrair e multiplicar classes de equivalência em $\mathbb{Z}_n$ e é perceptível o quanto se assemelha às operações em $\mathbb{Z}$. Além disso, se considerarmos $\bar{a}$, $\bar{b}$ e $\bar{c}$ em $\mathbb{Z}_n$, temos as seguintes propriedades para a adição e multiplicação:

$$\begin{aligned} (\bar{a} + \bar{b}) + \bar{c} &= \bar{a} + (\bar{b} + \bar{c}) \\ \bar{a} + \bar{b} &= \bar{b} + \bar{a} \\ \bar{a} + \bar{0} &= \bar{a} \\ \bar{a} + \overline{(-a)} &= \bar{0} \\ (\bar{a} \cdot \bar{b}) \cdot \bar{c} &= \bar{a} \cdot (\bar{b} \cdot \bar{c}) \\ \bar{a} \cdot \bar{b} &= \bar{b} \cdot \bar{a} \\ \bar{a} \cdot \bar{1} &= \bar{a} \\ \bar{a} \cdot (\bar{b} + \bar{c}) &= \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} \end{aligned}$$

Quando falamos de divisão no $\mathbb{Z}_n$, em vez de considerarmos a divisão como conhecemos para $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, vamos utilizar a ideia de "multiplicar pelo inverso". O que é equivalente dizer que estamos dividindo a por b. Para isso, precisamos provar que existe inverso em $\mathbb{Z}_n$.

Teorema 5.6. *A classe $\bar{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$ se, e somente se, a e n são primos entre si.*

Demonstração. Queremos provar basicamente, que dada uma classe de equivalência, conseguimos encontrar uma classe inversa. Primeiramente, tome uma classe $\bar{a} \neq \bar{0}$ tal que existe $\bar{h}$, de modo que $\bar{a} \cdot \bar{h} = \bar{1}$ em $\mathbb{Z}_n$.

Por hipótese, temos que $\bar{a} \cdot \bar{h} = \bar{1}$, subtraindo $\bar{1}$ em ambos os lados temos $\bar{a} \cdot \bar{h} - \bar{1} = \bar{1} - \bar{1} \Rightarrow \bar{a} \cdot \bar{h} - \bar{1} = \bar{0}$. Logo, $\bar{a} \cdot \bar{h} - \bar{1}$ é múltiplo de n. Ou seja, $a \cdot h + k \cdot n = 1$ para algum inteiro k. Pelo Teorema 3.4, temos que $mdc(a, n) = 1$. Assim, se $\bar{a}$ possui inverso em $\mathbb{Z}_n$ então o $mdc(a, n) = 1$.

Para provar a recíproca, temos por hipótese que o $mdc(a, n) = 1$ e queremos provar que $\bar{a}$ tem inverso em $\mathbb{Z}_n$. Ou seja, existe um $\bar{h}$ tal que $\bar{a} \cdot \bar{h} = \bar{1}$. Portanto, por Bezóut novamente, existe s e h inteiros, de modo que $a \cdot h + n \cdot s = 1$. Logo, $\bar{a} \cdot \bar{h} = \bar{1}$, para todo $\bar{a} \in \mathbb{Z}_n$.

■

Além disso, podemos notar que se n for um número primo p, então $mdc(a, p) = 1$, para todo $\bar{a} \in \mathbb{Z}_n - \{\bar{0}\}$, Logo, quando n é primo, todas as classes que são diferentes de $\bar{0}$ possuem inverso.

Quando calculamos os restos da divisão de uma potência por um número qualquer, basicamente estamos aplicando o estudo da congruência. Por exemplo, vamos calcular o resto da divisão de 3^{64} por 31. A primeira potência de 3 que é cônguo módulo 31 é $3^3 \equiv -4 (\text{mod } 31)$. Dividindo o 64 por 3, temos $64 = 3 \cdot 21 + 1$. Assim, conseguimos as seguintes congruências,

$$3^{64} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv -(2)^{42} \cdot 3.$$

Outra congruência módulo 31 que temos, é $2^5 \equiv 1 (\text{mod } 31)$. Substituindo na congruência anterior o fato de que $42 = 8 \cdot 5 + 2$, temos

$$3^{64} \equiv -(2)^{42} \cdot 3 \equiv -(2^5)^8 \cdot 2^2 \cdot 3 \equiv -12.$$

E como $-12 \equiv 19 (\text{mod } 31)$, logo, o resto da divisão de 3^{64} por 31 é 19.

