DALILA PACHECO BERNARDO

APLICAÇÃO DO ALGORITMO DE EUCLIDES PARA O PRIMEIRO GRAU: CONGRUÊNCIA

FLORIANÓPOLIS

1999

Dalila Pacheco Bernardo

Professora de Matemática de 1º e 2º graus

Aplicação do Algoritmo de Euclides para o Primeiro Grau: Congruência

Trabalho de Conclusão de Curso apresentado ao Curso de Matemática - Licenciatura, Departamento de Matemática, Centro de Ciências Física e Matemática, Universidade Federal de Santa Catarina. Orientadora: Professora Jane de Oliveira Crippa .

Florianópolis

1999

200822

Esta Monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** no Curso de Matemática – Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designados pela Portaria nº .../ SCG/ 99.

Profª Carmem Suzane Comitre Gimenez
Professora da disciplina

Banca Examinadora:

Jane de Oliveira Crippa
Orientadora

Antônio Vladimir Martins

Carmem Suzane Comitre Gimenez

TCCFINAL.DOC

Dedico este trabalho
a todos os amigos que
conquistei durante
minha graduação.

AGRADECIMENTOS

Aos meus pais.

À minha orientadora.

Aos meus alunos.

À minha amiga Sônia.

Às Secretárias Sílvia e Iara da Coordenadoria de Matemática.

E a todos que direta ou indiretamente contribuíram para a finalização deste.

SUMÁRIO

INTRODUÇÃO

Este trabalho tem como objetivo principal relatar a experiência vivenciada ao ser aplicado o conteúdo congruência em turmas de 5ª e 6ª séries do primeiro grau do Colégio Estadual Professor José Rodrigues Lopes (Garopaba-SC), sendo que o mesmo está dividido em três etapas.

Primeiramente, mostrou-se alguns aspectos históricos relacionados a congruência e ao algoritmo de Euclides que esta diretamente ligado à primeira.

Em seguida desenvolveu-se alguns tópicos envolvendo congruência, como propriedades, teoremas, proposições, aplicações, etc., a fim de um maior conhecimento sobre o assunto.

Por fim, mostrou-se o procedimento das aulas sobre congruência para os alunos, relatando os resultados obtidos e as dificuldades encontradas.

Desde já ressalta-se que não pretendia-se ensinar detalhadamente nem abranger tudo a respeito de congruência para os alunos, apenas introduzir algo que, de uma maneira geral, caracterizasse congruência e não fugisse do conhecimento que o aluno já possui em relação a outros conteúdos interligados com a mesma.

ASPECTOS HISTÓRICOS

Euclides - Infelizmente muito pouco se sabe sobre a vida e a personalidade de Euclides, apenas que foi ele, segundo parece, o criador da famosa e duradoura escola de matemática de Alexandria da qual, sem dúvida foi professor. Desconhecem-se também a data e o local de seu nascimento, mas é provável que sua formação matemática tenha se dado na escola platônica de Atenas.

Embora Euclides fosse autor de pelo menos dez trabalhos, cinco obras sobreviveram até hoje: Os Elementos, Os Dados, Divisão de figuras, Os Fenômenos e Óptica. Sua fama repousa principalmente sobre seus Elementos. Parece que esse trabalho notável, imediata e completamente superou todos os Elementos precedentes; de fato, nenhum vestígio restou de esforços anteriores, ganhou o mais alto respeito e, dos sucessores de Euclides até os tempos modernos, a mera citação do número de um livro e o de uma proposição de sua obra-prima é suficiente para identificar um Teorema de construção particular.

Contrariamente à impressão muito difundida, os Elementos de Euclides não tratam apenas de geometria. Contém bastante teoria dos números e álgebra elementar (geométrica). Os livros se compõem de 465 proposições distribuídos em treze livros, dos quais os seis primeiros são sobre geometria plana elementar, os três seguintes sobre teoria dos números, o livro X sobre incomensuráveis e os três últimos versam principalmente sobre geometria no espaço.

Os livros VII, VIII e IX, que no total tem 102 (cento e duas) proposições, tratam da teoria elementar dos números. Em todos esses livros cada número é representado por um segmento, de modo que Euclides se refere a um número AB. Por isso Euclides não usa frase como "é um múltiplo de" ou "é um fator de", pois ele as substitui por "é medido por" e "mede respectivamente", isto é, um número **n** é medido por outro número **m** se existe um terceiro número **k** tal que $n = km$. O livro VII começa com o processo, hoje conhecido como algoritmo euclidiano, para achar o máximo divisor comum de dois ou mais números e o usa para verificar se dois números são primos entre si. Encontra-se nele também uma exposição da teoria das proposições numéricas ou pitagóricas. Estabelecem-se ainda nesse

livro muitas propriedades numéricas básicas. Enfim, como descreveu Proclus, Os Elementos em relação ao resto da Matemática são como as letras do alfabeto em relação a linguagem.

O algoritmo de Euclides - O algoritmo euclidiano, processo para se achar o máximo divisor comum (MDC) de dois números inteiros, tem esse nome porque se encontra no início do livro VII dos Elementos de Euclides, embora o processo em si fosse conhecido muito tempo antes. Esse algoritmo se encontra nos fundamentos de vários progressos da matemática moderna. Enunciado em forma de regra, é o seguinte: divida o maior dos dois números inteiros positivos pelo menor e então divida o divisor pelo resto. Continue esse processo de dividir o último divisor pelo resto, até que a divisão seja exata. O divisor final é o MDC procurado.

Gauss - Homem de estofo e talento matemático impressionante, Carl Friedrich Gauss sobressai-se nos séculos XVIII e XIX como um Colosso de Rodes da matemática. Ele é universalmente considerado como o maior matemático do século XIX e, ao lado de Arquimedes e Isaac Newton, como um dos maiores de todos os tempos.

Gauss nasceu em Brunswick, Alemanha em 1777. Seu pai era um trabalhador braçal que tinha uma opinião teimosamente pouco favorável a respeito da educação. Sua mãe porém, ainda que inculta, encorajava-o nos estudos e manteve por toda a vida grande orgulho pelas realizações do filho.

Gauss foi uma das mais notáveis crianças-prodígio. Diz-se que com três anos de idade detectou um erro aritmético no borrador de seu pai. Há uma história segundo a qual o professor de Gauss na escola pública quando ele tinha dez anos de idade, teria passado á classe para mantê-la ocupada, a tarefa de somar números de 1 à 100. Quase que imediatamente Gauss colocou sua lousa sobre a escrivaninha do irritado professor. Quando as lousas foram finalmente viradas, o professor surpreso verificou que Gauss tinha sido o único a acertar a resposta correta, 5050, mas sem fazê-lo acompanhar de nenhum cálculo.

Gauss havia mentalmente calculado a soma da progressão aritmética
$1 + 2 + 3 + ... + 98 + 99 + 100$, observando que $100 + 1 = 101$, $99 + 2 = 101$, $98 + 3 = 101$ e assim por diante com os cinqüenta pares possíveis dessa maneira, sendo a soma portanto $50 \times 101 = 5050$. Mais tarde, quando adulto, Gauss costumava comentar de ter aprendido a contar antes de aprender a falar.

A publicação unitária mais importante de Gauss é a sua Disquisitiones Arithmetical, um trabalho de importância fundamental na moderna teoria dos números. As descobertas de Gauss sobre construções de polígonos regulares aparecem nesse trabalho, assim como sua fácil notação para congruência e uma demonstração da bela lei da reciprocidade quadrada.
Em 1801, Gauss introduziu o conceito e a notação de congruência em sua Disquisitiones Arithmetical. A exposição começa com a definição: se um número **"a"** divide a diferença entre dois números **"b"** e **"c"** então **"b"** e **"c"** dizem-se congruentes , de outra forma incongruentes; e **"a"** chama-se o módulo. Qualquer dos números diz-se um resíduo do outro, no primeiro caso e um não - resíduo no segundo caso.

A notação que Gauss adotou foi a que se usa hoje : $\mathbf{b \equiv c \pmod{a}}$, e ele passou a construir uma álgebra para a relação denotada por ≡ semelhante à familiar álgebra comum expressa na linguagem de igualdade.

Gauss também deu contribuições notáveis à Astronomia, Geodesia, Cristalografia, Magnetismo e Eletricidade.

É famosa a afirmação de Gauss de que a Matemática é a rainha das ciências e a teoria dos números é a rainha da matemática.

Gauss morreu em sua casa no observatório de Gottingen em 23 de fevereiro de 1855 e logo depois o rei de Hanover ordenou que se preparasse uma medalha comemorativa em sua homenagem. Nela figura a inscrição "Jorge V rei de Hanover ao Príncipe Matemático". Desde então Gauss é conhecido como o príncipe matemático.

CONGRUÊNCIA

Definição: Seja **m** um número inteiro positivo fixo. Para inteiros arbitrários **x** e **y** dizemos que **x** é côngruo a **y**, módulo **m**, se **m** divide **x - y**.

Notação: $x \equiv y \pmod{m}$. Isto significa dizer que existe um inteiro **q** tal que $x - y = qm$ ou $x = y + qm$. Assim, para todo inteiro **x**, o algoritmo de Euclides (algoritmo da divisão) garante a existência de inteiros **q** e **r** tais que $x = qm + r$, $0 \leq r < m$. Com isto podemos concluir que fixado um inteiro **m** positivo, teremos que qualquer inteiro **x** será côngruo a um único inteiro **r** com $0 \leq r < m$. Vejamos a seguir o algoritmo de Euclides:

Para quaisquer $a, b \in N$, $b \neq 0$ existe um único par de números **q** e **r** de maneira que $a = bq + r$ onde $r = 0$ ou $r < b$.

Os elementos **a, b, q** e **r** são chamados respectivamente, dividendo , divisor, quociente e resto da divisão de **a** por **b**.

Prova:

Sabemos que **b** é um número natural não nulo. Se $a \in N$, então **a** é múltiplo de **b**, ou $a < b$, ou **a** está entre dois múltiplos consecutivos de **b**, isto é, $bq \leq a < b(q + 1)$.Quando **a** é múltiplo de **b**, temos que existe um natural **q** tal que $a = bq$, portanto $r = 0$ .No caso em que $a < b$ então $q = 0$ e $r = a$ onde $r < b$. No caso em que $bq \leq a < b(q + 1)$, $q + 1$ é o mínimo do conjunto $\{n \in N / bn > a\}$, que é não vazio , pois contém o elemento $a + 1$. De fato, como $b \geq 1$ então multiplicando "a" em ambos os lados da igualdade temos $ab \geq a$ e somando **b** em ambos os lados da igualdade temos $ab + b \geq a + b$, o que resulta em $b(a + 1) \geq a + b > a$.

De $bq \leq a$ resulta que existe $r \in N$ tal que $a = bq + r$. Mostremos que $r < b$. Se $r = a - bq \geq b$ então somando bq em ambos os lados da igualdade temos $(a - bq) + bq \geq b + bq$ e daí $a \geq b(1 + q)$ o que não é possível pois $bq \leq a < b(q + 1)$.

Assim $a = bq + r$ $(r < b)$.

Agora provaremos que **r** e **q** são únicos: se $r = 0$ então **a** é múltiplo de **b**. Suponhamos $a = bq + r = bq_1 + r_1$ onde $r < b$ e $r_1 < b$.

Admitamos que se pudesse ter $r \neq r_1$ digamos $0 < r - r_1 < b$. Mas então da igualdade $bq + r = bq_1 + r_1$ decorre que $bq + (r - r_1) = bq_1$ e portanto b divide $r - r_1$, já que se b divide a soma e uma das parcelas, então b divide a outra parcela. Assim $b \leq r - r_1$, o que é absurdo pois $0 < r - r_1 < b$. Logo $r = r_1$ e portanto $q = q_1$.

Propriedades da Congruência:

1) Para todo $m > 0$, a relação $\equiv$ é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência.

1a) **Reflexiva**: Para todo $x \in Z$ temos que $x \equiv x \pmod m$.

Prova:

Temos que $x - x = 0$ e sabemos que m divide **zero**. Logo $x \equiv x \pmod m$.

1b) **Simétrica:** Se $x \equiv y \pmod m$ então $y \equiv x \pmod m$.

Prova:

Por hipótese m divide $x - y$.

Portanto existe $q \in Z$ tal que $x - y = qm$.

Multiplicando a igualdade $x - y = qm$ por -1, obteremos: $-x + y = -qm$, ou seja

$y - x = (-q)m$.

Portanto m divide $y - x$.

Logo $y \equiv x \pmod m$.

