UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO

MATEMÁTICA EM REDE NACIONAL

MESTRADO PROFISSIONAL

MAYKON COSTA DE OLIVEIRA

ARITMÉTICA: CRIPTOGRAFIA E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS

CAMPO GRANDE-MS

ABRIL-2013

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO

MATEMÁTICA EM REDE NACIONAL

MESTRADO PROFISSIONAL

MAYKON COSTA DE OLIVEIRA

ARITMÉTICA: CRIPTOGRAFIA E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS

Orientadora: Prof. Drª. Elisabete Sousa Freitas

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-Graduação em Matemática em Rede Nacional do Centro de Ciências Exatas e Tecnologia CCET/UFMS, como parte dos requisitos para obtenção do título de Mestre.

CAMPO GRANDE - MS

ABRIL -2013

ARITMÉTICA: CRIPTOGRAFIA E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS

MAYKON COSTA DE OLIVEIRA

Trabalho de Conclusão de Curso submetido ao Programa de Pós-Graduação em Matemática em Rede Nacional do Centro de Ciências Exatas e Tecnologia, da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

Aprovado pela Banca Examinadora:

Profa. Dra. Elisabete Sousa Freitas (orientadora) - UFMS

Profa. Dra. Anamaria Gomide - UNICAMP

Prof. Dr. Claudemir Aniz - UFMS

CAMPO GRANDE-MS

ABRIL-2013

Dedicatória: Decifre usando a Criptografia de Cifras Afins, sendo $m = 7$ e $n = 5$.

$00 - 07 - 00 - 09 - 19 - 25$
$07 - 01 - 08 - 07$
$08 - 20 - 05 - 12 - 05 - 04 - 02 - 25$
05
$22 - 25 - 19 - 07$
$04 - 07 - 09 - 08 - 25 - 20,$
$06 - 25 - 09 - 01$
$08 - 07 - 22 - 07$
$05 - 11 - 25 - 20,$
$05-06-20-07-18-00-09-24-05-21-07-11$
07
$19 - 15 - 11 - 06 - 20 - 09 - 15$
05
$11 - 07 - 08 - 05$
$07 - 11$
$11 - 05 - 08 - 07 - 11 - 05 - 08 - 09 - 19 - 05$

Epígrafe

Sempre me pareceu estranho que todos aqueles que estudam seriamente esta ciência acabam tomados de uma espécie de paixão pela mesma. Em verdade, o que proporciona o máximo de prazer não é conhecimento e sim a aprendizagem, não é a posse, mas a aquisição, não é a presença, mas o ato de atingir a meta.

Carl Friedrich Gauss

AGRADECIMENTOS

Agradeço, primeiramente, a Aquele que merece toda graça e louvor, a Aquele que me deu sabedoria e oportunidade na matemática para chegar até aqui. Força humana eu tenho, mas a força espiritual é toda Dele. Obrigado Senhor Deus por estar ao meu lado em todos os momentos, carregando-me nos piores.

A minha mãe Vera que disse sim, ao me aceitar como filho dentro de seu ventre. Preocupada com minha educação, proporcionou-me oportunidade de me dedicar aos estudos.

A minha noiva Charlene, por estar sempre ao meu lado, incentivando-me nos momentos de desânimo e sendo compreensiva nos momentos que estive ausente.

Ao meus irmão gêmeo Jefferson que, com sua sensibilidade fraterna, incentivou-me e aconselhou-me em diversos momentos.

Ao meu irmão Cleiton que, como exemplo de irmão mais velho mostrou-me, com gestos e atitudes, que a vontade de estudar e se aperfeiçoar não tem idade.

Aos amigos que, de certa forma, auxiliaram na elaboração desse trabalho, sobretudo ao Juvenal, primeiramente pelos 18 anos de amizade e, ainda, pela revisão textual desse trabalho.

As diretoras Marilene e Maria de Fátima que demonstraram ser compreensíveis com minhas ausências nas aulas e reuniões importantes.

Aos colegas do mestrado, em especial, Helen, Ildálio e Josiane, pela grande contribuição nos estudos e trabalhos durante esse período de dedicação.

A organização estrutural do Mestrado Profissional: CAPES e PROFMAT, sem os quais o desenvolvimento desse programa não seria possível.

Ao professor coordenador Dr. Claudemir Aniz, que se dedicou aos professores e mestrandos, possibilitando o sucesso do nosso polo.

E um obrigado especial a professora orientadora Dra. Elisabete de Sousa Freitas,

que, orientou-me com doçura e experiência, sabiamente, a fim de que eu concluísse mais essa etapa de meus estudos.

Um obrigado a todos.

Resumo

O presente trabalho centra-se na aplicação da Teoria dos Números no Ensino Médio com ênfase na Aritmética Modular. Para a realização deste, antes de qualquer aplicação, foi necessária, a introdução de conceitos básicos da Teoria dos Números, a qual contempla: Divisibilidade, Números Primos, Congruência e o Pequeno Teorema de Fermat. As aplicações foram: Equações Diofantinas Lineares e Conceitos de Criptografia de César, de Cifras Afins e sistema RSA, com vistas a trazer ferramentas de cálculos e algoritmos, de modo a agilizar as resoluções de problemas, em sala de aula. A última parte do trabalho apresenta, nos exemplos citados, o uso do software Microsoft Excel.

Palavras-Chave: Aritmética. Congruência. Criptografia.

Abstract

This paper focuses on the application of Number theory in high school with emphasis on Modular Arithmetic. To accomplish this, before any application, it was required, an introduction of basic concepts of the Theory of Numbers, which includes: Divisibility, Prime Numbers, Congruence and Fermat's Little Theorem. The applications were: Linear Diophantine Equations and Concepts of Encryption Caesar, Affine Cipher and RSA system, aiming to bring new tools for calculations and algorithms in order to expedite the resolution of problems, in use in the classroom. The last part presents, in the examples cited, the use of Microsoft Excel software.

Keywords: Arithmetic. Congruence, Encryption.

Sumário

Capítulo 1

Introdução

A Teoria dos Números, de um modo geral, estuda as propriedades dos números, onde aquela que se refere aos números inteiros é denominada Teoria Elementar dos Números.

Inicialmente, apresentaremos os resultados sobre a Aritmética Modular, abordados nas diversas referências utilizadas na elaboração deste trabalho, a fim de que o professor de matemática do Ensino Médio possa, familiarizar-se e, com base no entendimento da proposta, organizar um roteiro de estudo para seus alunos. Após esse estudo, apresentaremos as aplicações da mesma no Ensino Médio: Equações Diofantinas Lineares, com a utlização do Algoritmo Euclidiano Estendido e Criptografia, área que protege as diversas comunicações atuais como, por exemplo, comunicações bancárias para transferências eletrônicas de valores e, até mesmo, comunicações pessoais via internet, para que pessoas não autorizadas não tenham acesso a dados sigilosos e importantes, com vistas a trazer novas ferramentas de cálculos, conteúdos e algoritmos em sala de aula.

O objetivo principal deste trabalho é uma proposta de material de apoio, para que professores de matemática possam utilizá-lo em seus estudos, para elaborarem um roteiro de aplicação em sala de aula e para os alunos do Ensino Médio, um instrumento de motivação para que cada vez mais se dediquem e aprofundem em seus estudos.

Os vários exemplos das aplicações aqui tratados têm como objetivo tornar ainda mais rápida e fácil sua compreensão. Encerrando, relatamos no apêndice o uso do software Microsoft Excel, que nos auxiliou nas contas das aplicações aqui apresentadas, disponível nas salas de tecnologia das escolas públicas, de forma a introduzir um recurso digital, sendo esperado o surgimento de outros que possam enriquecer o nosso trabalho.

Capítulo 2

Conceitos Básicos da Teoria dos Números

"A matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas". Carl Friedrich Gauss.

Nessa seção do trabalho, faremos um estudo dos conteúdos básicos para compreendermos a parte aritmética na resolução das Equações Diofantinas Lineares e da Criptografia, que é desenvolvida e justificada por meio da área da matemática denominada Teoria dos Números.

A Teoria dos Números também chamada de Aritmética, de um modo geral, estuda as propriedades dos números. A denominada Teoria Elementar dos Números investiga as propriedades do conjunto dos números naturais e, um pouco mais geral, dos números inteiros.

Denota-se por $\mathbb{N}$ o conjunto dos números naturais e por $\mathbb{Z}$ o conjunto dos números inteiros. Assim

$\mathbb{N}= \{0,\ 1,\ 2,\ 3,\ 4, ...\}$ e $\mathbb{Z}= \{0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3, ...\}$.

Admite-se conhecidas em $\mathbb{Z}$ as operações usuais de adição $(+)$ e multiplicação $(.)$, juntamente com a relação de ordem, $\leq$, com suas propriedades básicas, lembrando:

- *Princípio da Boa Ordenação:* Todo subconjunto não vazio dos números naturais possui um menor elemento.

2.1 Divisibilidade

Definição 1. Sejam a e b números inteiros. Diz-se que b divide a quando existe um número inteiro c tal que $a = bc$.

Usaremos a notação $b \mid a$ para indicar que b divide a. A negação será indicada por $b \nmid a$.

Quando $b \mid a$, dizemos também que b é um divisor de a ou que a é um múltiplo de b.

Exemplo 1. Tem-se que $6 \mid 30$, pois $30 = 6.5$.

Observação 1. Observamos que, se $b \neq 0$, o inteiro c nas condições da definição é único, e o denominamos *quociente* de a por b e é indicado por $c = \frac{a}{b}$.

De fato, se $a = b.c = b.c'$ então $b.(c - c') = 0$, onde $b \neq 0$, e daí $c = c'$.

Quando $b = 0$ divide a, tem-se que $a = 0$ e neste caso $0 = 0.c$, para todo c inteiro.

Assim, pela definição, $0 \mid 0$ mas $\frac{0}{0}$ é uma indeterminação.

Exemplo 2. Tem-se que $6 \mid 30$ e $5 = \frac{30}{6}$.