Proposição 5.7. *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$.*

Demonstração. Utilizaremos o método da demonstração por indução. Para isso, veremos primeiro se para o menor valor de n a afirmação é verdade. Então, dado $n = 1$, temos $a^1 \equiv b^1 \pmod{m}$. Por hipótese, isso é verdade. Vamos supor agora que $a^n \equiv b^n \pmod{m}$. Temos que provar que vale para $a^{n+1} \equiv b^{n+1} \pmod{m}$.
Por hipótese de indução, temos que $a^n \equiv b^n \pmod{m}$. Por hipótese temos também que $a \equiv b \pmod{m}$. Então, multiplicando por a a primeira congruência e por b a segunda congruência da hipótese ficando com,

$$\begin{aligned} a^n \equiv b^n \pmod{m} &\Rightarrow a^n \cdot a \equiv b^n \cdot b \pmod{m} \\ &\Rightarrow a^{n+1} \equiv b^{n+1} \pmod{m}. \end{aligned}$$

Como queríamos provar.

■

6 CRIPTOGRAFIA RSA

Chegamos então, no capítulo que vamos entender como funciona a criptografia RSA. Mas, antes de finalmente entender, precisamos ver em mais detalhes como funciona a segurança do RSA. Ou seja, o porquê de ser difícil a quebra de uma mensagem que está criptografada com o RSA.

Leonhard Euler ao longo de sua vida, contribuiu para diversas áreas do conhecimento. Euler definiu uma função importante e muito utilizada na Criptografia. Essa função, é conhecida como *Função ϕ de Euler* ou *Função Totiente de Euler*, que associa a cada inteiro positivo n a quantidade de inteiros positivos menores do que n que são coprimos (primos entre si) com n. Utilizaremos muito essa função nesse capítulo.

Proposição 6.1. *Seja p um número primo, então todos os inteiros positivos menores que p são primos com p. Logo,*

$$\phi(p) = p - 1.$$

Teorema 6.2. *Se p, q são inteiros positivos tais que mdc(p,q) = 1, então*

$$\phi(pq) = \phi(p) \cdot \phi(q).$$

É possível encontrar as demonstrações em [2] (página 141). Basicamente vamos utilizar o fato de que, como $n = p \cdot q$ e p e q são primos entre si, então $\phi(n) = (p-1) \cdot (q-1)$.

6.1 PRÉ-CODIFICAÇÃO

O primeiro passo a ser executado para que possamos utilizar o RSA é converter as letras em números. Ou seja, converter uma frase, em uma sequência de números. Sem perda de generalidade, vamos escolher uma frase que contenha apenas palavras: “Do tamanho

do céu". Utilizaremos a seguinte tabela para converter a frase:

A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19

K	L	M	N	O	P	Q	R	S	T
20	21	22	23	24	25	26	27	28	29

U	V	W	X	Y	Z
30	31	32	33	34	35

Para o espaço entre as palavras, vamos utilizar o número 99. Um questionamento que pode aparecer é por que não começar do 1. Exemplo: A = 1, B = 2. Justamente, pra não causar ambiguidade. Por exemplos, vamos pré-codificar a palavra ABALAR. Utilizando uma tabela em que A=1, B=2 e assim por diante, teríamos 12112118. Se não conhecermos a palavra, quem nos garante que os dois primeiros dígitos 12 não correspondem a letra L, em vez de A e B. Assim, escolher números de um algarismo traz esse tipo de interpretação equivocada.

Convertendo então a mensagem utilizando a tabela acima, temos:

$$1324992910221023172499132499121430.$$

A última parte da pré-codificação é separar em blocos o número que obtivemos convertendo a frase. Vamos fazer todos os blocos tendo valor menor a n. Podemos obter os seguintes blocos:

$$1 - 32 - 49 - 9 - 29 - 10 - 2 - 2 - 10 - 2 - 31 - 7 - 2 - 49 - 9 - 1 - 32 - 49 - 9 - 1 - 21 - 4 - 30.$$

A maneira que escolhemos os blocos não é única. Somente alguns cuidados devem ser tomados, como: evitar dividir em blocos onde o valor inicial é 0 (zero). Também devemos evitar quebrar os blocos exatamente em sílabas e letras, pois a decodificação por frequência, pode ser suficiente para decodificar a mensagem.