1c) **Transitiva:** Se $x \equiv y \pmod m$ e $y \equiv z \pmod m$ então $x \equiv z \pmod m$.

Prova:

Por hipótese m divide $x - y$ e m divide $y - z$.

Assim existe q e $t \in Z$ tal que $x - y = qm$ e $y - z = tm$, ou seja, $x = qm + y$ (1) e $y = tm + z$ (2).

Substituindo (2) em (1) temos:

$x = qm + tm + z$, consequentemente $x - z = (q + t)\,m$.

Portanto m divide $x - z$.

Logo $x \equiv z \pmod m$.

2) Para quaisquer $x, y \in \mathbf{Z}$, $x \equiv y \pmod m$ se, e somente se, x e y fornecem o mesmo resto na divisão euclidiana por m.

Prova:

$\Rightarrow$ Por hipótese m divide $x - y$, ou seja, existe $q \in \mathbf{Z}$ tal que $x = qm + y$. Aplicando o algoritmo de Euclides para y e m obtemos:

$y = km + r$ onde k e $r \in \mathbf{Z}$ e $0 \leq r < m$.

Então $x = qm + km + r$ e

$x = (q + k)\,m + r$

Como $0 \leq r < m$, r também é o resto da divisão de x por m.

$\Leftarrow$ Se $x = qm + r$ e $y = km + r$ com $0 \leq r < m$,

então $x - y = qm + r - (km + r)$ e

$x - y = qm + r - km - r$

$x - y = (q - k)\,m$

Portanto m divide $x - y$.

Logo $x \equiv y \pmod m$.

3) Se $x \equiv y \pmod m$ então $x + z \equiv y + z \pmod m$ e $xz \equiv yz \pmod m$, para todo $z \in \mathbf{Z}$.

3a) Se $x \equiv y \pmod m$ então $x + z \equiv y + z \pmod m$

Prova:

Por hipótese m divide $x - y$, ou seja, existe $q \in \mathbf{Z}$ tal que $x = qm + y$.

Somando-se z em ambos os lados da igualdade, temos:

$x + z \equiv qm + y + z$, ou seja, $(x + z) - (y + z) = qm$

Portanto m divide $(x + z) - (y + z)$.

Logo $x + z \equiv y + z \pmod m$.

De maneira análoga prova-se que $x - y \equiv y - z \pmod m$.

3b) Se $x \equiv y \pmod m$ então $xz \equiv yz \pmod m$

Prova:

Por hipótese m divide $x - y$, ou seja, existe $q \in Z$ tal que $x - y = qm$.

Multiplicando-se z em ambos os lados da igualdade temos:

$(x - y)z = qmz$ ou $xz - yz = (qz)m$, o que implica que m divide $xz - yz$,

isto é $xz \equiv yz \pmod m$.

4) Se $x \equiv y \pmod m$ e $p \equiv r \pmod m$, então $x + p \equiv y + r \pmod m$ e $xp \equiv yr \pmod m$.

4a) Se $x \equiv y \pmod m$ e $p \equiv r \pmod m$ então $x + p \equiv y + r \pmod m$.

Prova:

Por hipótese m divide $x - y$, ou seja, existe $q \in Z$ tal que $x - y = qm$ e m divide $p - r$,

ou seja, existe $t \in Z$ tal que $p - r = tm$.

Mas $(x - y) + (p - r) = qm + tm$, ou seja,

$x - y + p - r = (q + t)m$ de onde

$(x + p) - (y + r) = m(q + t)$ o que implica que m divide:

$(x + p) - (y + r)$.

Logo $x + p \equiv y + r \pmod m$

De maneira análoga prova-se que $x - p \equiv y - r \pmod m$.

4b) Se $x \equiv y \pmod m$ e $p \equiv r \pmod m$ então $xp \equiv yr \pmod m$.

Prova:

Pela propriedade 3b) temos:

$xp \equiv yp \pmod m$ e $py \equiv ry \pmod m$.

Pela transitividade temos:

$xp \equiv yr \pmod m$, como queríamos provar.

5) Se $x \equiv y \pmod{m}$ então $x^r \equiv y^r \pmod{m}$, para todo inteiro $r \geq 1$.

Prova:

Vamos provar por indução:

Para $r = 1$ temos $x \equiv y \pmod{m}$ pela hipótese.

Suponhamos que para $r = k$ teremos

$x^k \equiv y^k \pmod{m}$ (hipóteses de indução)

Agora provemos para $r = k + 1$

$x^{k+1} = x^k . x$

Como $x^k \equiv y^k \pmod{m}$ (hipótese de indução), e $x \equiv y \pmod{m}$ então pela propriedade 4b) temos $x^k x \equiv y^k y \pmod{m}$. Portanto $x^{k+1} \equiv y^{k+1} \pmod{m}$.

Logo $x^r \equiv y^r \pmod{m}$ para todo $r \geq 1$.

6) Se $cx \equiv cy \pmod{m}$ e $mdc(m, c) = d > 0$ então $x \equiv y \pmod{m_1}$ onde $m = m_1.d$

Prova:

Por hipótese m divide $c(x - y)$ ou seja, existe $q \in Z$ tal que $c(x - y) = qm$.

Como d divide c temos que existe $c_1 \in Z$ tal que $c = dc_1$

Assim $dc_1(x - y) = m_1 d\, q$.

Como $d > 0$ temos pela propriedade do cancelamento que $c_1(x - y) = m_1 q$.

Portanto m_1 divide $c_1(x - y)$. Como $mdc(m_1, c_1) = 1$, temos que m_1 divide $x - y$ ou seja $x \equiv y \pmod{m_1}$.

Como caso particular temos o seguinte resultado: se $cx \equiv cy$ e $mdc(m, c) = 1$, então $x \equiv y \pmod{m}$.

APLICAÇÕES DE CONGRUÊNCIA

Critérios de Divisibilidade

Por 2:

Seja $n = a_r 10^r + ... + a_1 10 + a_0$ a representação do número natural **n** na base decimal, com $r \geq 1$.

Sabemos que $10 \equiv 0 \pmod 2$. Usando a propriedade 5 temos $10^k \equiv 0^k \pmod 2$, ou seja: $10^k \equiv 0 \pmod 2$ para $k \geq 1$.

Assim $a_r 10^r + ... + a_1 10 + a_0 \equiv a_r 0 + ... + a_1 0 + a_0 \pmod 2$ ou seja

$a_r 10^r + ... + a_1 10 + a_0 \equiv a_0 \pmod 2$.

Portanto se $a_0 \equiv 0 \pmod 2$ então pela propriedade 1c) $a_r 10^r + ... + a_1 10 + a_0 \equiv 0 \pmod 2$ e se $n \equiv 0 \pmod 2$, então $a_0 \equiv 0 \pmod 2$. E ainda se $a_0 \equiv 0 \pmod 2$ então 2 divide $a_0 - 0$, ou seja, existe $q \in Z$ tal que $a_0 = 2q$. Consequentemente concluímos que $a_0 \in \{0, 2, 4, 6, 8\}$.

Logo n é divisível por 2 se e somente se $a_0 \in \{0, 2, 4, 6, 8\}$.

Por 3:

Seja $n = a_r 10^r + ... + a_1 10 + a_0$ a representação do número natural **n** na base decimal, com $r \geq 1$.

Sabemos que $10 \equiv 1 \pmod 3$ Usando a propriedade 5 temos $10^k \equiv 1^k \pmod 3$, ou seja: $10^k \equiv 1 \pmod 3$ para $k \geq 1$. Devemos observar também que $10^0 = 1$ e que $1 \equiv 1 \pmod 1$

Assim $a_r 10^r + ... + a_1 10 + a_0 \equiv a_r + ... + a_1 + a_0 \pmod 3$

Portanto se $a_r + ... + a_1 + a_0 \equiv 0 \pmod 3$ então pela propriedade 1c)

$a_r 10^r + ... + a_1 10 + a_0 \equiv 0 \pmod 3$. E se $n \equiv 0 \pmod 3$, então $a_r + ... + a_1 + a_0 \equiv 0 \pmod 3$.

E, assim, se $a_r + ... + a_1 + a_0 \equiv 0 \pmod 3$ então 3 divide $a_r + ... a_1 + a_0 - 0$, ou seja, existe $q \in Z$ tal que $a_r + ... + a_1 + a_0 = 3q$.

Logo **n** é divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3.

Por 4:

Seja $n = a_r 10^r + ... + a_1 10 + a_0$ a representação do número natural **n** na base decimal, com $r \geq 2$.

Sabemos que $10 \equiv 2 \pmod 4$

Mas $10^2 \equiv 2^2 \pmod 4$ e $4 \equiv 0 \pmod 4$

Assim pela propriedade 3b) temos $10^2\ 10^k \equiv 0\ 10^k \pmod 4$, ou seja, $10^{2+k} \equiv 0 \pmod 4$, para $k \geq 0$.

Com isso $a_r 10^r + ... + a_1 10 + a_0 \equiv a_r 0 + ... + a_1 10 + a_0 \pmod 4$, ou seja,

$a_r 10^r + ... + a_1 10 + a_0 \equiv 10\, a_1 + a_0 \pmod 4$.

Portanto se $10\, a_1 + a_0 \equiv 0 \pmod 4$ então pela propriedade 1c)

$a_r 10^r + ... + a_1 10 + a_0 \equiv 0 \pmod 4$. E se $n \equiv 0 \pmod 4$, então $10\, a_1 + a_0 \equiv 0 \pmod 4$. E se $10\, a_1 + a_0 \equiv 0 \pmod 4$ então 4 divide $10\, a_1 + a_0 - 0$, ou seja, existe $q \in \mathbb{Z}$ tal que

$10\, a_1 + a_0 = 4q$.

Logo **n** é divisível por 4 se e somente se o número formado pelos dois últimos algarismos for divisível por 4.

Por 5:

Seja $n = a_r 10^r + ... + a_1 10 + a_0$ a representação do número natural **n** na base decimal, com $r \geq 1$.

Sabemos que $10 \equiv 0 \pmod 5$.

Usando a propriedade 5 temos $10^k \equiv 0^k \pmod 5$, ou seja:

$10^k \equiv 0 \pmod 5$ para todo $k \geq 1$.

Assim $a_r 10^r + ... + a_1 10 + a_0 \equiv a_r 0 + ... + a_1 0 + a_0 \pmod 5$ ou seja

$a_r 10^r + ... + a_1 10 + a_0 \equiv a_0 \pmod 5$.

Portanto se $a_0 \equiv 0 \pmod 5$ então pela propriedade 1c)

$a_r 10^r + ... + a_1 10 + a_0 \equiv 0 \pmod 5$. E se $n \equiv 0 \pmod 5$, então $a_0 \equiv 0 \pmod 5$. E, sendo

assim, se $n \equiv 0 \pmod 5$, então 5 divide $a_0 - 0$, ou seja, existe $q \in Z$ tal que $a_0 = 5q$.

Logo **n** é divisível por 5 se, e somente se,o seu algarismo das unidades for **0** ou **5**.

Por 11:

Seja $n = a_r 10^r + ... + a_1 10 + a_0$ a representação do número natural **n** na base decimal, com $r \geq 1$.

Sabemos que $10 \equiv -1 \pmod{11}$ e

usando a propriedade 5 temos que $10^k \equiv (-1)^k \pmod{11}$, onde se **k** for par

$10^k \equiv 1 \pmod{11}$ e se **k** for ímpar $10^k \equiv -1 \pmod{11}$. Assim,

$a_0 \equiv a_0 \pmod{11}$

$10a_1 \equiv -a_1 \pmod{11}$, $10a_2 \equiv a_2 \pmod{11}$, $10\,a_3 \equiv -a_3 \pmod{11}$, ...

Com isso $a_r 10^r + ... + a_1 10 + a_0 \equiv (-1)^r a_r + ... + (-a_1) + a_0 \pmod{11}$.

Portanto se $(-1)^r a_r + ... + a_2 - a_1 + a_0 \equiv 0 \pmod{11}$ então pela propriedade 1c)

$a_r 10^r + ... + a_1 10 + a_0 \equiv 0 \pmod{11}$.

E se $n \equiv 0 \pmod{11}$ então $(-1)\, a_r + ... + a_2 - a_1 + a_0 \equiv 0 \pmod{11}$

Assim se $(-1)^r a_r + ... + a_2 - a_1 + a_0 \equiv 0 \pmod{11}$ então 11 divide

$(-1)\, a_r + ... + a_2 - a_1 + a_0 - 0$, ou seja, existe $q \in Z$ tal que $(-1)\, a_r + ... + a_2 - a_1 + a_0 \equiv 11q$

Logo **n** é divisível por **11** se, e somente se, o seu último algarismo menos o penúltimo mais o antepenúltimo e assim sucessivamente, for divisível por **11**.