Proposição 1. *(Propriedades da divisibilidade em $\mathbb{Z}$).*

Sejam a, b, c, d números inteiros quaisquer. Então valem:

1. Se $b \mid a$ e $a \neq 0$ então $\mid b \mid \leq \mid a \mid$. (*Todo divisor de a é menor ou igual $a \mid a \mid$.)*

2. Se $b \mid a$ e $a \mid b$, então $a = \pm b$.

3. $1 \mid a$.

4. Se $b \mid 1$, então $b = \pm 1$.

5. $a \mid a$.

6. $a \mid 0$ (*Qualquer inteiro é divisor de zero*).

7. Se $a \mid b$ e $b \mid c$, então $a \mid c$.

8. Se $a \mid b$ e $a \mid c$, então $a \mid b + c$.

9. Se $a \mid b$, então $a \mid b.c$.

10. Se $a \mid b$ e $a \mid c$, então $a \mid m.b + n.c$, quaisquer $m,\ n \in \mathbb{Z}$.

11. $a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b$.

Demonstração. .

1. Se $b \mid a$ com $a \neq 0$, então existe um inteiro $q \neq 0$ tal que $a = b.q$, logo,

$|a| = |bq| = |b| \,.\, |q| \geq |b|$.

Portanto, $|b| \leq |a|$.

2. Suponhamos que $b \mid a$ e que $a \mid b$. Se $a = 0$ ou $b = 0$, temos que $a = b = 0$.

No caso $a,\ b \neq 0$ temos que, pelo item 1 temos que $|a| \leq |b|$ e $|b| \leq |a|$logo, $|a| = |b|$,ou seja, $a = \pm b$.

3.De fato, $1 \mid a$ pois $a = a.1$ para todo inteiro a.

4.Suponhamos que $b \mid 1$. Do item 3 temos que $1 \mid b$ para todo inteiro b. Logo pelo item 2 segue que $b = \pm 1$.

5.De fato, $a \mid a$ pois $a = 1.a$.

6.De fato, $a \mid 0$ pois $0 = a.0$.

7.Se $a \mid b$ e $b \mid c$ então existem q_1e q_2 inteiros, tais que $b = a.q_1$ e $c = b.q_2$. Substituindo a primeira na segunda obtemos, $c = a.(q_1.q_2)$, portanto $a \mid c$.

8. Se $a \mid b$ e $a \mid c$ então existem q_1 e $q_2$inteiros tais que $b = a.q_1$ e $c = a.q_2$. Somando as duas equações temos, $b + c = a.(q_1 + q_2)$. Portanto $a \mid b + c$.

9. Se $a \mid b$ então existe um número inteiro q tal que, $b = a.q$. Multiplicando a equação por um inteiro c temos que, $bc = a.(qc)$. Portanto $a \mid bc$.

10. Se $a \mid b$ e $a \mid c$ temos pelo item anterior que $a \mid bm$ e $a \mid cn$ para quaisquer inteiros m e n. Logo, pelo item 8 segue que $a \mid bm + cn$.

11.

$a \mid b \iff b = aq,\ q \in \mathbb{Z} \iff b = (-a).(-q),\ -q \in \mathbb{Z} \iff -b = a.(-q),\ q \in \mathbb{Z} \iff$

$\iff -q \in \mathbb{Z} \iff -b = (-a).q,\ -q \in \mathbb{Z} \iff -b = (-a).q,\ q \in \mathbb{Z}$ □

Teorema 1. *Algoritmo da Divisão.*

Sejam $a,\ b \in \mathbb{Z}$ com $b > 0$. Então existem inteiros q e r únicos, tais que $a = b.q + r$ e $0 \leq r < b$.

Demonstração. Primeiramente vamos mostrar a existência dos números q e r no caso em que $a \in \mathbb{N}$.

Seja a um número natural. Considere o conjunto:

$S = \{a - b.x$, onde $x \in \mathbb{N}$ e $a - b.x \geq 0\}$

Note que $S \subset \mathbb{N}$ e que $S \neq \emptyset$, pois $a = a - b.0 \geq 0$. Assim, como S é um subconjunto não vazio de $\mathbb{N}$ pode-se afirmar, em virtude do Princípio da Boa Ordenação, que S possui um menor elemento. Vamos denotá-lo por r. Como $r \in S$, existe um natural x tal que $r = a - b.x$, chamando $x = q$, temos que:

$$a = b.q + r$$

Como $r \in S$, tem-se imediatamente $r \geq 0$. Agora, supõe por absurdo que $r \geq b$. Segue-se desta suposição que $r - b \geq 0$.

Assim, como $r = a - bq \iff r - b = a - bq - b \iff r - b = a - b.(q - 1) \in S$. Observe agora que $r - b$ é menor que r, um absurdo, pois r é o menor elemento de S, logo $r < b$.

Portanto, no caso $a,\ b \in \mathbb{N}$ com $b > 0$ existem q e r naturais com $0 \leq r < b$.

Agora consideremos o caso $a < 0$ e $b > 0$. Temos então que $-a \in \mathbb{N}$ e daí existem $q',\ r' \in \mathbb{N}$ tais que $-a = b.q' + r'$ e $0 \leq r' < b$. Segue que $+a = b.(-q') - r' = b.(-q') - b + b - r'$.

$a = b.(-q' - 1) + b - r'$ onde $0 \leq b - r' < b$. Logo, basta tomar $q = -q' - 1$ e $r = b - r'$, ou seja,

$a = bq + r$ onde $0 \leq r < b$ para $a < 0$ e $b > 0$.

Vamos mostrar agora a unicidade.

Suponha que existam $q^{'}$ e $r^{'}$ inteiros tais que $a = b.q^{'} + r^{'}$ com $0 \leq r^{'} < b$.

Afirmação: $0 \leq |r' - r| < b$.

De fato, como $0 \leq r < b$, obtém-se multiplicando esta desigualdade por (-1):

$-b < -r \leq 0$. Temos então quatro desigualdades:

$$\begin{array}{ll} 0 \leq r^{'} & r^{'} < b \\ -b < -r & -r \leq 0 \end{array}$$

Somando os termos das desigualdades obtemos:

$0 - b < r^{'} - r$ e $r^{'} - r < b$

Das duas desigualdades tiramos respectivamente: $-(r^{'} - r) < b$ e $r^{'} - r < b$, o que pode ser escrito como $\left|r^{'} - r\right| < b$.

Como $a = bq + r$ e $a = bq^{'} + r^{'}$, segue que:

$$bq^{'} + r^{'} = bq + r \Longleftrightarrow r^{'} - r = b.(q^{'} - q).$$

Dai $|r' - r| = b.\,|q' - q| < b$, donde $0 \leq |q' - q| < 1$.

Portanto $q' = q$ e $r' = r$. □

Exemplo 3. Determine q e r nos itens abaixo:

(i) $a = 18$ e $b = 4$;

$18 = 4.4 + 2$, onde $q = 4$ e $r = 2$.

(ii) $a = 37$ $b = 12$;

$37 = 12.3 + 1$, onde $q = 3$ e $r = 1$.

(iii) $a = -20$ e $b = 3$;

$20 = 3.6 + 2$ multipique por (-1)

$(-20) = 3.(-6) - 2$. Somando $+3 - 3$ no segundo membro temos que:

$(-20) = 3.(-6) - 2 + 3 - 3 = 3.(-6 - 1) + 1 = 3.(-7) + 1$ onde $q = -7$ e $r = 1$.

2.2 Máximo Divisor Comum

Seja a um número inteiro. Indicaremos por $D(a)$ o conjunto dos divisores de a. Por exemplo,

$$D(18) = \{-1,\ 1,\ -2,\ 2,\ -3,\ 3, -6,\ 6,\ -9,\ 9,\ -18,\ 18\}.$$

Observamos que para qualquer inteiro $a \neq 0$, tem-se que $D(a)$ é finito.

Definição 2. Um inteiro c diz-se um divisor comum de a e b se $c \mid a$ e $c \mid b$. Se a e b não são simultaneamente nulos, o conjunto $D(a,\ b)$ de todos os divisores comuns de a e b é finito, de fato, $D(a,\ b) = D(a) \cap D(b)$, onde pelo menos um dos conjuntos é finito.

Definição 3. Sejam a e b inteiros, não simultaneamentes nulos. Chama-se máximo divisor comum de a e b, indicado por $mdc(a,\ b)$, o maior de seus divisores comuns. Assim,

$$mdc(a,\ b) = max\ D(a,\ b)$$

Observe que como $a \neq 0$ ou $b \neq 0$, $D(a,\ b)$ é finito e assim sempre possui um maior elemento e $mdc(a,\ b) \geq 1$

Exemplo 4. Considere $a = 18$ e $b = 12$. Tem-se que

$D(18) = \{-1,\ 1,\ -2,\ 2,\ -3,\ 3,\ ,-6,\ 6,\ -9,\ 9,\ -18,\ 18\}$

$D(12) = \{-1,\ 1,\ -2,\ 2,\ -3,\ 3,\ -4,\ 4,\ -6,\ 6,\ -12,\ 12\}$

$D(18,\ 12) = \{-1,\ 1,\ -2,\ 2,\ -3,\ 3,\ -6,\ 6\}$

Portanto $mdc\,(18,\ 12) = 6$.

Proposição 2. *Sejam $a = b.q + r$, onde a, b, q, r são inteiros. Então $mdc(a,\ b) = mdc(b,\ r)$.*

Demonstração. Basta mostrar que os divisores comuns entre a e b são os mesmos divisores comuns entre b e r.

Suponha que $d \mid a$ e $d \mid b$. Segue daí que $d \mid a - q.b = r$. Portanto um divisor comum de a e b também é divisor comum de b e r.

Por outro lado, suponha $d \mid b$ e $d \mid r$. Segue daí que $d \mid b.q + r = a$. Portanto um divisor comum de b e r também é um divisor comum de a e b. □

Definição 4. Dois números inteiros a e b chamam-se relativamente primos entre si, ou apenas, primos entre si, se $mdc\,(a,\ b) = 1$.

Exemplo 5. Os números 35 e 18 são primos entre si, pois:

$D(35) = \{-1,\ 1,\ -5\,5,\ -7,\ 7,\ -35,\ 35\}$

$D(18) = \{-1,\ 1,\ -2,\ 2,\ -3,\ 3,\ ,-6,\ 6,\ -9,\ 9,\ -18,\ 18\}$

$D(35,\ 18) = \{-1,\ 1\}$

Portanto $mdc\,(35,\ 18) = 1$.