6.2 CODIFICANDO

Para a próxima etapa, a de codificação, precisamos de n que será o produto de dois primos p e q. E de um número e que seja inversível módulo $\phi(n)$. Ou seja, com $mdc(e, \phi(n)) = 1$. Como sabemos quem são os primos p e q, fica fácil descobrir $\phi(n)$.

Considere $p = 5$ e $q = 11$. Daí, basta fazer $\phi(n) = (p-1) \cdot (q-1)$, que no nosso exemplo é, $\phi(55) = (5-1) \cdot (11-1) \Rightarrow \phi(55) = 4 \cdot 10 \Rightarrow \phi(55) = 40$.

Assim, nossa *chave de codificação* será o par (n, e). O próximo passo é codificar cada bloco separadamente. E a mensagem então codificada, será a sequência de blocos codificados. Uma coisa a ressaltar é que depois de codificados, os blocos não poderão ser juntados a fim de formar um novo número maior. Se isso acontecer, jamais conseguiremos decodificar a mensagem.

Vamos denotar cada bloco codificado por $C(b)$, onde b é o bloco, que é um inteiro positivo menor que n. Assim, para codificar utilizaremos o seguinte:

$$C(b) = \text{resto da divisão de } b^e \text{ por n.}$$

Em outras palavras $C(b) \equiv b^e (\text{mod } n)$. No nosso exemplo, $n = 55$ e o menor valor para e é 3, pois é o menor inteiro primo que não divide $\phi(55) = 40$. Assim, se pegarmos o primeiro bloco 1, para codificá-lo, precisamos encontrar o resto da divisão de 1^3 por 55. Assim, $C(1) = 1$. Codificando todos os blocos da nossa mensagem temos:

b^e	**C(b)**
$1^3 = 1$	1
$32^3 = 32768$	43
$49^3 = 117649$	4
$9^3 = 729$	14
$29^3 = 24389$	24
$10^3 = 1000$	10
$2^3 = 8$	8
$2^3 = 8$	8
$10^3 = 1000$	10
$2^3 = 8$	8
$31^3 = 29791$	36
$7^3 = 343$	13
$2^3 = 8$	8
$49^3 = 117649$	4
$9^3 = 729$	14
$1^3 = 1$	1
$32^3 = 32768$	43
$49^3 = 117649$	4
$9^3 = 729$	14
$1^3 = 1$	1
$21^3 = 9261$	21
$4^3 = 64$	9
$30^3 = 27000$	50

Assim, nossa mensagem foi codificada pela criptografia RSA, nos seguintes blocos:

1 - 43 - 4 - 14 - 24 - 10 - 8 - 8 - 10 - 8 - 36 - 13 - 8 - 4 - 14 - 1 - 43 - 4 - 14 - 1 - 21 - 9 - 50.

6.3 DECODIFICANDO

Para decodificar um bloco de mensagens codificadas, precisamos de duas informações básicas. n e o inverso de e módulo $\phi(n)$, que vamos chamar de d. Assim, a nossa *chave de decodificação* é o

par (n, d). Assim como denominamos os blocos de codificação por $C(b)$, vamos chamar de $D(a)$ os blocos de decodificação, onde a são os blocos codificados. Para decodificar, temos que realizar a seguinte operação:

$$D(a) = \text{resto da divisão de } a^d \text{ por } n.$$

Do mesmo modo, em outras palavras, se tratando de aritmética modular, podemos entender $D(a)$ como a^d módulo n. Se conhecermos o valor de e e de $\phi(n)$, encontramos de imediato o valor de d.

De outra forma, se codificamos um bloco b, quando decodificarmos o bloco de mensagem codificada, esperamos encontrar o bloco b, que corresponde a mensagem original.

Para encontrar d, vamos utilizar o algoritmo de Euclides, e realizar algumas divisões. No nosso exemplo, temos que $n = 55$ e que $e = 3$, dividindo $\phi(55) = 40$ por 3, temos:

$$\begin{array}{r|l} 40 & 3 \\ \cline{2-2} -\,3 & 13 \\ \cline{1-1} 10 & \\ -\;\;9 & \\ \cline{1-1} 1 & \end{array}$$

Nesse caso, na primeira divisão, já obtemos o resto 1. De outra forma, podemos escrever essa divisão como:

$$40 = 13 \cdot 3 + 1.$$

Isolando o resto 1, ficamos com:

$$40 - 13 \cdot 3 = 1.$$

Portanto, o inverso de 3 módulo 40 é -13. Porém, precisamos trabalhar com d positivo. Então, $d = 40 - 13 = 27$, que nada mais é do que o primeiro inteiro positivo, que é congruente ao -13 no módulo 40.