Determinação de resto na divisão euclidiana

1) Ache os restos nas seguintes divisões:

a) 2^{30} por **17**

Resolução:

Sabemos que $2^4 = 16$ e $16 \equiv -1 \pmod{17}$, pois $16 - (-1) = 16 + 1 = 17$ e $17 = 17.1 + 0$.

Portanto $2^4 \equiv -1 \pmod{17}$.

Como $2^{28} = (2^4)^7$ e pela propriedade 5 $(2^4)^7 \equiv (-1)^7 \pmod{17}$, ou seja, $2^{28} \equiv -1 \pmod{17}$.

Como $2^{30} = 2^{28+2} = 2^{28}2^2 = 2^{28}4$ então pela propriedade 3b $2^{28}4 \equiv (-1)\,4 \pmod{17}$, ou seja,

$2^{30} \equiv -4 \pmod{17}$.

Como $-4 \equiv 13 \pmod{17}$ pois $-4-13=-17$ e $-17 = 17(-1)+0$,

então pela propriedade 1c) $2^{30} \equiv 13 \pmod{17}$.

Logo o resto da divisão de 2^{30} por 17 é 13.

b) $3^{10}.42^5 + 6^8$ por 5.

Resolução:

Sabemos que $3 \equiv -2 \pmod{5}$ e pela propriedade 5 temos que $3^2 \equiv (-2)^2 \pmod{5}$.

Como $(-2)^2 = 4$ então $3^2 \equiv 4 \pmod{5}$. Mas $4 \equiv -1 \pmod{5}$. Assim pela propriedade 1c) temos que $3^2 \equiv -1 \pmod{5}$.

Como $3^{10} = (3^2)^5$ e $(3^2)^5 \equiv (-1)^5 \pmod{5}$,

então $3^{10} \equiv -1 \pmod{5}$.

Sabemos que $42 \equiv 2 \pmod{5}$ e $42^2 \equiv 2^2 \pmod{5}$ (propriedade 5). Como $2^2 \equiv 4$

então $42^2 \equiv 4 \pmod{5}$. Mas $4 \equiv -1 \pmod{5}$. Assim $42^2 \equiv -1 \pmod{5}$ (propriedade 1c).

Como $42^4 = (42^2)^2$ e $(42^2)^2 \equiv (-1)^2 \pmod{5}$ (propriedade 5),

então $42^4 \equiv 1 \pmod{5}$.

Como $42^5 = 42^{4+1} = 42^4 . 42$ e $42^4 . 42 \equiv 1.2 \pmod{5}$ (propriedade 1b),

então $42^5 \equiv 2 \pmod{5}$.

Sabemos que $6 \equiv 1 \pmod{5}$

então $6^8 \equiv 1^8 \pmod{5}$ (propriedade 5) e $6^8 \equiv 1 \pmod{5}$.

Assim $3^{10}.42^5 + 6^8 \equiv (-1)\,2 + 1 \pmod{5}$ (propriedade 4a) e 4b)), ou seja,

$3^{10}.42^5 + 6^8 \equiv -1 \pmod{5}$.

Mas $-1 \equiv 4 \pmod{5}$.

Então $3^{10}.42^5 + 6^8 \equiv 4 \pmod{5}$ (propriedade 1c)

Logo o resto da divisão euclidiana de $3^{10}.42^5 + 6^8$ por 5 é 4.

c) $5^2 . 4841 + 28^5$ por 3

Sabemos $5 \equiv 2 \pmod 3$ e que $2 \equiv -1 \pmod 3$.

Assim pela propriedade 1c) $5 \equiv -1 \pmod 3$

Logo $5^2 \equiv (-1)^2 \pmod 3$ (propriedade 5), ou seja, $5^2 \equiv 1 \pmod 3$.

Sabemos que $4841 \equiv 2 \pmod 3$ pois

$4841 = 3.1613 + 2$

Sabemos que $28 \equiv 1 \pmod 3$ e pela propriedade 5

$28^5 \equiv 1^5 \pmod 3$, ou seja $28^5 \equiv 1 \pmod 3$

Assim $5^2 . 4841 + 28^5 \equiv 1 . 2 + 1 \pmod 3$ (propriedade 4a) e 4b))

onde $5^2 . 4841 + 28^5 \equiv 3 \pmod 3$. Como $3 \equiv 0 \pmod 3$,

então $5^2 . 4841 + 28^5 \equiv 0 \pmod 3$ (propriedade 1c).

Logo o resto da divisão de $5^2 . 4841 + 28^5$ por 3 é 0, ou seja,

$5^2 . 4841 + 28^5$ é divisível por 3.

2) Mostre que $10^{200} - 1$ é divisível por 11.

Resolução:

Como $10 \equiv -1 \pmod{11}$, temos pela propriedade 5 que $10^{200} \equiv (-1)^{200} \pmod{11}$, ou seja, $10^{200} \equiv 1 \pmod{11}$.

Pela propriedade 3 a) $10^{200} - 1 \equiv 1 - 1 \pmod{11}$, ou seja, $10^{200} - 1 \equiv 0 \pmod{11}$, onde $10^{200} - 1$ dividido por 11 tem resto 0.

Logo, $10^{200} - 1$ é divisível por 11.

Prova dos noves

A chamada prova dos nove é baseada, em princípio, no fato de que:

Se $a = b \pm c$ então $a' \equiv b' \pm c' \pmod 9$.

Se $a = bc$ então $a' \equiv b'c' \pmod 9$.

onde a' é a soma dos algarismos de **a**, b' é a soma dos algarismos de **b** e c' é a soma dos algarismos de **c**.

Como essas implicações não valem em sentido contrário, então essa prova pode detectar se há erros num cálculo, mas não garante que este esteja necessariamente certo. A escolha do "nove", por outro lado, é apenas uma conveniência decorrente de nosso sistema de numeração. De fato, se a representação polinomial decimal de um inteiro $n > 0$ é $a_r10^r + ... + a_210^2 + a_110 + a_0$ onde $0 \leq a_i \leq 9$ então $n \equiv a_r + ... + a_2 + a_1 + a_0 \pmod 9$ pois o fato de que $10 \equiv 1 \pmod 9$ implica $10^k \equiv 1 \pmod 9$, para todo $k \geq 1$.

Assim, **n** e $a_r+...+a_2 + a_1 + a_0$ têm o mesmo resto na divisão euclidiana por **9**. Então é bastante cômodo achar o resto da divisão de **n** por **9**. Daí a escolha desse número para a prova.

1) Verifique se as seguintes contas estão corretas:

   a) $a = 2910273$ dividido por $b = 7158$ tem quociente $q = 406$ e resto $r = 4125$.

   Resolução:

   Como devemos ter que $a = bq + r$ então $a \equiv bq + r \pmod 9$.

   Para cada um desse inteiros **"noves fora"**, obtemos:

   $a \equiv 2 + 9 + 1 + 0 + 2 + 7 + 3 \pmod 9$, ou seja, $a \equiv 6 \pmod 9$

   $b \equiv 7 + 1 + 5 + 8 \pmod 9$, ou seja, $b \equiv 3 \pmod 9$

   $q \equiv 4 + 0 + 6 \pmod 9$, ou seja, $q \equiv 1 \pmod 9$

   $r \equiv 4 + 1 + 2 + 5 \pmod 9$, ou seja, $r \equiv 3 \pmod 9$.

   Então $bq + r \equiv 3.1 + 3 \pmod 9$, ou seja, $bq + r \equiv 6 \pmod 9$.

   Como $a \equiv 6 \pmod 9$ então $a \equiv bq + r \pmod 9$.

   Logo a divisão feita passou pela **"prova dos noves"**. Isto não significa que a divisão está correta. Mas, de fato, $2910273 = 7158.406 + 4125$.

b) **a = 72435** adicionado a **b = 98106** obtém – se **c = 160531**

Resolução:

Como devemos ter que **c = a + b** então **c ≡ a + b (mod 9).**

Para cada um desse inteiros **"noves fora"**, obtemos:

a ≡ 7 + 2 + 4 + 3 + 5 (mod 9), ou seja, **a ≡ 3 (mod 9)**

b ≡ 9 + 8 + 1 + 0 + 6 (mod 9), ou seja, **b ≡ 6 (mod 9)**

c ≡ 1 + 6 + 0 + 5 + 3 + 1 (mod 9), ou seja, **c ≡ 7 (mod 9)**

Então **a + b ≡ 3 + 6 (mod 9),** ou seja, **a + b ≡ 0 (mod 9).**

Como **c ≡ 7 (mod 9)** então **c** não é côngruo a **a + b** módulo **9.**

Logo a adição feita não passou pela **"prova dos noves".** Isto significa que a adição não está correta.

c) **a = 1821211** subtraído de **b = 3469** obtém - se **c = 822278.**

Resolução:

Como devemos ter que **c = a - b** então **c ≡ a - b (mod 9).**

Para cada um desse inteiros **"noves fora"**, obtemos:

a ≡ 1 + 8 + 2 + 1 + 2 + 1 + 1 (mod 9), ou seja, **a ≡ 7 (mod 9)**

b ≡ 3 + 4 + 6 + 9 (mod 9), ou seja, **b ≡ 4 (mod 9)**

c ≡ 1 + 8 + 2 + 2 + 2 + 7 + 8 (mod 9), ou seja, **c ≡ 3 (mod 9).**

Então **a - b ≡ 7 - 4 (mod 9),** ou seja, **a - b ≡ 3 (mod 9).**

Como **c ≡ 3 (mod 9)** então **c ≡ a - b (mod 9).**

Portanto a subtração feita passou pela **"prova dos nove".** Isto não significa que a subtração está correta. E de fato não está pois **1821211 – 3469 = 1817742.**

Logo a **"prova dos noves"** falhou.

CONGRUÊNCIAS LINEARES

O objetivo deste tópico é apresentar o **Teorema do Resto Chinês.** Este teorema é importante para que o professor possa preparar problemas interessantes de aplicação do algoritmo de Euclides.

Definição: Uma congruência do tipo

$$\mathbf{ax \equiv b \pmod{m}}$$

onde $\mathbf{a, b, m \in Z, a \neq 0}$ e $\mathbf{m > 0}$, recebe o nome de congruência linear ou congruência de primeiro grau.

Vejamos que se **c** é uma solução de $\mathbf{ax \equiv b \pmod{m}}$ então qualquer $\mathbf{d \in Z}$ tal que $\mathbf{d \equiv c \pmod{m}}$ também é uma solução de $\mathbf{ax \equiv b \pmod{m}}$.

Em particular temos que o resto **r** da divisão euclidiana de **c** por **m** também é solução desta equação.

Se **c** é solução de $\mathbf{ax \equiv b \pmod{m}}$, então $\mathbf{ac \equiv b \pmod{m}}$.

Como $\mathbf{d \equiv c \pmod{m}}$, temos que $\mathbf{ad \equiv ac \pmod{m}}$ (propriedade 3 b)) e pela propriedade 1c) temos que $\mathbf{ad \equiv b \pmod{m}}$ e portanto **d** é solução de $\mathbf{ax \equiv b \pmod{m}}$.

Convencionamos que todo os $\mathbf{x \in Z}$ tais que $\mathbf{x \equiv r \pmod{m}}$ constituem uma única solução de $\mathbf{ax \equiv b \pmod{m}}$.

Sistemas de Congruência Linear: Um sistema com várias congruências lineares é chamado sistema de congruência linear.

O Teorema do Resto Chinês depende de outras proposições para ser demonstrado. No entanto, faremos apenas a citação destas proposições sem demonstrá-las.

Proposição 1: Uma congruência linear $\mathbf{ax \equiv b \pmod m}$ onde $\mathbf{a \neq 0}$, admite soluções em **Z** se, e somente se, **b** é divisível por $\mathbf{d = mdc\ (a, m)}$. E neste caso, se $\mathbf{x_0}$ é uma solução particular, então o conjunto de todas as soluções tem **d** elementos, a saber:

$$\mathbf{x_0}, \mathbf{x_0} + \frac{m}{d}, \mathbf{x_0} + 2\frac{m}{d}, \ldots, \mathbf{x_0} + (\mathbf{d}-1)\frac{m}{d}$$

Proposição 2: Um sistema:
$$\begin{cases} \mathbf{x \equiv a_1 \pmod{m_1}} \\ \mathbf{x \equiv a_2 \pmod{m_2}} \end{cases}$$

Admite solução, se, e somente se, $\mathbf{a_1 - a_2}$ é divisível por $\mathbf{d = mdc\ (m_1, m_2)}$.
Neste caso, se $\mathbf{x_0}$ é uma solução particular do sistema e se $\mathbf{m = mmc\ (m_1, m_2)}$
Então $\mathbf{x \equiv x_0 \pmod m}$ é sua solução geral.