2.3 Algoritmo Euclidiano

Sejam $a,\ b\ \in \mathbb{N}$ não simultaneamente nulos. Aplicando sucessivamente a divisão euclidiana tem-se que:

$a = b.q_0 + r_1,\ 0 \leq r_1 < b$

$b = r_1.q_1 + r_2,\ 0 \leq r_2 < r_1$

$r_1 = r_2.q_2 + r_3,\ 0 \leq r_3 < r_2$

$\vdots$

$r_k = r_{k+1}.q_{k+1} + r_{k+2},\ 0 \leq r_{k+2} < r_{k+1}$

$\vdots$

Observando que $0 \leq \ldots\ldots < r_3 < r_2 < r_1$ (sequências decrescente de números naturais), considere o primeiro s tal que $r_{s+1} = 0$. Usando a Proposição 2 temos que:

$$mdc\ (a,\ b) = mdc\ (b,\ r_1) = mdc\ (r_1,\ r_2) = \ldots\ldots = mdc\ (r_s,\ r_{s+1}) = r_s$$

.

As divisões sucessivas do Algoritmo Euclidiano costumam ser representadas do seguinte modo:

	q_0	q_1	q_2	.	.	q_{s-2}	q_{s-1}	q_s
a	b	r_1	r_2	.	.	r_{s-2}	r_{s-1}	r_s
r_1	r_2	r_3	r_4	.	.	r_s	0	

Sem perda de generalidade, podemos supor que $a \geq b$.

Exemplo 6. Vamos aplicar o Algoritmo de Euclides para determinar o $mdc\ (360,\ 126)$:

	1	6	$\leftarrow$	*quocientes*
126	108	18		
18	0		$\leftarrow$	*restos*

Assim $mdc\ (360,\ 126) = 18$.

Exemplo 7. Calcule $mdc\ (32,\ 12)$.

	2	1	2
32	12	8	4
8	4	0	

Logo $mdc\ (32,\ 12) = 4$.

2.4 Algoritmo Euclidiano Estendido

O Algoritmo Euclidiano pode ser estendido para provar que existem inteiros x e y tais que $mdc\ (a,\ b) = ax + by$ (Bézout).

A ideia do Algoritmo é expressar cada resto r_1, obtido na sequência de divisões do Algoritmo Euclidiano, em função de a e b, e obter daí $mdc\ (a,\ b) = r_s = ax + by$.

Por exemplo, como $a = q_0 b + r_1$ obtém-se $r_1 = a + b.(-q_0)$.Continuando,

$r_2 = b - q_1.r_1 = b - q_1.(a + b.(-q_0)) = a(-q_1) + b(1 + q_0 q_1)$,e assim por diante.

Observe que, se na primeira divisão $r_1 = 0$, teremos $mdc\ (a,\ b) = r_0 = b$ e neste caso $mdc\ (a,\ b) = r_0 = b = 0.a + 1.b$.

Escrevendo a lista completa das divisões, ao lado de cada equação colocamos as expressões dos restos r_i, onde x_i e y_i são inteiros a determinar.

$$\begin{array}{rcccrcl}
a & = & bq_0 + r_1 & \text{e} & r_1 & = & ax_1 + by_1 \\
b & = & r_1 q_1 + r_2 & \text{e} & r_2 & = & ax_2 + by_2 \\
r_1 & = & r_2 q_2 + r_3 & \text{e} & r_3 & = & ax_3 + by_3 \\
r_2 & = & r_3 q_3 + r_4 & \text{e} & r_4 & = & ax_4 + by_4 \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \\
r_{s-2} & = & r_{s-1} q_{s-1} + r_s & \text{e} & r_s & = & ax_s + by_s \\
r_{s-1} & = & r_s q_s + r_{s+1} = r_s q_s + 0 & & & &
\end{array}$$

Vamos colocar as informações acima em uma tabela, onde acrescentamos duas

linhas no início. Essas linhas são necessárias para o início do procedimento.

restos	quocientes	x	y
a	$*$	x_{-1}	y_{-1}
b	$*$	x_0	y_0
r_1	q_0	x_1	y_1
r_2	q_1	x_2	y_2
r_3	q_2	x_3	y_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{s-2}	q_{s-3}	x_{s-2}	y_{s-2}
r_{s-1}	q_{s-2}	x_{s-1}	y_{s-1}
r_s	q_{s-1}	x_s	y_s

As duas primeiras colunas são preenchidas usando o Algoritmo de Euclides e agora vamos descobrir como preencher as duas últimas.

Vamos supor que a tabela foi preenchida até a $(j-1)$ $-$*ésima linha.* Escrevemos as linhas de ordem $(j-2)$, $(j-1)$ e j na tabela abaixo.

restos	quocientes	x	y
r_{j-2}	q_{j-3}	x_{j-2}	y_{j-2}
r_{j-1}	q_{j-2}	x_{j-1}	y_{j-1}
r_j	q_{j-1}	x_j	y_j

Onde tem-se que

$r_{j-2} = r_{j-1}q_{j-1} + r_j$

$r_{j-2} = ax_{j-2} + by_{j-2}$

$r_{j-1} = ax_{x-1} + by_{y-1}$,

daí obtém-se que

$r_j = r_{j-2} - r_{j-1}q_{j-1} = ax_{j-2} + by_{j-2} - q_{j-1}.(ax_{j-1} + by_{j-1})$,

donde

$r_j = a.(x_{j-2} - q_{j-1}x_{j-1}) + b.(y_{j-2} - q_{j-1}y_{j-1})$

Assim,

$x_j = x_{j-2} - q_{j-1}x_{j-1}$ e $y_j = y_{j-2} - q_{j-1}y_{j-1}$

Portanto para preencher qualquer linha da tabela, basta conhecer as duas linhas anteriores a ela.

Para iniciar o procedimento basta observar que

$$x_{-1} = 1,\ y_{-1} = 0,\ x_0 = 0\ e\ y_0 = 1$$

Assim, obtemos no final do processo, $mdc\ (a,\ b) = r_s = a.x + b.y$, onde $x = x_s$ e $y = y_s$.

Portanto, fica provada o seguinte Teorema:

Teorema 2. *(Teorema de Bézout)*

Se $d = mdc\ (a,\ b)$ então existem x e y inteiros, de maneira que $a.x + b.y = d$.

Exemplo 8. Determine dois inteiros x e y tais que $41x + 12y = mdc\ (41,\ 12)$.

Aplicando o Algoritmo Euclidiano temos:

	3	2	2	2
41	12	5	2	1
5	2	1	0	

Logo, $mdc\ (41,\ 12) = 1$.

Assim, devemos determinar os inteiros x e y tais que $41x + 12y = 1$.

Usando o Algoritmo Euclidiano Estendido temos:

restos	quociente	x	y
41	$*$	1	0
12	$*$	0	1
5	3	1	-3
2	2	-2	7
1	2	5	-17

Logo, $x = 5$ e $y = -17$.

Exemplo 9. Sabe-se que $mdc\ (24,\ 9) = 3$. Determine os inteiros x e y tais que $24x + 9y = 3$.

Primeiramente, aplica-se o Algoritmo Euclidiano:

	2	1	2
24	9	6	3
6	3	0	

Logo, usando o Algoritmo Euclidiano Estendido temos o seguinte:

restos	quocientes	x	y
24	$*$	1	0
9	$*$	0	1
6	2	1	-2
3	1	-1	3

Logo, $x = -1$ e $y = 3$. Observe a verificação:

$24.(-1) + 9.3 = -24 + 27 = 3$.

Proposição 3. *Dois números inteiros a e b são primos entre si se, e somente se, existem inteiros r e s tais que $a.r + b.s = 1$.*

Demonstração. Sejam a e b inteiros primos entre si. Pelo Teorema de Bezout existem r e s inteiros tais que $a.r + b.s = 1$.

Por outro lado, suponha que existam $r,\ s \in \mathbb{Z}$ tais que $a.r + b.s = 1$ e considere $d = mdc\ (a,\ b)$, como $d \mid a$ e $d \mid b$ temos que $d \mid a.r + b.s = 1$. Portanto $d = 1$. □

Corolário 1. *Sejam a e b inteiros. Se $d = mdc\,(a,\ b)$ então $mdc\,(\frac{a}{d},\ \frac{b}{d}) = 1$.*

Demonstração. Como $mdc\,(a,\ b) = d$, temos pelo Teorema de Bézout, que existem inteiros x e y tais que $ax + by = d$. Dividindo essa equação por d segue que $\frac{ax}{d} + \frac{by}{d} = 1$, ou seja, existem inteiros x e y tais que $\frac{a}{d}.x + \frac{b}{d}.y = 1$, portanto $mdc\,(\frac{a}{d},\ \frac{b}{d}) = 1$. □

Proposição 4. *Seja $a,\ b$ e c inteiros tal que $a \neq 0$. Se $a \mid bc$ e $mdc\,(a,\ b) = 1$ então $a \mid c$.*

Demonstração. Como $mdc\,(a,\ b) = 1$, existem inteiros x e y tais que $a.x + b.y = 1$. Multiplicando essa equação por c temos que:

$axc + byc = c$. Como $a \mid axc$ e $a \mid bcy$ conluímos que

$a \mid axc + bcy$, ou seja, $a \mid c$. □

Proposição 5. *Sejam $a,\ b,\ c$ inteiros tais que a e b são não nulos. Se $a \mid c$ e $b \mid c$ e $mdc\,(a,\ b) = 1$ então $a.b \mid c$.*

Demonstração. Temos por hipótese que:

$a \mid c$, então existe um inteiro $k_1$tal que $c = a.k_1$ (1);

$b \mid c$, então existe um inteiro k_2 tal que $c = b.k_2$ (2);

$mdc\,(a,\ b) = 1$, então existem inteiros x e y tais que $ax + by = 1$ (3);

Multiplicando a equação (3) por c obtemos $axc + byc = c$ (4);

Substituindo (1) e (2) na equação (4) obtemos que $a.x.b.k_2 + b.y.a.k_1 = c$, ou seja, $a.b(x.k_2 + y.k_1) = c$.