Logo, para decodificar toda a mensagem, temos que pegar cada bloco codificado a, elevar por 27, e encontrar o resto da divisão por 55. No nosso exemplo:

a^d	**D(a)**
1^{27}	1
43^{27}	32
4^{27}	49
14^{27}	9
24^{27}	29
10^{27}	10
8^{27}	2
8^{27}	2
10^{27}	10
8^{27}	2
36^{27}	31

13^{27}	7
8^{27}	2
4^{27}	49
14^{27}	9
1^{27}	1
43^{27}	32
4^{27}	49
14^{27}	9
1^{27}	1
21^{27}	21
9^{27}	4
50^{27}	30

Nesse exemplo, os cálculos já ultrapassaram lápis e papel. Então, foram desenvolvidos no programa MATLAB. Mas, foi possível verificar que realmente, quando decodificado um bloco a, voltamos a ter o bloco b de início. Decodificando assim, a mensagem codificada.

6.4 POR QUE A CRIPTOGRAFIA RSA FUNCIONA?

Vimos que para funcionar, temos que decodificar um bloco codificado e deve voltar ao bloco que corresponde à mensagem original. Em outras palavras, vamos considerar novamente um bloco b. Ou seja, um bloco que ainda não foi codificado. Assim, quando codificarmos, teremos $C(b)$. Agora, quando decodificarmos, teremos $D(C(b))$, que terá que ser b.

Para isso, precisamos provar que se b é um inteiro maior ou igual a 1 e menor igual que $n-1$, então $D(C(b)) \equiv b \pmod{n}$. Como $D(C(b)) < n$, pois os blocos codificados precisavam ser menor que n, basta mostrar que $D(C(b)) = b$. Esse é um dos motivos do valor de b ser menor que n e porque devemos manter os blocos separados

depois da codificação.

Assim, por definição $D(a) \equiv a^d (\text{mod } n)$ e $C(b) \equiv b^e (\text{mod } n)$. Elevando ambos os lados da segunda congruência por d, então:

$$C(b) \equiv b^e (\text{mod } n) \Rightarrow [C(b)]^d \equiv (b^e)^d (\text{mod } n) \Rightarrow D(C(b)) \equiv b^{ed} (\text{mod } n).$$

Porém d é o inverso multiplicativo de e (mod $\phi(n)$), logo

$$e \cdot d = 1 + k \cdot \phi(n) \tag{6.1}$$

para algum inteiro k. Como e e d são inteiros maiores que 2 e $\phi(n)$ é obrigatoriamente maior que 0, então k também será maior que zero. Então, vamos substituir $e \cdot d$ em (6.1). Assim, ficamos com:

$$b^{ed} \equiv b^{1+k\cdot\phi(n)} \equiv b \cdot (b^{\phi(n)})^k \ (\text{mod } n)$$

Sabemos que $n = p \cdot q$, onde p e q são primos distintos. Vamos então, encontrar a forma reduzida de b^{ed} (mod p) e b^{ed} (mod q). Vimos anteriormente que $\phi(n) = (p-1) \cdot (q-1)$, substituindo isso em (6.1) ficamos com:

$$e \cdot d = 1 + k \cdot (p-1) \cdot (q-1)$$

Substituindo a nova forma de $e \cdot d$

$$b^{ed} \equiv b^{1+k\cdot\phi(n)} \equiv b \cdot (b^{\phi(n)})^k \equiv b \cdot (b^{p-1})^{k\cdot(q-1)}$$

Isso tudo, côngruo módulo p.

Para prosseguir com a prova, vamos ter que supor que b e p são primos entre si, assim, pelo pequeno Teorema de Fermat - demonstração é facilmente encontrada na página 41 de [6] - temos que $b^{p-1} \equiv 1$ (mod p)e, daí,

$$b^{ed} \equiv b \cdot (b^{p-1})^{k\cdot(q-1)} \equiv b \cdot 1^{k\cdot(q-1)} \equiv b$$

Portanto, $b^{ed} \equiv b$ (mod p).