Corolário: Um sistemas de congruências
$$\begin{cases} \mathbf{x \equiv a_1 \pmod{m_1}} \\ \mathbf{x \equiv a_2 \pmod{m_2}} \\ \\ \mathbf{x \equiv a_r \pmod{m_r}} \end{cases}$$

admite soluções se e somente se $\mathbf{a_i - a_j}$ é divisível por $\mathbf{d_{ij} = mdc\ (m_i, m_j)}$ para qualquer par de índices **i, j** ($\mathbf{i \neq j}$), Neste caso, se $\mathbf{x_0}$ é uma solução particular, então a solução geral do sistema é dada por:
$\mathbf{x \equiv x_0 \pmod m}$ onde $\mathbf{m = mmc\ (m_1, m_2, m_3, \ldots, m_r)}$.

Proposição 3 (Teorema do Resto Chinês): Sejam $m_1, m_2, ..., m_r$, números inteiros maiores que **zero** e tais que **mdc** $(m_i, m_j) = 1$ sempre que $i \neq j$. Façamos $m = m_1 m_2 m_3 ... m_r$ e sejam $b_1, b_2, ..., b_r$, respectivamente, soluções das congruências lineares.

$$\frac{m}{m_j} y \equiv 1 \pmod{m_j} \quad (j = 1, 2, ..., r)$$

Então o sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_r \pmod{m_r} \end{cases}$$

é possível (admite soluções) para quaisquer $a_1, a_2, ..., a_r \in \mathbf{Z}$ e sua solução geral é dada por:

$$x \equiv a_1 b_1 \frac{m}{m_1} + ... + a_r b_r \frac{m}{m_r} \pmod{m}.$$

Demonstração: Que o sistema é possível decorre do corolário da proposição anterior. Notemos que, como **mdc** $(m_j, m_i) = 1$ para $i \neq j$ então,

mdc $(m_j, \frac{m}{m_j}) = 1$, já que $m = m_1 m_2 m_3 ... m_r$, o que implica a existência de soluções para

cada congruência linear $\frac{m}{m_j} y \equiv 1 \pmod{m_j}$

as quais estamos indicando por b_j $(j = 1, 2, 3, ..., r)$

Assim $\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$ e portanto

$a_j b_j \frac{m}{m_j} \equiv a_j \pmod{mj}$ pela propriedade 3b).

Por outro lado , se $i \neq j$, $\frac{m}{m_i} \equiv 0 \pmod{m_j}$,

então $\mathbf{a_i b_i} \frac{m}{m_i} \equiv 0$ **(mod $\mathbf{m_j}$)** pela propriedade 3b).

Portanto

$$\mathbf{a_1 b_1} \frac{m}{m_1} + ... + \mathbf{a_j b_j} \frac{m}{m_j} + ... + \mathbf{a_r b_r} \frac{m}{m_r} \equiv \mathbf{a_j b_j} \frac{m}{m_j} \quad \textbf{(mod } \mathbf{m_j}\textbf{)}$$

Como $\mathbf{b_j} \frac{m}{m_j} \equiv 1$ **(mod $\mathbf{m_j}$)** então, pela propriedade 3b) $\mathbf{a_j b_j} \frac{m}{m_j} \equiv \mathbf{a_j}$ **(mod $\mathbf{m_j}$).**

Logo $\mathbf{a_1 b_1} \frac{m}{m_1} + ... + \mathbf{a_j b_j} \frac{m}{m_j} + ... + \mathbf{a_r b_r} \frac{m}{m_r} \equiv \mathbf{a_j}$ **(mod $\mathbf{m_j}$)**

Para todo **j**, $\mathbf{1 \leq j \leq r}$.

Assim, de fato, $\mathbf{x_0} = \sum_{i=1}^{r} a_i b_i \frac{m}{m_i}$ é uma solução particular do sistema. O corolário da proposição anterior garante então que $\mathbf{x \equiv x_0}$ **(mod m)**

é solução geral e como **mdc** $(\mathbf{m_i}, \mathbf{m_j}) = 1$ sempre que $\mathbf{i \neq j}$, então

mmc $(\mathbf{m_1}, \mathbf{m_2}, ..., \mathbf{m_r}) = \mathbf{m_1 m_2 ... m_r} = \mathbf{m}$.

APLICAÇÃO DE CONGRUÊNCIA LINEAR

1) Um bando de **17** piratas ao tentar dividir entre si, igualmente as moedas de ouro de uma arca, verifica que **3** moedas sobrariam. Na discussão que se seguiu um dos piratas foi morto; na nova tentativa de divisão, já com um pirata a menos, desta feita **10** moedas sobrariam. Nova quiproquo e mais um pirata é morto. Mas agora, por fim é possível dividir igualmente a fortuna entre eles. Qual o menor número de moedas que a arca poderia conter?

Resolução:

Temos que resolver o seguinte sistema:

$$\begin{cases} \mathbf{x \equiv 3 \pmod{17}} \\ \mathbf{x \equiv 10 \pmod{16}} \\ \mathbf{x \equiv 0 \pmod{15}} \end{cases}$$

O primeiro passo é achar os valores de $\mathbf{b_i}$ nas seguintes congruências lineares:

$\frac{m}{m_j}\mathbf{y \equiv 1 \pmod{m_j}}$ onde $\mathbf{m = m_1 m_2 m_3}$ e $\mathbf{j = 1, 2, 3.}$

1) $\frac{m}{m_1}\mathbf{b_1 \equiv 1 \pmod{m_1}}$ onde $\mathbf{m_1 = 17,\ m = 4080.}$

Assim, $\mathbf{240\ b_1 \equiv 1 \pmod{17}}$ onde $\mathbf{b_1 = -8}$ é uma solução particular pois $\mathbf{240\ (-8) = -1920}$ e $\mathbf{-1920 \equiv -16 \pmod{17}}$. Mas $\mathbf{-16 \equiv 1 \pmod{17}}$. Logo $\mathbf{-1920 \equiv 1 \pmod{17}}$.

2) $\frac{m}{m_2}\mathbf{b_2 \equiv 1 \pmod{m_2}}$ onde $\mathbf{m_2 = 16}$ e $\mathbf{m = 4080.}$

Assim, $\mathbf{255\ b_2 \equiv 1 \pmod{16}}$ onde $\mathbf{b_2 = -1}$ é uma solução particular pois $\mathbf{255\ (-1) = -255}$ e $\mathbf{-255 \equiv -15 \pmod{16}}$. Mas $\mathbf{-15 \equiv 1 \pmod{16}}$. Logo $\mathbf{-255 \equiv 1 \pmod{16}}$.

3) $\frac{m}{m_3}\mathbf{b_3} \equiv \mathbf{1\ (mod\ m_1)}$ onde $\mathbf{m_3 = 15}$ e $\mathbf{m = 4080.}$

Assim, $\mathbf{272\ b_3 \equiv 1\ (mod\ 15)}$ onde $\mathbf{b_3 = -7}$ é uma solução particular pois $\mathbf{272\ (-7) = -1904}$ e $\mathbf{-1904 \equiv -14\ (mod\ 15)}$. Mas $\mathbf{-14 \equiv 1\ (mod\ 15)}$. Logo $\mathbf{904 \equiv 1 (mod\ 15).}$

Pelo teorema do resto chinês,

$$\mathbf{x \equiv a_1 b_1 \frac{m}{m_1} + a_2 b_2 \frac{m}{m_2} + a_3 b_3 \frac{m}{m_3}\ (mod\ m)} \text{ onde } \mathbf{a_1 = 3,\ a_2 = 10,\ a_3 = 0}$$

é uma solução geral do sistema considerado.

Portanto, temos:

$\mathbf{x \equiv 3\ (-8).240 + 10\ (-1).255 + 0\ (-7).272\ (mod\ 4080)}$

$\mathbf{x \equiv -5760 - 2550\ (mod\ 4080)}$

$\mathbf{x \equiv -8310\ (mod\ 4080).}$

Mas o problema pede o menor número de moedas que a arca poderia conter. Portanto devemos ainda determinar este valor que será maior que **zero**.

$\mathbf{x \equiv -8310\ (mod\ 4080).}$ Então $\mathbf{x \equiv -8310 + 4080\ t}$, para $\mathbf{t \in Z.}$

Se $\mathbf{x > 0}$ então $\mathbf{4080 > 8310 = 2.4080 + 150 > 2.4080.}$ Então $\mathbf{t > 2}$.

Como queremos a menor quantidade de moedas, consideramos $\mathbf{t = 3}$ e temos

$\mathbf{x = -8310 + 4080.3 = 3930.}$

Logo, o menor número de moedas que a arca poderia conter era **3930.**

AULAS COM CONGRUÊNCIA PARA ALUNOS DE 5ª E 6ª SÉRIES

As aulas relatadas a seguir foram ministradas para 5ª e 6ª séries do 1º grau (uma turma de cada série), uma vez que é nestas séries que o aluno passa a conhecer de maneira mais aprofundada o Conjunto dos Números Naturais e Inteiros, o algoritmo de Euclides, Máximo e Mínimo Divisor Comum etc., conteúdos estes que dão todo o embasamento para a definição de congruência.

E por que fazer tal aplicação?

Além de ter exercícios muito interessantes e diferentes em relação aos exercícios habituais e que envolvem a aplicação do algoritmo de Euclides, tornando-se bastante atrativo para os alunos, com congruência consegue-se dar explicações para muitos resultados e regras que acabam sendo ensinados, ou para melhor dizer, transmitidos de forma mecânica onde o aluno simplesmente decora e pronto, como, por exemplo, os critérios de divisibilidade.

No entanto, tais regras não foram demonstradas para os alunos. Procurou-se apenas verificar se a própria definição de congruência, bem como sua notação, seria algo perceptivo para os mesmos.

Em 8 (oito) aulas procurou-se, portanto, apresentar uma parte de tal conteúdo, sem a preocupação de um aprofundamento, mostrando apenas que a congruência faz parte da aplicação do algoritmo de Euclides e esta abrange vários caminhos a serem descobertos e que só vem a somar pontos positivos no aprendizado.

1ª aula:

Inicialmente, para uma melhor compreensão e fixação do algoritmo de Euclides que é muito usado em congruência, introduziu-se algumas divisões:

a) **104 | 3**_____ que também pode ser escrita da seguinte maneira:

14 34 **104 = 3 . 34 + 2**

2

b) **2927 | 7**____ que também pode ser escrita da seguinte maneira:

12 418 **2927 = 7 . 418 + 1**

57

1

c) **11282 | 2**_____ que também pode ser escrita da seguinte maneira:

12 5641 **11282 = 5641 . 2 + 0**

08

02

0

Em todos os casos a segunda maneira é chamada de algoritmo de Euclides, a prova real de uma divisão por chaves como todos conhecem.

Exercícios

1) Ache o quociente e o resto na divisão Euclidiana de **a** por **b** nos seguintes casos (aplique o algoritmo de Euclides).

a) **a = 390**

b = 74

Resolução:

390 = 74 . 5 + 20

Resposta: quociente: **5** e resto: **20**

b) **a = 124**

b = 18

Resolução

124 = 18 . 6 + 16

Resposta: quociente: **6** e resto: **16**

c) **a = 420**

b = 58

Resolução

420 = 58 . 7 + 14

Resposta: quociente: **7** e resto: **14**

Comentário sobre a primeira aula:

Para os alunos, o algoritmo de Euclides significava a prova real do método da divisão por chaves. E portanto não seria importante usar o algoritmo quando se tinha a certeza do resultado obtido.

No entanto, mesmo preferindo o método das chaves, os alunos não mostraram

dificuldade quanto à aplicação do algoritmo nos exercícios, apesar de muitos deles (principalmente os alunos da 5° série) resolverem primeiro pelo método da chave e depois aplicarem os resultados obtidos no algoritmo de Euclides.