Como $x.k_2 + y.k_1$é inteiro, concluímos que $a.b \mid c$. □

2.5 Números Primos

> "*Na verdade, os números primos, que desempenham um papel importante em vários ramos na Matemática, são como o hidrogênio e o oxigênio do mundo dos números, eles são os átomos da Matemática".*
>
> Marcus du Saltoy

Definição 5. Seja p um número natural. Dizemos que p é primo, se:

- $p > 1$;
- Possuir exatamente dois divisores positivos, 1 e p.

Os números naturais maiores do que 1 não primos, serão denominados *números compostos*, o que significa que possuem mais do que dois divisores positivos.

Veja que o número 1 não é considerado primo e nem composto, pois ele possui apenas um divisor positivo, 1, ou seja, ele mesmo.

Logo, para determinarmos se um número é primo ou não, basta encontrar seu conjunto de divisores positivos.

$D(2) = \{1,\ 2\} \Longrightarrow 2$ *é primo*

$D(3) = \{1,\ 3\} \Longrightarrow 3$ *é primo*

$D(4) = \{1,\ 2,\ 4\} \Longrightarrow 4$ *é composto*

$D(5) = \{1,\ 5\} \Longrightarrow 5$ *é primo*

$D(6) = \{1,\ 2,\ 3,\ 6\} \Longrightarrow 6$ *é composto*

Lema 1. *Sejam p e q números primos e a um inteiro qualquer. Temos que:*

(a) Se $p \mid q$ então $p = q$.

(*b*) *Se* $p \nmid a$ *então* $mdc\ (p,\ a) = 1$.

Demonstração. .

(a) Como q é primo, por hipótese, seus únicos divisores positivos são 1, q. Como $p \mid q$ e $p \neq 1$ temos que $p = q$.

(b) Seja $d = mdc\ (p,\ a)$. Segue que $d \mid p$ e $d \mid a$. Como p é primo temos que $d = 1$ ou $d = p$. Assim, concluímos que $d = 1$ pois $p \nmid a$. □

Proposição 6. *Propriedade Fundamental dos Números Primos*

Se p *é um número primo e* $a,\ b \in \mathbb{Z}$, *então*:

$$p \mid ab \implies p \mid a \text{ ou } p \mid b.$$

Demonstração. Suponhamos que $p \nmid a$. Então pelo Lema 1 item b, $mdc\ (p,\ a) = 1$ e daí usando a Proposição 4 segue que $p \mid b$. □

Proposição 7. *O menor divisor maior do que* 1, *de qualquer natural* $n \neq 0$ *é necessariamente um número primo.*

Demonstração. Sejam $n \in \mathbb{N}$, $n \neq 0$ e d o menor divisor, maior do que 1, de n. Se d fosse composto, então teríamos um divisor d' tal que $1 < d' < d$. Dai $d' \mid d$ e $d \mid n$. Assim, teríamos $d' \mid n$ o que contraria a escolha de d. □

Teorema 3. *Existem infinitos números primos.*

Antes de provarmos o Teorema 3, vamos esquematizar como Euclides pode ter chegado a essa conclusão.

Considere a lista dos cinco primeiros primos, 2, 3, 5, 7, 11. Multilplicando-os obtemos o número 2310. Adicionando 1 a esse número, teremos 2311. Como 2311 é primo, está fora da nossa lista de primos.

Demonstração. Suponhamos, por absurdo, que exista um número finito de primos. Vamos indicar por

$$L = \{p_1,\ p_2,\ .....,\ p_k\}$$

o conjunto de todos os primos. Considere o número n tal que

$n = p_1.p_2.....p_k + 1.$

Considere p, o menor divisor positivo de n, maior do que 1. Temos que, p é primo e $n = p.q$, com $q \in \mathbb{Z}$. Segue que,

$p_1.p_2.....p_k + 1 = p.q$

$1 = p.q - p_1.p_2.....p_k$

Como p pertence a L, pois p é primo, existe $1 \leq i \leq k$ tal que $p = p_i$.

$1 = p_i.q - p_1.p_2.....p_k = p_i.t$, com $t \in \mathbb{Z}$,

que significa $p_i \mid 1$, chegando a uma contradição. Portanto a nossa suposição de que existe um número finito de primos está errada, ou seja, existem infinitos números primos. □

2.5.1 Crivo de Eratóstenes

O Crivo de Eratóstenes é um algoritmo manual bastante simples para achar números primos menores que um número dado, embora se torne muito lento para números grandes. Funciona como uma peneira, que separa os números primos dos números compostos e é baseado no seguinte resultado:

Proposição 8. *Seja n um número natural $n \neq 0$. Se n é um número composto e p o menor divisor, maior do que 1, de n então p é primo e $p^2 \leq n$.*

Demonstração. Já sabemos que p é primo e como $p \mid n$ existe um natural q tal que $n = p.q$. Como n é composto temos que $p \leq q$ e daí

$n = p.q \geq p.p = p^2$

$n \geq p^2$. □

Observação 2. Isso quer dizer que, para determinar se um certo número n é composto, devemos encontrar algum fator primo p tal que $p^2 \leq n$.

Exemplo 10. Mostrar que o número 221 é composto.

Como $15^2 > 221$, devemos testar qual dos números primos menores do que 14 é fator de 221.

De fato, 13 é divisor de 221, logo, 221 é um número composto.

Veja um outro exemplo para determinar que um certo número inteiro positvo é primo.

Exemplo 11. O número 97 é primo ou composto?

Como $10^2 > 90$, devemos testar qual dos números primos 2, 3, 5, 7 é divisor de 97. Temos que:

2 não é divisor de 97.

3 não é divisor de 97.

5 não é divisor de 97.

7 não é divisor de 97.

Portanto, pela proposição 8, 97 é um número primo.

Eratóstenes usou esse resultado para descobrir todos os números primos menores que um número inteiro n dado. O procedimento é o seguinte:

- Devemos inicialmente escrever uma sequência de números do número 2 até o número n;
- Circulamos o número 2, pois ele é primo. Após, riscamos todos os números múltiplos de 2;

- Como $2^2 = 4$, os números menores que 4 não riscados são primos, no caso, o número 3. Risque todos os números múltiplos de 3;
- Como $3^2 = 9$, os números menores que 9 não riscados são primos, no caso, 5 e 7;
- Repete-se esse raciocínio até atingirmos um primo p tal que $p^2 > n$.

Exemplo 12. Construa o Crivo de Eratóstenes para determinar a sequência dos números primos até 100;

Basta construir uma tabela com os números de 2 até 100. Após, utilizar a ideia de riscar os múltiplos dos números primos, como o procedimento acima, no nosso exemplo, vamos marcar de vermelho os números primos e de azul os seus respectivos múltiplos. Observe:

	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	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Logo, os números primos menores que 100 são:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97.

2.6 Congruência Módulo n

Exemplo 13. Monte uma tabela de números inteiros positivos, e analise os restos deixados na divisão por 4.

números $\Longrightarrow$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
restos $\Longrightarrow$	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3

Nesse exemplo, percebe-se que os restos de uma divisão por 4 se comportam de uma maneira periódica, eles variam entre os números 0, 1, 2, 3, sempre em cículos.

Definição 6. Sejam $a,\ b,\ n\ \in\ \mathbb{Z}$ tal que $n > 0$. Dois números a e b serão congruentes módulo n se, e somente se, a e b possuir o mesmo resto na divisão por n. Denotaremos por $a\ \equiv\ b\ (mod\ n)$.

Observação 3. Quando a e b não são congruentes módulo n, usamos a notação

$$a\ \not\equiv\ b\ (mod\ n).$$

Exemplo 14. Justifique a congruência ou incongruência dos números abaixo:

- $15\ \equiv 7\ (mod\ 4)$

De fato, 15 e 7 deixam o mesmo resto 3 na divisão por 4.

- $78\ \equiv\ 28\ (mod\ 10)$

De fato, 78 e 28 deixam o mesmo resto na divisão por 10, no caso, resto 8.

- $34\ \not\equiv\ 16\ (mod\ 5)$

De fato, 34 deixa resto 4 na divisão por 5, enquanto 16 deixa resto 1, logo restos diferentes.

Proposição 9. *Sejam dados os números $a,\ b,\ n\ \in\ \mathbb{Z}$ tal que $n > 0$.*

Dois números a e b serão congruentes módulo n se, e somente se, $n \mid a - b$.

Demonstração.

$\Longrightarrow$)Se a e b são congruentes módulo n então $n \mid a - b$.

Como a e b são congruentes módulo n, então possuem o mesmo resto na divisão por n. Isso quer dizer que existem q_1 e q_2 inteiros tais que

$$a = n.q_1 + r, \text{ com } 0 \leq r < n \text{ e } b = n.q_2 + r, \text{ com } 0 \leq r < n.$$

Assim

$$a - b = n.(q_1 - q_2) + (r - r) = n.(q_1 - q_2).$$

Como $q_1 - q_2$ é inteiro então $n \mid a - b$.

$\Longleftarrow$) Se $n \mid a - b$ então a e b são congruentes módulo n.

Dividindo a e b por n, temos pelo Algoritmo da Divisão, que existem únicos inteiros $q_1,\ q_2,\ r_1,\ r_2$tais que:

$a = n.q_1 + r_1$, com $0 \leq r_1 < n$ (1)

$b = n.q_2 + r_2$,com $0 \leq r_2 < n$ (2)

Subtraindo (1) de (2) temos:

$a - b = n.(q_1 - q_2) + (r_1 - r_2)$, onde $0 < |r_1 - r_2| < n$.

Como $n \mid a - b$, segue que $n \mid r_1 - r_2$ e daí $r_1 = r_2$.

Portanto, a e b deixam o mesmo resto na divisão por n. □

Observação 4. Essa proposição pode ser escrita como:

$$a \equiv b\ (mod\ n) \Longleftrightarrow n \mid a - b.$$

Exemplo 15. Justifique a congruência dos números abaixo:

- $24 \equiv 4\ (mod\ 5)$.