Agora, se p divide b, e p é obrigatoriamente primo, então $b \equiv 0$ (mod p). Para qualquer valor de b, elevamos então ambos os lados da equivalência a ed, e temos que,

$$(b)^{ed} \equiv (0)^{ed} \Rightarrow (b)^{ed} \equiv 0 \pmod{p}$$

De maneira muito análoga, conseguimos demonstrar que para qualquer valor de q, $b^{ed} \equiv b \pmod{q}$. Em outras palavras, $b^{ed} - b$ é divisível por p e por q, como p e q são primos distintos. Ou seja, $mdc(p, q) = 1$. Pelo Lema 3.6, como p e q dividem $b^{ed} - b$, então o produto deles dividirá $b^{ed} - b$, então n divide $b^{ed} - b$. Ou seja, $b^{ed} \equiv b \pmod{n}$, para qualquer inteiro b. Como queríamos provar.

6.5 POR QUE A SEGURANÇA RSA É CONFIÁVEL?

Sabemos que a Criptografia RSA é uma chave pública, e que nossos parâmetros são p e q e que $n = p \cdot q$. O par (n, e) é a chave de codificação e é acessível a qualquer pessoa. Sabemos que a Criptografia só vai ser segura, se for difícil encontrar d.

Vimos anteriormente, que para calcular d basta utilizar sucessivas vezes o algoritmo de Euclides. Ou seja, basta pegar $\phi(n)$ e dividir por e até encontrar resto igual a 1 . Mas, não seria tão fácil, só sabemos quem é $\phi(n)$ se soubermos fatorar n para encontrar p e q. Na teoria tudo parece tranquilo, mas na prática, sabemos que só conseguimos fatorar n, se ele for um número pequeno.

Mas, vamos supor que alguém tenha inventado uma maneira de encontrar d através dos elementos da chave de codificação. Mais ainda, através de $\phi(n)$. Então, basicamente, alguém inventou uma maneira de fatorar esse número, pois, nesse caso $\phi(n) = (p-1)\cdot(q-1)$ e $n = p \cdot q$ seriam as peças conhecidas. Mas,

$$\phi(n) = (p-1) \cdot (q-1) = p \cdot q - (p+q) + 1 = n - (p+q) + 1 \Rightarrow$$
$$p + q = n - \phi(n) + 1$$

O que fizemos foi, basicamente resolver a fatoração com a propriedade distributiva, e depois substituir $p \cdot q$ por n. E por fim, isolar $p + q$. Porém,

$$(p+q)^2 - 4 \cdot n = (p^2 + q^2 + 2p \cdot q) - 4p \cdot q = (p-q)^2$$

Tirando a raíz de ambos os lados, ficamos com:

$$\sqrt{(p+q)^2 - 4 \cdot n} = \sqrt{(p-q)^2} \Rightarrow |p-q| = \sqrt{(p+q)^2 - 4 \cdot n}$$

que também é conhecido. Ora, conhecendo $p+q$ e $p-q$ conseguimos encontrar com facilidade p e q. Ou seja, fatoramos n.

7 CONSIDERAÇÕES FINAIS

Vimos nesse trabalho, que a Criptografia RSA não tem nada de muito complexo. Qualquer pessoa, que tenha o mínimo conhecimento dos assuntos fundamentais da Álgebra, entende como ela funciona e porque ela funciona. A utilização ainda, dos números primos, mostra o quanto eles, desde a antiguidade despertam o interesse e curiosidade de matemáticos e cientistas.

A Criptografia RSA está no dia a dia de todos nós há 41 anos, e até o presente momento, ninguém conseguiu ao menos chegar perto de tentar quebrá-la. Apesar de ninguém ter conseguido até agora, muitas outras Criptografias que utilizam outros parâmetros estão sendo desenvolvidas, como a criptografia multivariada e a criptografia pós-quântica.

REFERÊNCIAS

[1] *Bézout e Outros Bizus*. OBM. URL: http://www.obm.org.br/content/uploads/2017/01/bezout_e_outros_bizus.pdf.

[2] S.C Coutinho. *Números Inteiros e Criptografia RSA*. 1ª ed. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2014, p. 226.

[3] Euclides. *Os Elementos*. 1ª ed. São Paulo: UNESP, 2009, p. 600.

[4] Adilson Gonçalves. *Introdução à Álgebra*. 5ª ed. Projeto Euclides. Rio de Janeiro: IMPA, 2013, p. 194.

[5] G.H Hardy e E.M Wright. *An introduction to the theory of numbers*. 5ª ed. Oxford: Oxford Science Publications, 1994.

[6] José Plínio de Oliveira Santos. *Introdução à Teoria dos Números*. 1ª ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2000, p. 198.