2ª aula:

Anotando por **a : b** a aplicação do algoritmo de Euclides para **a** e **b**, observe o significado de:

a) 47: 3
b) 329: 5
c) 509 : 8

Sabemos que, pelo algoritmo de Euclides, temos:

a) **47 = 3 . 15 + 2** logo **47 : 3** tem quociente **15** e resto **2**
b) **329 = 5 . 65 + 4** logo **329 : 5** tem quociente **65** e resto **4**
c) **509 = 8 . 63 + 5** logo **509 : 8** tem quociente **63** e resto **5**

Vamos subtrair o dividendo pelo seu respectivo resto em cada operação:

a) 47 – 2 = 45
b) 329 – 4 = 325
c) 509 – 5 = 504

O que ocorrerá se dividirmos esse novo número obtido com as subtrações efetuadas pelos respectivos divisores de antes?
Vejamos:

45 : 3

Pelo algoritmo de Euclides temos:

45 = 35 + 0 onde o quociente é **5** e o resto é **0 (zero).**

325 : 5

Pelo algoritmo de Euclides temos:

325 = 5 . 65 + 0 onde o quociente é **65** e o resto é **0 (zero).**

504 : 8

Pelo algoritmo de Euclides temos:

504 = 8. 63 + 0 onde o quociente é **63** e o resto é **0 (zero).**

Podemos observar que em todas as operações o resto é **zero**, ou seja, as divisões obtidas são exatas.

Com isso concluímos que para todas as divisões, quando subtraímos o dividendo pelo resto e dividimos o número obtido pelo mesmo divisor essa divisão será exata.

Existe um conteúdo matemático chamado congruência cuja definição se baseia na conclusão acima.

Definição de congruência: Dados **x, y** e **z** números inteiros com $z \geq 1$, dizemos que **x** é côngruo a **y** módulo **z** se $x - y$ é divisível por **z.**

Notação: $x \equiv y \pmod{z}$

Assim aplicando a definição de congruência para os exemplos dados anteriormente teremos:

$47 \equiv 2 \pmod{3}$ pois $47 - 2$ é divisível por **3** ou seja:

$47 - 2 = 45$ e **$45 = 3 . 15 + 0$**

329 ≡ 4 (mod 5) pois **329 – 4** é divisível por **4** ou seja:

329 – 4 = 325 e **325 = 5 . 65 + 0**

509 ≡ 5 (mod 8) pois **509 – 5** é divisível por **8** ou seja:

509 – 5 = 504 e **504 = 8 . 63 + 0**

Logo em uma divisão o dividendo sempre será côngruo ao resto módulo divisor.

Exercícios

1) Verifique se é falsa ou verdadeira cada congruência abaixo:

a) **22 ≡ 3 (mod 5)**

Resolução:

22 – 3 = 19 e **19 = 5 . 3 + 4**

Portanto **19** não é divisível por **5** e **22** não é côngruo a **2** módulo **5.**

Logo essa congruência é falsa.

b) **37 ≡ 2 (mod 8)**

Resolução:

37 – 2 = 35 e **35 = 8 . 4 + 3**

Portanto **35** não é divisível por **8** e **37** não é côngruo a **2** módulo **8.**

Logo essa congruência é falsa.

c) **625 ≡ 1 (mod 3)**

Resolução:

625 – 1 = 624 e **624 = 3 . 208 + 0**

Portanto **624** é divisível por **3** e **625** é côngruo a **1** módulo **3**;

Logo essa congruência é verdadeira

d) **144 ≡ 0 (mod 12)**

Resolução:

144 – 0 = 144 e **144 = 12 . 12 + 0**

Portanto **144** é divisível por **12** e **144** é côngruo a **0** módulo **12.**

Logo essa congruência é verdadeira.

Comentários sobre a segunda aula

De uma maneira geral, não foi difícil os alunos entenderem a definição e a notação de congruência. Procurou–se relacionar os elementos divisor, dividendo e resto do algoritmo de Euclides com a definição de congruência, para desse modo, facilitar a introdução do novo assunto.

3ª aula:

a) Pelo algoritmo de Euclides temos que **359 : 4** é:

359 = 4 . 89 + 3

b) Pelo algoritmo de Euclides temos que **51 : 4** é:

51 = 4 . 12 + 3

Podemos observar que ambas têm o mesmo quociente e o mesmo resto.

Pela definição de congruência sabemos também que:

359 ≡ 3 (mod 4) pois **359 – 3 = 356** e

356 = 4 . 89 + 0

51 ≡ 3 (mod 4) pois **51 – 3 = 48** e

48 = 4 . 12 + 0

Vejamos agora a seguinte subtração:

359 - 51

O resultado dessa subtração é **308.**

Se dividirmos **308** por **4** obtemos **77** pois, pelo algoritmo de Euclides, **308 = 4 . 77 + 0**

Essa é uma divisão exata e pela definição de congruência temos então:

359 ≡ 51 (mod 4) pois **359 – 51** é divisível por **4.**

Logo, quando dois números diferentes são divididos pelo mesmo divisor e em ambas divisões obtém-se o mesmo resto, diz-se que eles são congruentes módulo divisor.

Exercícios

1) Ache **5** números inteiros **x** tais que:

   $5 \leq x \leq 100$ e **$x \equiv 5$ (mod 8)**

   Resolução:

   Por tentativa temos:

   a) **x = 5**

      $5 \equiv 5$ (mod 8) pois

      $5 - 5 = 0$ e

      $0 = 8 . 0 + 0$

   b) **x = 13**

      $13 \equiv 5$ (mod 8) pois

      $13 - 5 = 8$ e

      $8 = 8 . 1 + 0$

   c) **x = 21**

      $21 \equiv 5$ (mod 8) pois

      $21 - 5 = 16$ e

      $16 = 8 . 2 + 0$

d) $x = 29$

$29 \equiv 5 \pmod 8$ pois

$29 - 5 = 24$ e

$24 = 8 \cdot 3 + 0$

e) $x = 37$

$37 \equiv 5 \pmod 8$ pois

$37 - 5 = 32$ e

$32 = 8 \cdot 4 + 0$

2) Aplique o algoritmo de Euclides e forme 3 congruências com **324 : 7** e **527 : 7**

Resolução:

$324 = 7 \cdot 46 + 2$

$527 = 7 \cdot 75 + 2$

Podemos formar as seguinte congruências:

$324 \equiv 2 \pmod 7$ $\qquad$ $527 \equiv 324 \pmod 7$ $\qquad$ $527 \equiv 2 \pmod 7$

Comentários sobre a terceira aula:

Nesta aula, os alunos apresentaram um pouco mais de dificuldades. Muitos se fixaram na aplicação de congruência entre o divisor, o dividendo e o resto do algoritmo de Euclides, onde o dividendo é côngruo ao seu resto módulo divisor. Era difícil eles entenderem, por exemplo, que $359 \equiv 51 \pmod 4$, já que **359** dividido por **4** não deixava resto **51**. Mas, aos poucos foi sendo colocado que esta seria outra maneira de encarar a congruência e poderia ser aplicada uma vez que **359** dividido por **4** tem o mesmo resto que **51** dividido por **4**.

Em relação a resolução dos exercícios, cada aluno obteve seu resultado e na maior parte os resultados encontrados estavam certos. Quase todos os alunos perceberam que bastava por tentativa, achar o primeiro número, pois a soma deste com **8** daria o próximo número e assim sucessivamente.

Mas em todas as resoluções dos alunos verificou-se que o primeiro número era maior que **8.** Isto se deve ao fato de que os alunos não estão habituados a efetuar divisões euclidianas onde o dividendo é menor que o divisor, mesmo tendo consciência de que o resto é sempre menor que o divisor. Quando aparece, por exemplo, **5 : 8** eles automaticamente resolvem da seguinte maneira:

50 |__8_____
20 0, 625
40
0

Não conseguem concluir que **5 : 8** também pode ser efetuado dessa forma:

5 |__8___
5 0

obtendo assim uma divisão inteira, onde o resto **(5)** é menor que o divisor **(8).**

Sempre que a divisão, exata ou com resto, é ensinado aos alunos exercita-se divisões onde o dividendo sempre é maior que o divisor. E quando é ensinado aos alunos a divisão com vírgula aí sim mostra-se divisões onde o dividendo é menor que o divisor, afim de se obter um quociente decimal. Mas, neste caso, se está trabalhando com divisão de números racionais e isto não fica claro ao aluno. Esta é uma grande falha que deve ser corrigida por alguns professores de matemática.

4ª aula:

Quando analisamos as colunas de um calendário, cada coluna apresenta certos números que a partir do segundo é o anterior mais 7.

Logo **2° - 1°** é múltiplo de 7.
3° - 2° é múltiplo de 7.

Ou seja: $2^o \equiv 1^o \pmod 7$.

$3^o \equiv 2^o \pmod 7$.

Por exemplo: Se hoje é sábado, daqui a 152 dias, que dia da semana será?

Consideremos a seguinte relação: ao dia de hoje (sábado), associamos o número **0**, ao dia de amanhã, o número **1**, e assim por diante. Observe o quadro:

Sábado	Domingo	Segunda	Terça	Quarta	Quinta	Sexta
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.

Sabemos que os números de cada coluna serão congruentes entre si módulo **7.**

Como $152 = 7 \cdot 21 + 5$ isso significa que $152 \equiv 5 \pmod 7$. Portanto **152** estará na mesma coluna que o número **5**, ou seja quinta-feira.

Logo, se hoje é **sábado**, daqui a **152** dias será **quinta feira.**

Exercícios

1) Verifique se o 264^o e o 118^o dias do ano pertencem ao mesmo dia da semana.

Resolução:

Devemos verificar se $264 \equiv 118 \pmod 7$

Como $264 - 118 = 146$ e $146 = 7 \cdot 20 + 6$

Então **146** não é divisível por **7**. E portanto **264** não é côngruo a **118 módulo 7.**

Logo 264^o e 118^o dia dos ano não pertencem ao mesmo dia da semana.

2) Se hoje é quarta-feira, que dia da semana será daqui a **279** dias?

Resolução:

Consideremos a seguinte relação: ao dia de hoje (quarta-feira) associamos o número **0**, ao dia de amanhã o número **1** e assim por diante. Assim:

Quarta	Quinta	Sexta	Sábado	Domingo	Segunda	Terça
0	**1**	**2**	**3**	**4**	**5**	**6**
7	**8**	**9**	**10**	**11**	**12**	**13**
14	**15**	**16**	**17**	**18**	**19**	**20**
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.

Sabemos que os números de cada coluna serão congruentes entre si módulo 7.

Como $279 = 7 \cdot 39 + 6$

Então $279 \equiv 6 \pmod 7$. Portanto **279** estará na mesma coluna que o número **6**, ou seja terça-feira.

Logo se hoje é **quarta-feira**, daqui a **279** dias será **terça-feira.**

Comentário da quarta aula

Esta aula refere-se a uma aplicação da aula passada. Foi bastante divertida, agradável e proveitosa e que despertou nos alunos muito interesse. Não é fácil aplicar e explicar aos alunos exercícios como estes. No entanto, o resultado é *surpreendente*, fazendo com que o trabalho realizado se torne mais gratificante.

Em relação ao exemplo dado e ao exercício 2), foi trabalhado apenas dias posteriores, uma vez que os dias anteriores deveriam ser relacionados com números negativos. Mas os alunos ainda não estão aptos para tal aplicação.

5ª aula:

Já sabemos que a congruência pode ser aplicada entre o dividendo, divisor e o resto de uma divisão euclidiana, onde o dividendo é côngruo ao seu resto módulo divisor.

Sabemos também que dois números quaisquer são côngruos desde que esses números apresentem um mesmo resto quando divididos por um mesmo número.

No entanto, a aplicação de congruência pode ser apresentada de outras maneiras, ou seja, existem propriedades que facilitam a aplicação de congruência e no decorrer das próximas aulas, veremos algumas dessas propriedades.

Propriedades:

1ª) Quando temos, por exemplo, que **15 ≡ 3 (mod 4)** isto significa que também podemos formar a congruência **3 ≡ 15 (mod 4)**, isto é, se afirmamos que **15** é *côngruo* a **3** módulo 4, então **3** também é *côngruo* a **15** módulo **4**. Mesmo porque se **3 ≡ 15 (mod 4)** então **3 – 15** deve ser divisível por **4**. E de fato é, pois **3 – 15 = -12** e **-12 = 4 (-3) + 0**. Este é o algoritmo de Euclides aplicado a números inteiros menores que **zero**. Mas não iremos nos aprofundar nesta aplicação, mesmo porque o que nos interessa é saber que
se **15 ≡ 3 (mod 4)** então **3 ≡ 15 (mod 4)**.