De fato, $5 \mid 24 - 4 = 20$.

- $146 \equiv 50\ (mod\ 12)$.

De fato, $12 \mid 146 - 50 = 96$.

- $-52 \equiv 4 \ (mod\ 2)$.

De fato, $2 \mid -52 - 4 = -58$.

Proposição 10. *Propriedades da Congruência*

Sejam $a,\ b,\ c,\ d,\ n \in \mathbb{Z}$ *com* $n > 0$. *Temos:*

(1) $a \equiv a \ (mod\ n)$;

(2) Se $a \equiv b \ (mod\ n)$ então $b \equiv a \ (mod\ n)$;

(3) Se $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$ então $a \equiv c \ (mod\ n)$;

(4) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$ então $a + c \equiv b + d \ (mod\ n)$;

(5) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$ então $a.c \equiv b.d \ (mod\ n)$;

(6) $a + c \equiv b + c \ (mod\ n) \iff a \equiv b \ (mod\ n)$;

(7) Sejam $a \equiv b \ (mod\ n)$ e k um inteiro positivo qualquer então $a^k \equiv b^k \ (mod\ n)$;

(8) *Se* $ab \equiv ac \ (mod\ n)$ *e* $mdc\ (a,\ n) = 1$ *então* $b \equiv c \ (mod\ n)$;

Demonstração. Vamos mostrar apenas as propriedades 1, 4, 7 e 8. As demais seguem também das propriedades da divisibilidade.

1. De fato, $n \mid a - a = 0$.

4. Suponhamos que $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$. Então $n \mid b - a$ e $n \mid d - c$. Assim, $n \mid b - a + (d - c)$, ou seja, $n \mid b + d - (a + c)$. Portanto $a + c \equiv b + d \ (mod\ n)$.

7.Suponhamos que $a \equiv b \ (mod\ n)$. Aplicando a propriedade 5 dessa mesma proposição $k - 1$ vezes, temos:

$$k \text{ congruências } a \equiv b \ (mod\ n) \begin{cases} a \equiv b \ (mod\ n) \\ a \equiv b \ (mod\ n) \\ a \equiv b \ (mod\ n) \\ \vdots \\ a \equiv b \ (mod\ n) \end{cases} \Longrightarrow a^k \equiv b^k \ (mod\ n).$$

8. Suponhamos que $ab \equiv ac \ (mod\ n)$. Segue que

$$n \mid ab - ac = a.(b - c).$$

Como $mdc\ (a,\ n) = 1$ temos $n \mid b - c$. Portanto $b \equiv c \ (mod\ n)$. □

Exemplo 16. Determine o resto da divisão de 37^{88} por 4.

Veja que $37 \equiv 1 \ (mod\ 4)$. Assim, usando a propriedade 8, segue que:

$37^{88} \equiv 1^{88} \ (mod\ 4)$. Como $1^{88} = 1$ então temos que:

$37^{88} \equiv 1 \ (mod\ 4)$. Portanto o resto será 1.

Exemplo 17. Encontre o resto módulo 5 do número inteiro -14.

Queremos achar um número inteiro r, $0 \leq r < 5$ tal que $-14 \equiv r \ (mod\ 5)$.

$14 = 5.2 + 4$ (basta efetuar a divisão de 14 por 5). Multiplique a equação por (-1).

$-14 = 5.(-2) - 4$, ou seja, $-14 \equiv -4 \ (mod\ 5)$, mas -4 não é o resto módulo 5 pois é negativo. Porém, como $5 \equiv 0 \ (mod\ 5)$ segue que:

$-14 + 5 \equiv -4 + 5 \ (mod\ 5)$, ou seja, $-14 + 0 \equiv -4 + 5 \ (mod\ 5)$.

$-14 \equiv 1 \ (mod\ 5)$.

Exemplo 18. Determine o resto de -54 na divisão por 7.

Sabemos que $54 \equiv 5\ (mod\ 7)$. Multiplicando por (-1) obtemos $-54 \equiv -5\ (mod\ 7)$. Como $7 \equiv 0\ (mod\ 7)$ segue que

$$-54 \equiv -5 + 7 \equiv 2\ (mod\ 7)$$

2.6.1 Inverso Multiplicativo Módulo n

Definição 7. Dados dois números inteiros a e n com $(a,\ n) = 1$, chama-se inverso de a módulo n a qualquer um dos inteiros x tais que

$$a.x \equiv 1\ (mod\ n).$$

Observação 5. Se $(a,\ n) = 1$ existem x e y inteiros tais que $a.x + n.y = 1$. Resulta daí que $a.x \equiv 1\ (mod\ n)$.

Exemplo 19. Determine x tal que $41.x \equiv 1\ (mod\ 12)$.

Do exemplo 8 segue que $41.5 + 12.(-17) = 1$. Assim $41.5 \equiv 1\ (mod\ 12)$.

2.6.2 Congruência e Algoritmo da Divisão

Seja a um inteiro qualquer e n um inteiro positivo. Dividindo a por n, existem inteiros únicos q e r tais que:

$a = n.q + r$, com $0 \leq r < n$. Como $n.q \equiv 0\ (mod\ n)$ temos que $a \equiv r\ (mod\ n)$ onde $r \in \{0,\ 1,\ 2,\ .....,\ n-1\}$, que são os possíveis restos na divisão por n.

Além disso, se $i,\ j \in \{\{0,\ 1,\ 2,\ .....,\ n-1\}$ tem-se

$$i \equiv j\ (mod\ n) \iff i = j.$$

Assim, dois números distintos do conjunto $\{0,\ 1,\ 2,\ .....,\ n-1\}$ não são congruentes módulo n.

Definição 8. Chamaremos de *sistema completo de resíduos* módulo n a *todo conjunto de n números inteiros* cujos restos pela divisão por n são os números $0,\ 1,\ 2,\ ....,\ n-1$, sem repetições e numa ordem qualquer.

Assim, se $a_1,\ a_2,\ .....a_n$ são n inteiros, dois a dois não congruentes módulo n, então eles formam um sistema completo de resíduos módulo n.

De fato, os restos da divisão dos a_i com $1 \leq i \leq n-1$ por n são 2 a 2 distintos, o que implica que são os números $0,\ 1,\ 2,\ ....,\ n-1$ em alguma ordem.

Exemplo 20. Congruência módulo 4.

O conjunto$\{0,\ 1,\ 2,\ 3\}$ forma um sistema completo de resíduos módulo 4.

O conjunto $\{-2,\ -1,\ 0,\ 1\}$ é tal que

$-2 \equiv 2\ (mod\ 4)$

$-1 \equiv 3\ (mod\ 4)$

$0 \equiv 0\ (mod\ 4)$

$1 \equiv 1\ (mod\ 4)$

Portanto $\{-2,\ -1,\ 0,\ 1\}$ também é um sistema completo de resíduos módulo 4.

Exemplo 21. (Congruência módulo 3)

Indicaremos nas tabelas abaixo os restos das divisões de um inteiro por 3.

	0	1	2	3	4	5	6	7	8	9	10	11	...
restos da divisão por 3	0	1	2	0	1	2	0	1	2	0	1	2	...

	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	...
restos da divisão por 3	2	1	0	2	1	0	2	1	0	2	1	...

Tendo em vista estas tabelas fica fácil tomar um sistema completo de resíduos módulo 3, basta escolher três números que possuem restos distintos, por exemplo:

$\{7,\ -4,\ -6\}$ é um sistema completo de resíduos módulo 3.

Proposição 11. *Se* $\{a_1,\ a_2,\ .....,\ a_n\}$ *é um sistema completo de resíduos módulo* n*, onde* $a_1 \equiv 0\ (mod\ n)$ *então*

$$a_2.a_3.....a_n \equiv 1.2.3.....(n-1)\ (mod\ n).$$

Demonstração. De fato, para cada i, $2 \leq i \leq n$ existe um único b_i com $1 \leq b_i \leq n-1$ tal que $a_i \equiv b_i\ (mod\ n)$.

Como $\{a_2, a_3,\ .....\ a_n\}$ tem exatamente $n-1$ elementos não congruentes 2 a 2 e $\{b_2,\ b_3,\ .....,\ b_n\}$ tem exatamente $n-1$ elementos, temos $\{b_2,\ b_3,\ .....,\ b_n\} = \{1,\ 2,\ ....,\ n-1\}$.

Daí $a_2.a_3.....a_n \equiv b_2.b_3.....b_n \equiv 1.2.3.....n-1\ (mod\ n)$. □

Proposição 12. *Sejam $a,\ k,\ n\ \in \mathbb{Z}$ com $n > 1$ e $mdc\ (k,\ n) = 1$. Se $\{a_1,\ a_2,\ .....,\ a_n\}$ é um sistema completo de resíduos módulo n então $\{k.a_1,\ k, a_2,\ .....,\ k.a_n\}$ também é um sistema completo de resíduos módulo n.*

Demonstração. Tem-se que, para $1 \leq i,\ j \leq n$:

Como $mdc\ (k,\ n) = 1$, $k.a_i = k.a_j \iff a_i \equiv a_j\ (mod\ n) \iff i = j$.

Isso mostra que os n elementos de $\{k.a_1,\ .....,\ k.a_n\}$ são, dois a dois, não congruentes módulo n e portanto, formam um sistema completo de resíduos módulo n. □

Proposição 13. *Sejam p um número primo e a um inteiro tal que $p \nmid a$. Então*

$$a.(2a).(3a).....(p-1)a \equiv 1.2.3.....(p-1)\ (mod\ p).$$

Demonstração. Como $p \nmid a$ tem-se que $mdc\ (p,\ a) = 1$.

Considerando o sistema completo de resíduos módulo p, $\{0,\ 1,\ .....\ p-1\}$ e usando a proposição 11 tem-se que:

$\{0,\ a.1,\ a.2,\ ....,\ a.(p-1)\}$ também é um sistema completo de resíduos módulo p.

Agora usando a proposição 11 tem-se que

$$a.1.(2a).(3a).....(p-1)a \equiv 1.2.3.....(p-1)\ (mod\ p).$$

□

Usando os resultados acima, podemos provar o Pequeno Teorema de Fermat.