Exercícios

Verifique se é falsa ou verdadeira as seguintes congruências:

a) **7 ≡ 24 (mod 5)**

Resolução:

Se **7 ≡ 24 (mod 5)** então **24 ≡ 7 (mod 5)**.

Mas **24 – 7 = 17** e **17 = 5 . 3 + 2**

Portanto **17** não é divisível por **5** e **24** não é côngruo a **7** módulo **5**.

Logo **7** não é côngruo a **24** módulo **5** e essa congruência é falsa.

b) **33 ≡ 57 (mod 6)**

Resolução:

Se **33 ≡ 57 (mod 6)** então **57 ≡ 33 (mod 6).**

Como **57 – 33 = 24** e **24 = 6 . 4 + 0**

então **24** é divisível por **6** e **57** é côngruo a **33** módulo **6.**

Logo **33** é côngruo a **57** módulo **6** e essa congruência é verdadeira.

c) **12 ≡ 72 (mod 8)**

Resolução:

Se **12 ≡ 72 (mod 8)** então **72 ≡ 12 (mod 8)**

Mas **72 – 12 = 60** e **60 = 8 . 7 + 4**

Portanto **60** não é divisível por **8** e **72** não é côngruo a **12** módulo **8.**

Logo **12** não é côngruo a **72** módulo **8** e essa congruência é falsa.

d) **8 ≡ 545 (mod 3)**

Resolução:

Se **8 ≡ 545 (mod 3)** então **545 ≡ 8 (mod 3).**

Como **545 – 8 = 537** e **537 = 3 . 179 + 0**

Então **537** é divisível por **3** e **545** é côngruo a **8** módulo **3.**

Logo **8** é côngruo a **545** módulo **3** e essa congruência é verdadeira.

Comentário sobre a 5ª aula

Como os alunos não tinham conhecimento sobre números inteiros (ou pelo menos não o suficiente), tornou-se uma aula um pouco complicada.

No entanto, eles aceitaram facilmente o fato de que, por exemplo, se **15 ≡ 3 (mod 4)** já que **15 – 3 = 12** e **12 = 4 . 3 + 0**, então **3 ≡ 15 (mod 4)**
pois **3 – 15 = -12** e **–12 = 4 (-1) + 0.**

Para eles é complicado aplicar a definição de congruência para **3 ≡ 15 (mod 4)**, mas o mais importante é que eles sabem que é possível fazer essa aplicação.

6 ª aula:

Código Secreto

A congruência, desde tempos atrás, é usada para codificar e decodificar mensagens.

E como funciona?

Vejamos na tabela abaixo.

ESPAÇO	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Cada letra é representada por um número.

Agora vejamos a fórmula **c ≡ m + t (mod 27)**

Onde:
- **c** é o resultado
- **m** é o número que cada letra representa
- **t** é um número arbitrário entre **0** e **26** escolhido pela pessoa que manda o código

Exemplo:

Decifre a mensagem: **XGHCOTOVFTVC** para **t = 12**

Resolução:

Na fórmula **c ≡ m + t (mod 27)** queremos descobrir **c.**

1°) **X → X** corresponde ao número **24.** Logo **m** é **24.**

Então aplicando na fórmula temos:

c ≡ 24 + 12 (mod 27) ou seja **c ≡ 36 (mod 27).**

Se **c ≡ 36 (mod 27)** então **36 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **36** por **27.**

Como **36 = 27 . 1 + 9** então **c = 9**.

Consultando a tabela, percebemos que **9** representa **I**.

Logo **X** significa **I**

2°) **G → G** corresponde ao número **7**. Logo **m** é **7**.

Então aplicando na fórmula temos:

c ≡ 7 + 12 (mod 27) ou seja

c ≡ 19 (mod 27).

Se **c ≡ 19 (mod 27)** então **19 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **19** por **27**.

Como **19 = 27 . 0 + 19** então **c = 19**.

Consultando a tabela, percebemos que **19** representa **S**.

Logo **G** significa **S**.

3°) **H → H** corresponde ao número **8**. Logo **m** é **8**.

Então aplicando na fórmula temos:

c ≡ 8 + 12 (mod 27) ou seja

c ≡ 20 (mod 27).

Se **c ≡ 20 (mod 27)** então **20 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **20** por **27**.

Como **20 = 27 . 0 + 20** então **c = 20**.

Consultando a tabela, percebemos que **20** representa **T**.

Logo **H** significa **T**.

4°) **C → C** corresponde ao número **3**. Logo **m** é **3**.

Então aplicando na fórmula temos:

c ≡ 3 + 12 (mod 27) ou seja

c ≡ 15 (mod 27).

Se **c ≡ 15 (mod 27)** então **15 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **15** por **27.**

Como **15 = 27 . 0 + 15** então **c = 15.**

Consultando a tabela, percebemos que **15** representa **O.**

Logo **C** significa **O.**

5°) **O → O** corresponde ao número **15.** Logo **m** é **15.**

Então aplicando na fórmula temos:

c ≡ 15 + 12 (mod 27) ou seja

c ≡ 27 (mod 27).

Se **c ≡ 27 (mod 27)** então **27 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **27** por **27.**

Como **27 = 27 . 1 + 0** então **c = 0.**

Consultando a tabela, percebemos que **0** corresponde a um espaço (entre uma letra e outra).

6°) **T → T** corresponde ao número **20.** Logo **m** é **20.**

Então aplicando na fórmula temos:

c ≡ 20 + 12 (mod 27) ou seja

c ≡ 32 (mod 27).

Se **c ≡ 32 (mod 27)** então **32 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **32** por **27.**

Como **32 = 27 . 1 + 5** então **c = 5.**

Consultando a tabela, percebemos que **5** representa **E.**

Logo **T** significa **E.**

7°) **O →** já verificamos que **O** corresponde a um espaço.

8°) **V → V** corresponde ao número **22.** Logo **m** é **22.**

Então aplicando na fórmula temos:

$\mathbf{c \equiv 22 + 12 \pmod{27}}$ ou seja $\mathbf{c \equiv 34 \pmod{27}}$.

Se $\mathbf{c \equiv 34 \pmod{27}}$ então $\mathbf{34 \equiv c \pmod{27}}$, e nesse caso, **c** é o resto da divisão de **34** por **27.**

Como $\mathbf{34 = 27 . 1 + 7}$ então $\mathbf{c = 7}$.

Consultando a tabela, percebemos que **7** representa **G**.

Logo **V** significa **G.**

9°) **F** → **F** corresponde ao número **6.** Logo **m** é **6.**

Então aplicando na fórmula temos:

$\mathbf{c \equiv 6 + 12 \pmod{27}}$ ou seja

$\mathbf{c \equiv 18 \pmod{27}}$.

Se $\mathbf{c \equiv 18 \pmod{27}}$ então $\mathbf{18 \equiv c \pmod{27}}$, e nesse caso, **c** é o resto da divisão de **18** por **27.**

Como $\mathbf{18 = 27 . 0 + 18}$ então $\mathbf{c = 18}$.

Consultando a tabela, percebemos que **18** representa **R**.

Logo **F** significa **R.**

10°) **T** → já verificamos que **T** corresponde a letra **E.**

11°) **V** → já verificamos que **V** corresponde a letra **G.**

12°) **C** → já verificamos que **C** corresponde a letra **O.**

Logo **XGHCOTOVFTVC** corresponde a **I S TO É G R E G O.**

Exercício

1) Decifre o seguinte código: **VIJRCEIQRFHVDUVDUEQTEDXHKVTZR** para $\mathbf{t = 10}$.

Resolução:

Decifraremos esta mensagem através da fórmula $\mathbf{c \equiv m + t \pmod{27}}$, onde queremos descobrir o valor de **c**.

1°) **V** → **V** corresponde ao número **22**. Logo **m** é **22**.

Então aplicando na fórmula temos:

$\mathbf{c \equiv 22 + 10 \pmod{27}}$ ou seja

$\mathbf{c \equiv 32 \pmod{27}}$.

Se $\mathbf{c \equiv 32 \pmod{27}}$ então $\mathbf{32 \equiv c \pmod{27}}$, e nesse caso, **c** é o resto da divisão de **32** por **27**.

Como $\mathbf{32 = 27 \cdot 1 + 5}$ então $\mathbf{c = 5}$.

Consultando a tabela, percebemos que **5** representa letra **E**.

Logo **V** significa **E**.

2°) **I** → **I** corresponde ao número **9**. Logo **m** é **9**.

Então aplicando na fórmula temos:

$\mathbf{c \equiv 9 + 10 \pmod{27}}$ ou seja

$\mathbf{c \equiv 19 \pmod{27}}$.

Se $\mathbf{c \equiv 19 \pmod{27}}$ então $\mathbf{19 \equiv c \pmod{27}}$, e nesse caso, **c** é o resto da divisão de **19** por **27**.

Como $\mathbf{19 = 27 \cdot 0 + 19}$ então $\mathbf{c = 19}$.

Consultando a tabela, percebemos que **19** representa letra **S**.

Logo **I** significa **S**.

3°) **J** → **J** corresponde ao número **10**. Logo **m** é **10**.

Então aplicando na fórmula temos:

$\mathbf{c \equiv 10 + 10 \pmod{27}}$ ou seja

$\mathbf{c \equiv 20 \pmod{27}}$.

Se **c ≡ 20 (mod 27)** então **20 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **20** por **27.**

Como **20 = 27 . 0 + 20** então **c = 20.**

Consultando a tabela, percebemos que **20** representa letra **T.**

Logo **J** significa **T.**

4°) **R → R** corresponde ao número **18.** Logo **m** é **18.**

Então aplicando na fórmula temos:

c ≡ 18 + 10 (mod 27) ou seja

c ≡ 28 (mod 27).

Se **c ≡ 28 (mod 27)** então **28 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **28** por **27.**

Como **28 = 27 . 1 + 1** então **c = 1.**

Consultando a tabela, percebemos que **1** representa letra **A.**

Logo **R** significa **A**

5°) **C → C** corresponde ao número **3.** Logo **m** é **3.**

Então aplicando na fórmula temos:

c ≡ 3 + 10 (mod 27) ou seja

c ≡ 13 (mod 27).

Se **c ≡ 13 (mod 27)** então **13 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **13** por **27.**

Como **13 = 27 . 0 + 13** então **c = 13.**

Consultando a tabela, percebemos que **13** representa letra **M.**

Logo **C** significa **M.**

6°) **E → E** corresponde ao número **5.** Logo **m** é **5.**

Então aplicando na fórmula temos:

c ≡ 5 + 10 (mod 27) ou seja

c ≡ 15 (mod 27).

Se **c ≡ 15 (mod 27)** então **15 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **15** por **27.**

Como **15 = 27 . 0 + 15** então **c = 15.**

Consultando a tabela, percebemos que **15** representa letra **O.**

Logo **E** significa **O.**

7°) **I →** já vimos que **I** significa **S.**

8°) **Q →** **Q** é representado pelo número **17.** Logo **m** é **17.**

Então aplicando na fórmula temos:

c ≡ 17 + 10 (mod 27) ou seja

c ≡ 27 (mod 27).

Se **c ≡ 27 (mod 27)** então **27 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **27** por **27.**

Como **27 = 27 . 1 + 0** então **c = 0.**

Consultando a tabela, percebemos que **0** representa um espaço (entre uma letra e outra)

Logo **Q** significa um espaço.

9°) **R →** já vimos que **R** significa **A.**

10°) **F →** **F** corresponde ao número **6.** Logo **m** é **6.**

Então aplicando na fórmula temos:

c ≡ 6 + 10 (mod 27) ou seja

c ≡ 16 (mod 27).

Se **c ≡ 16 (mod 27)** então **16 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **16** por **27.**

Como **16 = 27 . 0 + 16** então **c = 16.**

Consultando a tabela, percebemos que **16** representa letra **P.**

Logo **F** significa **P.**

11°) **H** → **H** corresponde ao número **8.** Logo **m** é **8.**

Então aplicando na fórmula temos:

c ≡ 8 + 10 (mod 27) ou seja

c ≡ 18 (mod 27).

Se **c ≡ 18 (mod 27)** então **18 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **18** por **27.**

Como **18 = 27 . 0 + 18** então **c = 18.**

Consultando a tabela, percebemos que **18** representa letra **R.**

Logo **H** significa **R.**

12°) **V** → já vimos que **V** significa **E.**

13°) **D** → **D** corresponde ao número **4.** Logo **m** é **4.**

Então aplicando na fórmula temos:

c ≡ 4 + 10 (mod 27) ou seja

c ≡ 14 (mod 27).

Se **c ≡ 14 (mod 27)** então **14 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **14** por **27.**

Como **14 = 27 . 0 + 14** então **c = 14.**

Consultando a tabela, percebemos que **14** representa letra **N.**

Logo **D** significa **N.**

14°) **U** → **U** corresponde ao número **21.** Logo **m** é **21.**

Então aplicando na fórmula temos:

c ≡ 21 + 10 (mod 27) ou seja

c ≡ 31 (mod 27).

Se **c ≡ 31 (mod 27)** então **31 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **31** por **27.**

Como **31 = 27 . 1 + 4** então **c = 4.**

Consultando a tabela, percebemos que **4** representa letra **D.**

Logo **U** significa **D.**

15°) **V** → já vimos que **V** significa **E.**

16°) **D** → já vimos que **D** significa **N.**

17°) **U** → já vimos que **U** significa **D.**

18°) **E** → já vimos que **E** significa **O.**

19°) **Q** → já vimos que **Q** significa um espaço.

20°) **T** → **T** corresponde ao número **20.** Logo **m** é **20.**

Então aplicando na fórmula temos:

c ≡ 20 + 10 (mod 27) ou seja

c ≡ 30 (mod 27).

Se **c ≡ 30 (mod 27)** então **30 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **30** por **27.**

Como **30 = 27 . 1 + 3** então **c = 3.**

Consultando a tabela, percebemos que **3** representa letra **C.**

Logo **T** significa **C.**

21°) **E** → já vimos que **E** significa **O.**

22°) **D** → já vimos que **D** significa **N.**

23°) **X** → **X** corresponde ao número **24.** Logo **m** é **24.**

Então aplicando na fórmula temos:

c ≡ 24 + 10 (mod 27) ou seja

c ≡ 34 (mod 27).

Se **c ≡ 34 (mod 27)** então **34 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **34** por **27.**

Como **34 = 27 . 1 + 7** então **c = 7.**

Consultando a tabela, percebemos que **7** representa letra **G.**

Logo **X** significa **G.**

24°) **H** → já vimos que **H** significa **R.**

25°) **K** → **K** corresponde ao número **11.** Logo **m** é **11.**

Então aplicando na fórmula temos:

c ≡ 11 + 10 (mod 27) ou seja

c ≡ 21 (mod 27).

Se **c ≡ 21 (mod 27)** então **21 ≡ c (mod 27)**, e nesse caso, **c** é o resto da divisão de **21** por **27.**

Como **21 = 27 . 0 + 21** então **c = 21.**

Consultando a tabela, percebemos que **21** representa letra **U.**

Logo **K** significa **U.**

26°) **V** → já vimos que **V** significa **E.**

27°) **D** → já vimos que **D** significa **N.**

28°) **T** → já vimos que **T** significa **C.**

29°) **Z** → **Z** corresponde ao número **26.** Logo **m** é **26.**

Então aplicando na fórmula temos:

$c \equiv 26 + 10 \pmod{27}$ ou seja

$c \equiv 36 \pmod{27}$.

Se $c \equiv 36 \pmod{27}$ então $36 \equiv c \pmod{27}$, e nesse caso, **c** é o resto da divisão de **36** por **27.**

Como $36 = 27 \cdot 1 + 9$ então $c = 9$.

Consultando a tabela, percebemos que **9** representa letra **I**.

Logo **Z** significa **I.**

30°) **R** → já vimos que **R** significa **A**.

Logo temos que:

VIJRCEIQRFHVDUVDUEQTEDXHKVDTZR

significa: **E S T A M O S A P R E N D E N D O C O N G R U Ê N C I A**

Comentário sobre a 6ª aula

Exatamente como a 4ª aula esta foi bastante divertida e interessante.

A maior dificuldade apresentada pelo alunos foi em aplicar os números na fórmula. Depois desta etapa tudo se tornava mais fácil para eles.

Foi trabalhado apenas a decodificação das mensagens, pois a codificação muitas vezes necessita da aplicação dos números inteiros negativos, o que não é muito acessível para os alunos.

7ª aula:

Continuaremos as propriedades de congruência:

2ª) Quando temos, por exemplo, o seguinte caso: se $37 \equiv 23 \pmod 2$ pois $37 - 23 = 14$ e $14 = 2 \cdot 7 + 0$, se $23 \equiv 1 \pmod 2$ pois $23 - 1 = 22$ e $22 = 2 \cdot 11 + 0$, então podemos afirmar que $37 \equiv 1 \pmod 2$. E de fato $37 - 1 = 36$ e $36 = 2.13 + 0$.

3ª) Congruência envolvendo potência:
Se, por exemplo, $5 \equiv 1 \pmod 2$ então $5^2 \equiv 1^2 \pmod 2$, $5^3 \equiv 1^3 \pmod 3$ e assim por diante.
E se, por exemplo, $5 \equiv 2 \pmod 3$ então $5^2 \equiv 2^2 \pmod 3$, $5^3 \equiv 2^3 \pmod 3$ e assim por diante.

De fato:
1) Sabemos que $5 \equiv 1 \pmod 2$ pois $5 - 1 = 4$ e $4 = 2 \cdot 2 + 0$.
Sabemos também que $5^2 = 25$ e $25 \equiv 1 \pmod 2$ pois $25 - 1 = 24$ e $24 = 2.12 + 0$
Sabemos ainda que $5^3 = 125$ e $125 \equiv 1 \pmod 2$ pois $125 - 1 = 124$ e $124 = 2 \cdot 62 + 0$

Podemos observar que: $5 \equiv 1 \pmod 2$

$25 \equiv 1 \pmod 2$

$125 \equiv 1 \pmod 2$

ou seja $5 \equiv 1 \pmod 2$

$5^2 \equiv 1 \pmod 2$

$5^3 \equiv 1 \pmod 2$

2) Sabemos que $5 \equiv 2 \pmod 3$ pois $5 - 2 = 3$ e $3 = 3.1 + 0$
Sabemos também que $5^2 = 25$ e $25 \equiv 1 \pmod 3$ pois $25 - 1 = 24$ e $24 = 3 \cdot 8 + 0$.
Sabemos ainda que $5^3 = 125$ e $125 \equiv 2 \pmod 3$ pois $125 - 2 = 123$ e $123 = 3 \cdot 41 + 0$

Pela potência em congruência temos que: $5 \equiv 2 \pmod 3$

$$5^2 \equiv 2^2 \pmod 3$$

$$5^3 \equiv 2^3 \pmod 3$$

Como $2^2 = 4$ e $4 \equiv 1 \pmod 3$, *então pela 2ª propriedade de congruência* $5^2 \equiv 1 \pmod 3$.

Como $2^3 = 8$ e $8 \equiv 2 \pmod 3$, então pela 2ª propriedade de congruência $5^3 \equiv 2 \pmod 3$

E, ambos os resultados já tinham sido obtidos anteriormente.

Exercícios

1) Ache os restos nas seguintes divisões:

a) 2^{45} por 7

Resolução:

Sabemos que $2^3 = 8$ e $8 \equiv 1 \pmod 7$, ou seja, $2^3 \equiv 1 \pmod 7$.

Como $2^{45} = (2^3)^{15}$ e $(2^3)^{15} \equiv 1^{15} \pmod 7$

Então $2^{45} \equiv 1 \pmod 7$

Logo o resto é **1.**

b) 7^{121} por 2

Resolução:

Sabemos que $7 \equiv 1 \pmod 2$, pois $7 - 1 = 6$ e $6 = 2 \cdot 3 + 0$.

Como $7^{121} \equiv 1^{121} \pmod 2$

$7^{121} \equiv 1 \pmod 2$

Logo o resto é **1.**

2) Verifique se 4^{27} é divisível por **8.**

Resolução:

Sabemos que $4^3 = 64$ e $64 \equiv 0 \pmod 8$ pois $64 - 0 = 64$ e $64 = 8 \cdot 8 + 0$.

Como $4^{27} = (4^3)^9$ e $43^9 \equiv 0^9 \pmod 8$, então $4^{27} \equiv 0 \pmod 8$

Portanto o resto da divisão de 4^{27} por **8** é **0**.

Logo 4^{27} é divisível por **8.**

Comentário sobre a 7ª aula

Os alunos apresentaram um pouco de dificuldade em relação às propriedades da potência.

Aplicar a propriedade da congruência referente a potenciação não foi a maior barreira para os alunos durante a resolução dos exercícios.

8ª aula:

Nesta aula, foi aplicado um teste com 5 (cinco) questões objetivas afim de se fazer uma avaliação com os alunos para verificar o conhecimento e a aprendizagem destes em relação ao conteúdo dado, bem como o desempenho da professora durante as aulas. Desta forma, seria possível finalmente concluir se os objetivos traçados foram ou não alcançados.

Tal teste será apresentado a seguir.

TESTE

1) Verifique se são verdadeiras ou falsas as seguintes congruências:

a) $\mathbf{187 \equiv 1 \pmod 4}$

b) $\mathbf{329 \equiv 91 \pmod{17}}$

c) $\mathbf{5 \equiv 83 \pmod 6}$

2) Será que o **46°** e o **235°** dias do ano pertencem ao mesmo dia da semana?

3) Ache os restos nas seguintes divisões:

a) $\mathbf{6^{109}}$ por **5**

b) $\mathbf{3^{30}}$ por **8**

c) $\mathbf{121^{47}}$ por **11**

4) Um professor trouxe uma certa quantidade de livros para dividir entre alguns alunos. Se o professor dividir os livros que trouxe entre **3** alunos sobram **2** livros e se ele dividir entre **5** alunos sobram **3** livros. Sabendo que o professor trouxe menos de **10** livros, pergunta-se: quantos livros ele trouxe?

5) Um bando de **5** piratas ao tentar dividir entre si, igualmente as moedas de ouro de uma arca, verifica que **3** moedas sobrariam. Na discussão que se seguiu um dos piratas foi morto; na nova tentativa de divisão, já com um pirata a menos, desta feita **2** moedas sobrariam. Nova discussão e mais um pirata é morto. Mas agora, por fim é possível dividir igualmente a fortuna entre eles. Qual o menor número de moedas que a arca poderia conter?

RESOLUÇÃO DO TESTE

1) Verifique se são verdadeiras ou falsas as seguintes congruências:

a) $187 \equiv 1 \pmod 4$

Resolução:

$187 - 1 = 186$ e **$186 = 4 \cdot 46 + 3$**

Portanto **187** não é côngruo a **1** módulo **4**.

Logo essa congruência é falsa.

b) $329 \equiv 91 \pmod{17}$

Resolução:

$329 - 91 = 238$ e **$238 = 17 \cdot 14 + 0$**

Portanto **329** é côngruo a **91** módulo **17**.

Logo essa congruência é verdadeira.

c) $5 \equiv 83 \pmod 6$

Resolução:

Se **$5 \equiv 83 \pmod 6$** então **$83 \equiv 5 \pmod 6$**

Como **$83 - 5 = 78$** e **$78 = 6 \cdot 13 + 0$**

então **83** é côngruo a **5** módulo **6** e portanto **5** é côngruo a **83** módulo **6.**

Logo essa congruência é verdadeira.

2) Será que o **46º** e o **235º** dias do ano pertencem ao mesmo dia da semana?

Resolução:

Para o **46º** e o **235º** dias do ano pertencerem ao mesmo dia da semana, eles devem ser côngruos entre si módulo **7**. Assim devemos verificar se **$235 \equiv 46 \pmod 7$**

Como **$235 - 46 = 189$** e **$189 = 7 \cdot 27 + 0$** então **235** é côngruo a **46** módulo **7.**

Logo o **46º** e o **235º** dias, pertencem ao mesmo dia da semana.

3) Ache os restos nas seguintes divisões:

a) 6^{109} por **5**

Resolução:

Sabemos que $6 \equiv 1 \pmod 5$ pois $6 - 1 = 5$ e $5 = 5 \cdot 1 + 0$

Assim $6^{109} \equiv 1^{109} \pmod 5$ ou seja $6^{109} \equiv 1 \pmod 5$

Logo o resto da divisão de 6^{109} por **5** é **1**.

b) 3^{30} por **8**

Resolução:

Sabemos que $3^2 = 9$ e $9 \equiv 1 \pmod 8$ pois $9 - 1 = 8$ e $8 = 8 \cdot 1 + 0$

Assim $3^2 \equiv 1 \pmod 8$.

Como $3^{30} \equiv (3^2)^{15}$ então $(3^2)^{15} \equiv 1^{15} \pmod 8$,

ou seja $3^{30} \equiv 1 \pmod 8$.