2.7 Pequeno Teorema de Fermat

Teorema 4. *Pequeno Teorema de Fermat*

Se p é um número primo e a é um inteiro não divisível por p então

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Demonstração. Como $p \nmid a$ tem-se:

$a.(2a).(3a).....(p-1)a \equiv 1.2.3.....(p-1) \ (mod\ p)$

donde, $a^{p-1}.(1.2.3.....(p-1)) \equiv 1.2.3.....(p-1) \ (mod\ p)$

Agora observando que $mdc\ (p,\ 1.2.3.....(p-1)) = 1$ segue que

$a^{p-1} \equiv 1 \ (mod\ p)$ □

Corolário 2. *Se p é um número primo e a um inteiro qualquer então*

$$a^p \equiv a \ (mod\ p).$$

Demonstração. Caso $p \nmid a$, pelo Pequeno Teorema de Fermat, tem-se que $a^{p-1} \equiv 1 \ (mod\ p)$ e daí $a^p \equiv a \ (mod\ p)$.

Supondo $p \mid a$ tem-se $a \equiv 0 \ (mod\ p)$ e daí, trivialmente

$a^p \equiv a \ (mod\ p)$. □

Capítulo 3

Aplicações de Congruência Para o Ensino Médio

As aplicações citadas neste capítulo estão voltadas para o Ensino Médio. Cada uma das aplicações de aritmética modular que serão citadas neste tópico do trabalho tem sua relevância, seja ela por colaborar com a solução de algum problema da atualidade, seja por agilizar o processo de resolução de determinados problemas da matemática do ensino básico, seja para introduzir um novo problema de motivação para aprender matemática.

Citaremos aqui quatro exemplos de aplicações de aritmética modular que poderão ser utilizados por professores de matemática da educação básica, principalmente para aqueles que atuam no ensino médio, como forma de contextualizar a referida disciplina com as necessidades do nosso dia-a-dia.

3.1 Equações Diofantinas

Definição 9. Uma equação do tipo $a.x + b.y = c$, onde a ,b e c são números inteiros é denominada Equação Diofantina Linear.

Resolver uma Equação Diofantina Linear significa achar todas as soluções inteiras dessa equação. Começaremos com a seguinte proposição:

Proposição 14. *Uma equação diofantina linear do tipo $ax + by = c$ possui solução inteira x e y se, e somente se, $mdc\,(a,\ b) \mid c$.*

Demonstração.

$\Rightarrow$) Seja $ax + by = c$, onde $a,\ b$ e c são inteiros e que possua uma solução inteira, ou seja, existem x_0 e y_0 inteiros tais que:

$ax_0 + by_0 = c \quad (1)$.

Suponha que $d = mdc\,(a,\ b)$, assim existem m e n inteiros tais que:

$a = dm$ e $b = dn$, pois $d \mid a$ e $d \mid b$.

Substituindo na equação (1) temos:

$c = ax_0 + by_0 = dmx_0 + dny_0$

$c = d.(mx_0 + ny_0)$.

Como $mx_0 + ny_0$ é inteiro, concluímos que $d \mid c$.

$\Leftarrow$) Se $d = mdc\,(a,\ b)$ divide c, então existe um inteiro q tal que $c = dq$. Já sabemos que pelo Teorema de Bézout, existem inteiros x_0 e y_0 tais que

$mdc\,(a,\ b) = d = ax_0 + by_0 \quad (2)$

Multiplicando q em ambos os lados de equação (2), obtemos:

$dq = ax_0q + by_0q$.

Como $c = dq$, substituindo:

$c = a(x_0q) + b(y_0q)$

Se chamarmos de x_0q e y_0q de x e y respectivamente, temos $c = ax + by$.

Portanto se $d \mid c$ existem x e y que serão soluções da equação diofantina linear. □

Exemplo 22. Seja dada a equação diofantina linear, $5x + 8y = 4$.

Essa equação possui solução inteira, pois $mdc\ (5,\ 8) = 1$ e $1 \mid 4$. Nesse caso, é fácil descobrir que $x = 4$ e $y = -2$ é uma solução.

Afirmamos que: $\begin{cases} x = 4 + \left(\frac{8}{1}\right).t \\ y = -2 - \left(\frac{5}{1}\right).t \end{cases}$,para qualquer t inteiro também é solução.

Por exemplo, para $t = 2$, temos:

$\begin{cases} x = 4 + 16 = 20 \\ y = -2 - 10 = -12 \end{cases}$ é uma solução. Com efeito, $5.20+8.(-12) = 100-96 = 4$.

De um modo geral, se $(x_0,\ y_0)$ é uma solução particular de uma equação $ax+by = c$ então para qualquer inteiro t

$\begin{cases} x = x_0 + \left(\frac{b}{d}\right).t \\ y = y_0 - \left(\frac{a}{d}\right).t \end{cases}$ também é solução.

Com efeito, $a.(x_0 + \left(\frac{b}{d}\right).t) + b.(y_0 - \left(\frac{a}{d}\right).t) = a.x_0 + b.y_0 + \frac{ab}{d}.t - \frac{ab}{d}.t = c + 0 = c$.

De fato, esta fórmula nos dá todas as soluções inteiras, conforme a seguinte proposição:

Proposição 15. *(Solução Geral)*

Sejam $a,\ b$ e c inteiros e $d = mdc\ (a,\ b)$ tais que $d \mid c$, $(x,\ y)$ é solução da equação $ax + by = c$ se, e somente se, existe t inteiro tal que

$$\begin{cases} x = x_0 + \left(\frac{b}{d}\right).t \\ y = y_0 - \left(\frac{a}{d}\right).t \end{cases}$$

onde $(x_0,\ y_0)$ *é uma solução particular.*

Demonstração.

$\Longrightarrow$) Já verificada anteriormente.

$\Longleftarrow$) Seja $(x,\ y)$ uma solução da equação $ax+by=c$. Sabemos que $ax_0+by_0=c$, assim temos que:

$ax_0+by_0=ax+by$, ou seja, $ax_0-ax=by-by_0$ e daí $a.(x_0-x)=b.(y-y_0)$.

Assim $b \mid a.(x_0-x)$ e que $a \mid b.(y-y_0)$ (2).

Como $d=mdc\ (a,\ b)$ então existem inteiros a_1 e b_1 tais que:

$a=a_1.d$ e $b=b_1.d$. Substituindo essas equações em (2) temos:

$b_1.d \mid a_1.d.(x_0-x)$ e $a_1.d \mid b_1.d.(y-y_0) \implies b_1 \mid a_1.(x_0-x)$ e $a_1 \mid b_1.(y-y_0)$.

Como $mdc\ (a_1,\ b_1) = mdc\ (\frac{a}{d},\ \frac{b}{d}) = 1$.

Concluímos que:

$b_1 \mid x_0-x$ e que $a_1 \mid y-y_0$. Portanto existem inteiros t e t_1 tais que:

$x_0-x=b_1.t$ e $y-y_0=a_1.t_1$

$x=x_0+b_1.t$ e $y=y_0+a_1.t_1$, onde $b_1=\frac{b}{d}$ e que $a_1=\frac{a}{d}$. Substituindo temos:

$$\begin{cases} x=x_0+\left(\frac{b}{d}\right)t \\ y=y_0+\left(\frac{a}{d}\right).t_1 \end{cases}$$

Como $(x,\ y)$ é uma solução tem-se

$a.(x_0+\left(\frac{b}{d}\right)t+b.(y_0+\left(\frac{a}{d}\right).t_1)=c$

$a.x_0+b.y_0+\frac{ab}{d}.t+\frac{ab}{d}.t_1=c$

$c + \frac{ab}{d}.t + \frac{ab}{d}.t_1 = c$

$\frac{ab}{d}.t + \frac{ab}{d}.t_1 = 0$. Portanto $t_1 = t$ e dai

$$\begin{cases} x = x_0 + \left(\frac{b}{d}\right).t \\ y = y_0 - \left(\frac{a}{d}\right).t \end{cases} .$$

□

Observação 6. Podemos encontrar uma solução particular $(x_0,\ y_0)$ usando o Algoritmo Euclidiano Estendido, e daí temos a solução geral:

$$\begin{cases} x = x_0 + \left(\frac{b}{d}\right).t \\ y = y_0 - \left(\frac{a}{d}\right).t \end{cases} \quad t \in \mathbb{Z}.$$

Problema 1. Na loja varejista $MAYKEMÁTICA$ vende-se dois tipos de pacote de arroz: o da marca $JÓIA$ que custa $R\$\ 8,00$ cada pacote e outro da marca $COMERBEM$ que custa $R\$\ 5,00$ cada pacote. O Sr. Diofanto, dono da mercearia de Alexandria, possui $R\$\ 500,00$ e pretende gastar tudo comprando arroz. Lembrando que não sobrará troco e que a loja não trabalha com pacotes parciais, quantos pacotes de arroz de cada marca, o Sr. Diofanto vai levar para sua mercearia?

SOLUÇÃO:

Chamando

$j = \textit{número de pacotes de arroz da marca } JÓIA$

$c = \textit{número de pacotes de arroz da marca } COMERBEM,$

montamos a seguinte equação: $8j + 5c = 500$.

Pelo Algoritmo Euclidiano temos:

	1	1	1	2
8	5	3	2	1
3	2	1	0	

$mdc\ (8,\ 5) = 1$. Como $1 \mid 500$ segue que essa equação possui solução inteira.

Pelo Teorema de Bézout, existem x e y inteiros tais que:

$$8x + 5y = 1 \quad (1)$$

Para encontrarmos as soluções j e c do problema, basta solucionarmos (1) e multiplicar por 500, pois assim teremos $8.(500x) + 5.(500y) = 500$, onde $j = 500x$ e $c = 500y$.

Para solucionarmos (1) basta aplicar o Algoritmo Euclidiano Estendido

restos	quocientes	x	y
8	$*$	1	0
5	$*$	0	1
3	1	1	-1
2	1	-1	2
1	1	2	-3

Assim $x = 2$ e $y = -3$, ou seja, $8.2 + 5.(-3) = 1$. Multiplicando essa equação por 500 (esse número é o quociente da divisão c dividido por d), obtemos

$8.1000 + 5.(-1500) = 500$ ou seja, $x_0 = 1000$ e $y_0 = -1500$ são as soluções particulares. No nosso problema a solução $c = -1500$ não convém.