Logo o resto da divisão 3^{30} por **8** é **1**.

c) 121^{47} por **11**

Resolução:

Sabemos que $121 \equiv 0 \pmod{11}$ pois $121 - 0 = 121$ e $121 = 11 \cdot 11 + 0$

Assim $121^{47} \equiv 0^{47} \pmod 1$ ou seja $121^{47} \equiv 0 \pmod{11}$.

Logo o resto da divisão de 121^{47} por **11** é **0**.

4) Um professor trouxe uma certa quantidade de livros para dividir entre alguns alunos. Se o professor dividir os livros que trouxe entre **3** alunos sobram **2** livros e se ele dividir entre **5** alunos sobram **3** livros. Sabendo que o professor trouxe menos de **10** livros, pergunta-se: quantos livros ele trouxe?

Resolução:

Temos que achar um número que quando dividido por **3** dá resto **2** e quando dividido por **5** dá resto **3**. Assim, por tentativa temos:

nº. dividido por **3** com resto **2**	nº dividido por **5** com resto **3**
2	3
5	8
8	13
11	18
14	23
.	.
.	.
.	.

Logo o professor trouxe **8** livros.

5) Um bando de **5** piratas ao tentar dividir entre si, igualmente as moedas de ouro de uma arca, verifica que **3** moedas sobrariam. Na discussão que se seguiu um dos piratas foi morto; na nova tentativa de divisão, já com um pirata a menos, desta feita **2** moedas sobrariam. Nova discussão e mais um pirata é morto. Mas agora, por fim é possível dividir igualmente a fortuna entre eles. Qual o menor número de moedas que a arca poderia conter?

Resolução:

Temos que achar um número que quando dividido por **5** dá resto **3**, que quando divido por **4** dá resto **2** e quando dividido por **3** dá resto **zero**.

Assim, por tentativa ,temos:

nº. dividido 5 com resto 3	nº. dividido por 4 com resto 2	nº. dividido por 3 com resto 0
3	2	3
8	6	6
13	10	9
18	14	12
23	18	15
28	22	18
.	.	.
.	.	.
.	.	.

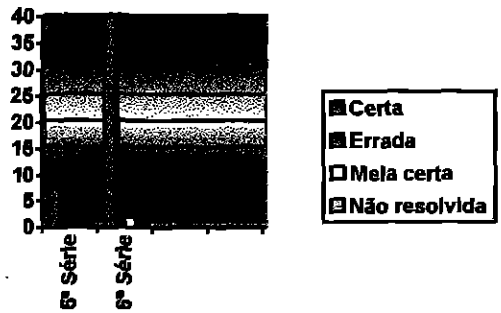
Logo o menor número de moedas que a arca poderia conter é **18**.

GRÁFICOS DO RESULTADO DO TESTE APLICADO

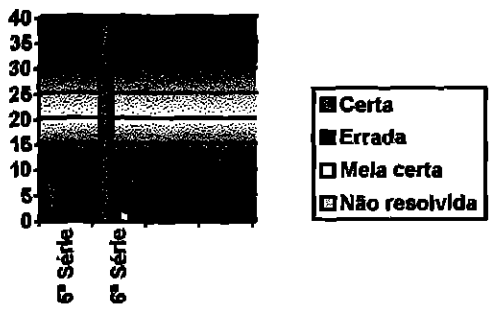
Os dados a seguir são referentes a uma turma de 5ª série com 8 (oito) alunos e uma turma de 6ª série com 42 (quarenta e dois) alunos.

1) Verifique se são verdadeiras ou falsas as seguintes congruências:

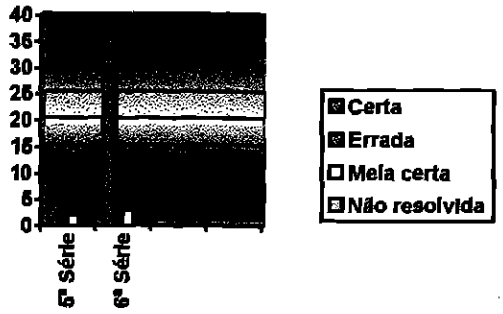
a) **$187 \equiv 1 \pmod 4$**



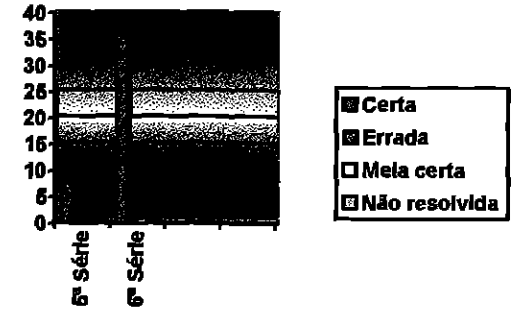
b) **$329 \equiv 91 \pmod{17}$**



c) $5 \equiv 83 \pmod 6$

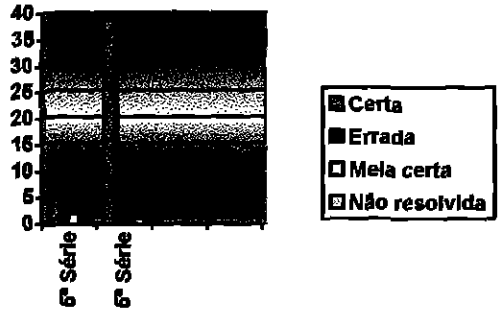


2) Será que o 46^{o} e o 235^{o} dias do ano pertencem ao mesmo dia da semana?

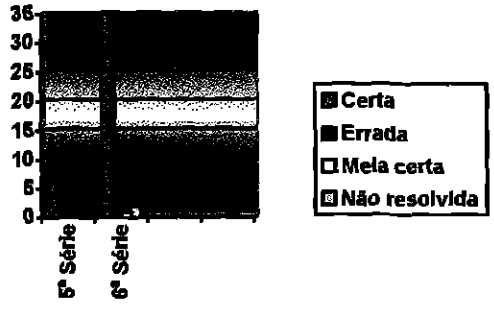


3) Ache os restos nas seguintes divisões:

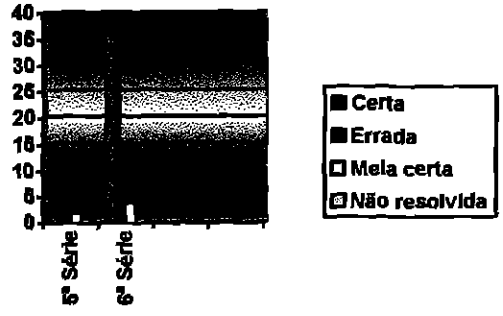
a) 6^{109} por 5



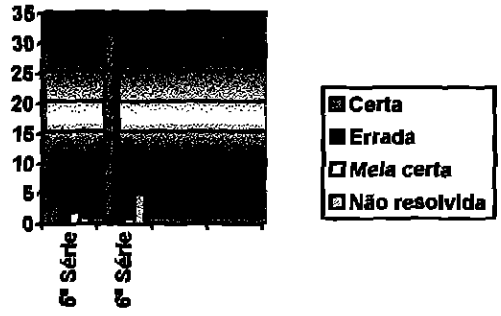
b) 3^{30} por 8



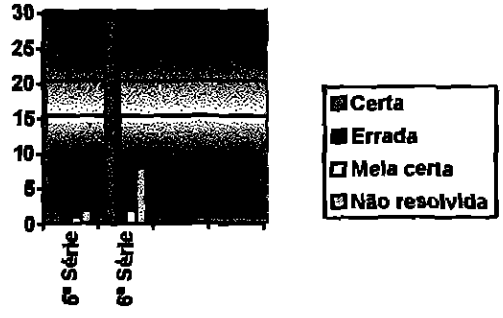
c) 121^{47} por 11



4) Um professor trouxe uma certa quantidade de livros para dividir entre alguns alunos. Se o professor dividir os livros que trouxe entre **3** alunos sobram **2** livros e se ele dividir entre **5** alunos sobram **3** livros. Sabendo que o professor trouxe menos de **10** livros, pergunta-se: quantos livros ele trouxe?



5) Um bando de **5** piratas ao tentar dividir entre si, igualmente as moedas de ouro de uma arca, verifica que **3** moedas sobrariam. Na discussão que se seguiu um dos piratas foi morto; na nova tentativa de divisão, já com um pirata a menos, desta feita **2** moedas sobrariam. Nova discussão e mais um pirata é morto. Mas agora, por fim é possível dividir igualmente a fortuna entre eles. Qual o menor número de moedas que a arca poderia conter?



Comentário sobre o teste aplicado

Os resultados dos testes correspondem ao desempenho dos alunos na sala de aula. Os maiores erros ocorreram com os problemas.

Percebe-se que os alunos apresentam dificuldade na interpretação dos mesmos. Mas isso ocorre com a maioria dos alunos e em outros conteúdos também. Quando apresenta-se problemas nos exercícios, logo surge a pergunta: O que eu faço, somo, subtraio, multiplico ou divido? Problema é um ponto em destaque que deve ser bastante trabalhado pelos professores de matemática.

Além disso, o conteúdo referente à resolução dos problemas (congruência linear) não foi trabalhado durante as aulas, mesmo porque é bastante complexo para ser aplicado. Portanto os problemas só podiam ser resolvidos por tentativa, como foi explicado durante o teste. Dessa forma era possível verificar como os alunos iriam usar seu conhecimento em relação ao algoritmo de Euclides, bem como seus elementos (divisor, dividendo, quociente e resto) para resolverem tais problemas.

Entretanto, é indispensável que o professor conheça congruência linear para assim elaborar bons problemas bem como chegar em suas resoluções.

CONCLUSÃO

Com este trabalho procurou-se mostrar que existem várias e diferentes maneiras de fazer aplicações com o algoritmo de Euclides e uma destas maneiras é com a congruência.

Os exercícios dos conteúdos matemáticos em geral são muito mecânicos, não levam o aluno a um determinado raciocínio lógico. Não existe um "porque" ou uma integração mais específica com a realidade.

Percebe-se que quando é feita tal integração, os alunos se interessam muito mais, melhoram seu rendimento e consequentemente seu aprendizado.

Foi exatamente isso que procurou-se fazer quanto à aplicação de congruência para os alunos. Tanto a definição e propriedades, como os exercícios relacionados à mesma, estavam diretamente ligados ao algoritmo de Euclides. Especialmente os exercícios atraíram muito a atenção e o interesse dos alunos, destacando-se entre tais exercícios o código secreto e o calendário.

Dessa forma, os alunos passaram a perceber a importância do algoritmo, verificando que o mesmo não serve simplesmente para tirar a prova real da divisão pelo método das chaves.

E num contexto geral, não foi difícil trabalhar congruência. Pelo contrário, os resultados obtidos foram mais positivos que o esperado.

Em se tratando de congruência, sua aplicação não se reduz apenas aquelas apresentadas neste trabalho. Existem ainda muitas outras questões que são solucionadas através da congruência e que certamente seriam temas interessantes para serem aplicadas em sala de aula.

REFERÊNCIAS BIBLIOGRÁFICAS

BOYER, Carl B.. **História da Matemática.** São Paulo: Editora Edgard Blücher, 1974.

GUNDLACH, Bernard H.. **Tópicos de história da Matemática: Números e Numerais.** São Paulo: Editora Atual, 1992.

BAUMGART, John k.. **Tópicos de história da Matemática: Álgebra**. São Paulo: Editora Atual, 1992.

DOMINGUES, Hygino H.. **Fundamentos de Aritmética.** São Paulo: Editora Atual, 1991.

HEFEZ, Abramo. **Curso de Álgebra**, volume 1. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1993.

TÁBOA, M. G. Carmem e Ribeiro, Hermano de Souza. Sobre critérios de divisibilidade. **Revista do professor de Matemática,** São Paulo, número 6, pg 21-24, 1985.

DANTE, Luiz Roberto. Restos, congruência e divisibilidade. **Revista do professor de Matemática,** São Paulo, número 10, pg 33-40, 1987.

TERADA, Routo. Criptografia e a importância das suas aplicações. **Revista do professor de Matemática**, São Paulo, número 12, pg 1-7, 1988.

GONÇALVES, Paulo Sérgio Argolo, Em que dia da semana foi proclamada a Independência do Brasil. **Revista do professor de Matemática**, São Paulo, número 15, pg 50-54,1989.

MORGADO, Augusto César. Em que dia da semana cai?. **Revista do professor de Matemática**, São Paulo, número 24, pg 25-29, 1993.