Usando a expressão da solução geral, obtemos:

$$\begin{cases} j = 1000 + 5t \\ c = -1500 - 8t \end{cases}, \text{ sendo } t \text{ um inteiro qualquer.}$$

Para esse problema, as soluções j e c devem ser ambas inteiras positivas, então

$$\begin{cases} j \geq 0 \\ c \geq 0 \end{cases} \Longrightarrow \begin{cases} 1000 + 5t \geq 0 \\ -1500 - 8t \geq 0 \end{cases} \Longrightarrow \begin{cases} t \geq -200 \\ t \leq -187,5 \end{cases},$$

onde t é um inteiro qualquer, ou seja, $-200 \leq t \leq -187,5$. Como t deve ser inteiro, os possíveis valores admitidos para t são $-200 \leq t \leq -188$, o que acarreta 13 opções inteiras para o parâmetro t.

Observe na tabela abaixo os possíveis valores para j e c que solucionam nosso problema, quando $-200 \leq t \leq -188$ para t inteiro, usando

$$\begin{cases} j = 1000 + 5t \\ c = -1500 - 8t \end{cases}$$

valores de $t \rightarrow$	-188	-189	-190	-191	-192	-193
j	60	55	50	45	40	35
c	4	12	20	28	36	44

valores de $t \rightarrow$	-194	-195	-196	-197	-198	-199
j	30	25	20	15	10	5
c	52	60	68	76	84	92

3.2 Criptografia

A palavra "*CRIPTOGRAFIA*" vem do grego, *kriptós:*escondido, oculto e *grápho*: grafia, ou seja, é a arte ou ciência de escrever mensagens de forma sigilosa em códigos, de forma a permitir que somente o destinatário real possa decodificá-la e compreendê-la.

A criptografia consiste nos conceitos e técnicas usados para a transmissão segura de dados ou mensagens sigilosas através de um sistema monitorado por pessoas não autorizadas a obter ou ler essas mensagens, sendo imprescindível a segurança das mesmas.

Antes de criptografar uma mensagem, o texto original deve ser adaptado a um sistema de números. A este procedimento inicial intitulamos pré-codificação, que consiste em considerar uma correspondência biunívoca de todos os grafemas (letras) usados na redação da mensagem de uma certa língua e um conjunto finito, sequencial e apropriado de números.

Um exemplo de tal correspondência é dado pelo ASCII-code (American Standard Code for Information Interchange), que significa Código Americano de Intercâmbio de Informação (atualmente usados nos computadores para digitação no teclado). Serve de exemplo também as correspondências EBCDIC e HTML.

A seguir, apresentamos as Criptografias de César, de Cifras Afins e RSA.

3.2.1 Criptografia de César

A criptografia de César foi uma das pioneiras em relação à aplicação da criptografia e foi utilizada pelos comandados do imperador Júlio César nas guerras de expansão de seu território.

A codificação da Criptografia de César está relacionada na transposição de um determinado número de casas para frente das letras do alfabeto, conforme o exemplo a seguir:

A	B	C	D	E	F	G	H	I	J	K	L	M
d	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
q	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*	*a*	*b*	*c*

Exemplo 23. Codifique a mensagem "$CÉSAR\,É\,REI$" usando a Criptografia de César.

Basta substituir cada letra da mensagem original pela sua letra minúscula, ou seja:

"$f\,hvdu\,uhl$".

Considere a seguinte pré-codificação:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	*01*	*02*	*03*	*04*	*05*	*06*	*07*	*08*	*09*	*10*	*11*	*12*
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*

A pré-codificação transforma a mensagem em números e a codificação o transforma em outros números. Assim para codificarmos uma mensagem usando a Criptografia de César, aplicamos a pré-codificação e a codificamos usando um número natural k chamado de chave, que fará a transposição.

Exemplo 24. Considerando a chave $k = 3$ (chave original da Criptografia de César), codifique a mensagem

"$MATEMÁTICA$"

Primeiramente, vamos pré-codificar essa mensagem usando a correspondência citada acima:

$$12 - 00 - 19 - 04 - 12 - 00 - 19 - 08 - 02 - 00$$

Para codificar esses números, usaremos a chave $k = 3$, ou seja, cada número será adicionado 3 unidades, ou seja, a codificação será:

$$15 - 03 - 22 - 07 - 15 - 03 - 22 - 11 - 05 - 03$$

Veja que ao utilizar a correspondência, obteremos a seguinte mensagem:

$$"PDWHPDWLFD"$$

diferente da nossa mensagem original "$MATEMÁTICA$".

Observação 7. Veja que essa correspondência biunívoca totaliza 26 símbolos (letras sem acentuação), de 00 até 25, ou seja, todos os possíveis restos de uma divisão onde o divisor é 26. Logo, na Criptografia de César podemos aplicar uma chave k tal que $0 < k < 26$.

Exemplo 25. Codifique a mensagem

$$"MARIA"$$

usando a chave $k = 15$ na Criptografia de César.

Pré-codificação de "$MARIA$" : $12 - 00 - 17 - 08 - 00$

Codificando:

$12 + 15 = 27 \equiv 01 \ (mod\ 26)$

$00 + 15 = 15 \equiv 15 \ (mod\ 26)$

$17 + 15 = 32 \equiv 06 \ (mod\ 26)$

$08 + 15 = 23 \equiv 23 \ (mod\ 26)$

$00 + 15 = 15 \equiv 15 \ (mod\ 26)$

Logo a codificação será:

$$01 - 15 - 06 - 23 - 15$$

Assim, qualquer mensagem codificada na Criptografia de César usando uma chave qualquer k tal que $0 < k < 26$, é resultado da expressão:

$$C(a) \equiv a + k \ (mod\ 26) \qquad (1)$$

onde

$$\begin{cases} a \rightarrow número\ pré\ codificado \\ C(a) \rightarrow número\ codificado \\ k \rightarrow chave\ da\ Criptografia\ de\ César \end{cases}$$

Para a decodificação aplicamos a seguinte expressão:

$$D(b) \equiv b - k \ (mod\ 26)$$

onde $b = C(a)$.

De fato,

$D(b) \equiv b - k \ (mod\ 26)$

$D(C(a)) \equiv C(a) - k \ (mod\ 26)$

substituindo (1) nessa expressão obtemos:

$D(C(a)) \equiv a + k - k \ (mod\ 26)$, logo

$$D(C(a)) \equiv a \ (mod\ 26)$$

Exemplo 26. Considere a mensagem "$MESTRADO$". Codifique-a usando a chave $k = 13$.

Pré-codificação de "$MESTRADO$": $12 - 04 - 18 - 19 - 17 - 00 - 03 - 14$

Para codificar, vamos usar a expressão: $C(a) \equiv a + 13 \ (mod\ 26)$

$C(12) \equiv 12 + 13 \equiv 25 \ (mod\ 26)$

$C(04) \equiv 04 + 13 \equiv 17 \ (mod\ 26)$

$C(18) \equiv 18 + 13 \equiv 31 \equiv 05 \ (mod\ 26)$

$C(19) \equiv 19 + 13 \equiv 32 \equiv 06 \ (mod\ 26)$

$C(17) \equiv 17 + 13 \equiv 30 \equiv 04 \ (mod\ 26)$

$C(00) \equiv 00 + 13 \equiv 13 \ (mod\ 26)$

$C(03) \equiv 03 + 13 \equiv 16 \ (mod\ 26)$

$C(14) \equiv 14 + 13 \equiv 27 \equiv 01 \ (mod\ 26)$

Logo, a mensagem codificada a ser enviada é:

$$25 - 17 - 05 - 06 - 04 - 13 - 16 - 01$$

Para decodificá-la, aplicamos a expressão $D(b) \equiv b - k \ (mod\ 26)$ onde b são os número da mensagem codificada.

$D(25) \equiv 25 - 13 \equiv 12 \ (mod\ 26)$

$D(17) \equiv 17 - 13 \equiv 04 \ (mod\ 26)$

$D(05) \equiv 05 - 13 \equiv -08 \ (mod\ 26)$ e $-08 + 26 \equiv 18 \ (mod\ 26)$

$D(06) \equiv 06 - 13 \equiv -07 \ (mod\ 26)$ e $-07 + 26 \equiv 19 \ (mod\ 26)$

Continuando o procedimento para os outros números da codificação, obtemos:

$$12 - 04 - 18 - 19 - 17 - 00 - 03 - 14$$

traduzindo usando a correspondência obtemos a mensagem original:

$$"MESTRADO"$$

Observação 8. A segurança da Criptografia de César é ineficaz, pois mesmo desconhecendo a chave k, que deve ser mantida em sigilo, é possível decifrar a mensagem codificada, basta aplicar a ideia de frequência de letras de uma certa língua em frases longas. Segundo S.C. Coutinho, em seu livro Criptografia, as letras que mais aparecem em frases longas na Língua Portuguesa são as vogais A, E e O. Assim, para decodificar, basta aplicar algumas simulações, descobrindo a letra que é mais frequente na mensagem, observando o código que mais aparece.

Exemplo 27. Decifre a mensagem codificada:

$$13 - 25 - 13 - 06 - 17 - 25 - 13 - 06 - 21 - 15 - 13 - 17 - 14 - 17 - 14 - 13$$

desconhecendo a chave k.

Usando a técnica de frequência de letras do nosso alfabeto, os códigos que aparecem com maior frequência são 13 e 17. Sendo, 13 uma frequência de 5 vezes e 17 de 3 vezes. Assim, supondo que 13 seja o número codificado de A e que 17 seja o número codificado do E, verificamos que a chave k deve ser 13.

Aplicando a expressão $D(b) \equiv b - 13 \ (mod\ 26)$, para cada número da mensagem codificada, obtemos a mensagem:

$$"A\ MATEMÁTICA\ É\ BELA"$$

3.2.2 Criptografia de Cifras Afins

Vamos considerar a mesma tabela de correspondência de pré-codificação utilizada na Criptografia de César.

Definição 10. Sejam

$$\begin{cases} m \text{ e } n \text{ inteiros estritamente positivos} \\ mdc\ (m,\ 26) = 1 \\ a = \text{número pré codificado} \end{cases}$$

Chamaremos de cifra afim a seguinte equação:

$$C(a) \equiv m.a + n\ (mod\ 26)$$

onde m e n são as chaves da cifra afim.

Observação 9. Como $mdc\ (m,\ 26) = 1$ existe $x \in \mathbb{Z}$ tal que $m.x \equiv 1\ (mod\ 26)$. Usaremos a notação m^{-1} para indicar qualquer inteiro tal que $m^{-1}.m \equiv 1\ (mod\ 26)$.

Lema 2. *Seja* $D(b) \equiv m^{-1}.(b-n)\ (mod\ 26)$, *onde* m^{-1} *é um inteiro tal que*

$m^{-1}.m \equiv 1\ (mod\ 26)$. *Então*

$$D(C(a)) \equiv a\ (mod\ 26).$$

Demonstração. Substituindo $b = C(a)$ na expressão $D(b) \equiv m^{-1}.(b-n)\ (mod\ 26)$ obtemos:

$D(C(a)) \equiv m^{-1}.(C(a)-n)\ (mod\ 26)$

Substituindo $C(a) \equiv ma + n\ (mod\ 26)$ na expressão acima, temos que:

$D(C(a)) \equiv m^{-1}.(ma+n-n)\ (mod\ 26)$

$D(C(a)) \equiv m^{-1}.ma\ (mod\ 26)$, logo

$$D(C(a)) \equiv a\ (mod\ 26).$$

Portanto a expressão $D(b) \equiv m^{-1}.(b-n)\ (mod\ 26)$ é a decodificação da Criptografia de Cifras Afins. □

Observação 10. A criptografia de César é um caso particular da criptografia de cifras afins.

De fato, basta considerar $m = 1$, pois $mdc\ (1,\ 26) = 1$.

Exemplo 28. Codifique a mensagem "$OBMEP$".

Para isso, devemos escolher dois números inteiros estritamente positivos m e n tal que $mdc\ (m,\ 26) = 1$.

Seja $m = 5$ e $n = 2$. Temos que $mdc\ (5,\ 26) = 1$.

Primeiramente, vamos pré-codificar a mensagem:

$$14 - 01 - 12 - 04 - 15$$

Para codificar, usamos a expressão $C(a) \equiv 5a + 2\ (mod\ 26)$ para cada bloco da pré-codificação.

$C(14) \equiv 5.14 + 2 \equiv 72 \equiv 20\ (mod\ 26)$

$C(01) \equiv 5.1 + 2 \equiv 7\ (mod\ 26)$

$C(12) \equiv 5.12 + 2 \equiv 62 \equiv 10\ (mod\ 26)$

$C(04) \equiv 5.4 + 2 \equiv 22\ (mod\ 26)$

$C(15) \equiv 5.15 + 2 \equiv 77 \equiv 25\ (mod\ 26)$

Logo, obtemos a mensagem codificada:

$$20 - 07 - 10 - 22 - 25$$

Exemplo 29. Decifre a mensagem

$$23 - 10 - 17 - 19 - 00$$

onde $m = 3$ e $n = 7$ são as chaves.

Como $mdc\ (26,\ 3) = 1$ existem x e y tais que $26x+3y = 1$ e daí $3.y \equiv 1\ (mod\ 26)$, ou seja, $y \equiv 3^{-1}\ (mod\ 26)$.

Assim, para determinar 3^{-1} módulo 26 basta resolver a equação $26x + 3y = 1$, aplicando o Algoritmo Euclidiano e o Algoritmo Euclidiano Estendido.

Algoritmo Euclidiano

	8	1	2
26	3	2	1
2	1	0	

Algoritmo Euclidiano Estendido temos:

restos	quocientes	x	y
26	*	1	0
3	*	0	1
2	8	1	-8
1	1	-1	9

Logo $x = -1$ e $y = 9$.

Portanto $3^{-1} = 9$ módulo 26.

Assim para decifrarmos a mensagem $23 - 10 - 17 - 19 - 00$ usamos a expressão

$$D(b) \equiv 9.(b - 7)\ (mod\ 26)$$

onde b é cada número da mensagem codificada. Então:

$D(23) \equiv 9.(23 - 7) \equiv 144 \equiv 14\ (mod\ 26)$

$D(10) \equiv 9.(10 - 7) \equiv 27 \equiv 01\ (mod\ 26)$

$D(17) \equiv 9.(17 - 7) \equiv 90 \equiv 12\ (mod\ 26)$

$D(19) \equiv 9.(19 - 7) \equiv 108 \equiv 04\ (mod\ 26)$

$D(00) \equiv 9.(00 - 7) \equiv -63 \equiv 15\ (mod\ 26)$.

Logo, temos a mensagem decodificada:

$$14 - 01 - 12 - 04 - 15$$

Fazendo a devida correspondência, obtemos:

$$"OBMEP"$$

Da mesma forma que a Criptografia de César, a Criptografia de Cifras Afins também não é considerada segura, pois usando a mesma ideia de frequência das letras da Língua Portuguesa conseguimos decifrá-la, mesmo não sendo o destinatário autorizado.

3.2.3 Criptografia RSA

Exemplo 30. Digamos que resolvo efetuar uma compra via internet em uma loja virtual usando o meu computador. Após ter escolhido os produtos no *site* da loja, vou ao "caixa-virtual" e efetuo o pagamento com o meu cartão de débito. Para isso, preciso informar a loja os dados do meu cartão. Contudo, isso significa que qualquer outra pessoa, "hacker", que obtiver estes meus dados, poderá efetuar compras em qualquer outro lugar com o meu cartão. Para evitar esse problema, os dados do meu cartão são codificados pelo meu computador e enviados para a loja.

Observe que o meu computador não pode usar um código qualquer como o utilizado na Criptografia de César ou de Cifras Afins, pois sua segurança é muito fraca, ou um outro código qualquer de chave secreta, pois a loja precisa lê-las e, para isso, tem que saber como decodificar a mensagem. Então, o meu computador tem que se comunicar com o da loja, trocar algumas informações de como serão feitas a codificação e a decodificação, sempre secretamente, o que torna o processo redundante, como a história do ovo e da galinha.

A Criptografia RSA está baseada na distribuição de chaves públicas, as quais são usadas para a codificação e não para a decodificação, criadas primeiramente pelos matemáticos, Whitfield Diffie e Martin Hellman, que pensaram em elaborar funções matemáticas

em que sua inversa seria praticamente impossível de ser determinada, ou seja, consiste em usar, do ponto de vista computacional, uma função f com a propriedade que seja simples calcular $f(n)$, mas que seja inviável na prática, computacional ou de outra forma, calcular sua inversa.

Nessa perspectiva, o meu computador se comunica com o da loja que repassa a chave pública para codificar meus dados bancários. Desse modo, meu computador codifica e envia para a loja, que é a única que possui a chave privada, aquela que decodifica os meus dados. Então, após codificar e enviar, nem o meu próprio computador é capaz de decodificar os dados, apenas a loja.

Com esse conceito de chaves públicas, os matemáticos Ron Rivest, Adi Shamir e Leonard Adleman elaboraram o sistema RSA, iniciais de seus sobrenomes. A chave pública da Criptografia RSA apoia-se na facilidade de se efetuar a multiplicação de dois números primos grandes p e q e na dificuldade prática de se inverter o processo, ou seja, de determinar os fatores primos de um número grande.

Antes de se codificar uma mensagem, é necessário a conversão dos grafemas linguísticos em uma sequência de números, a já conhecida pré-codificação. Vamos supor, para simplificar nossos exemplos, que a mensagem original contenha apenas palavras, portanto, a mensagem será constituída pelas letras e os espaços entre as palavras.

A conversão de letras por números será feita pela tabela abaixo, sendo esta a primeira parte da pré-codificação:

A	B	C	D	E	F	G	H	I
10	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*
J	K	L	M	N	O	P	Q	R
19	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*
S	T	U	V	W	X	Y	Z	espaço
28	*29*	*30*	*31*	*32*	*33*	*34*	*35*	*36*

Observe que utilizaremos também um código numérico para o espaço, representado por 36.

Exemplo 31. A frase

"$MAYKEMATICA\ MAGICA$"

é convertida no número

$$2210342014221029181210362210161812 10.$$

Observação 11. A tabela de pré-codificação foi escolhida, iniciando no número 10, para simplificar nas contas e pela vantagem de evitar algumas ambiguidades. Suponha que utilizássemos a tabela de pré-codificação da Criptografia de César, a correspondência de B seria 1 e da C seria 2. Nesse caso, 12 poderia ser BC ou M.

Antes de continuar, precisamos escolher os parâmetros do sistema, dois números primos distintos p e q. Considere por $N = p.q$. Assim, a última fase da pré-codificação, consiste em separar em blocos o grande número formado, onde cada bloco deve ser menor que N.

Exemplo 32. Seja a mensagem acima, 2210342014221029181210362210161812 10. Se escolhermos os primos $p = 13$ e $q = 17$ teremos $N = 13.17 = 221$. Nesse caso a mensagem pode ser separada nos seguintes blocos:

$$22 - 103 - 4 - 201 - 42 - 210 - 29 - 181 - 210 - 36 - 22 - 101 - 61 - 81 - 210.$$

Observação 12. A maneira de se separar uma mensagem não é única, porém deve-se tomar cuidado, é necessário evitar que o bloco inicie com 0, para não trazer problemas na hora da decodificação.

Aqui termina a pré-codificação.

Vamos dar início a etapa codificação. Observe o seguinte exemplo:

Exemplo 33. Ana pretende enviar uma mensagem a Fred, de forma sigilosa.

Para Ana codificar a mensagem, ela vai necessitar do par $(N,\ e)$, chave pública do sistema informada por Fred, tal que:

$$\begin{cases} N = p.q \\ mdc\ (e,\ m) = 1 \end{cases}$$

onde $m = (p-1).(q-1)$. Para codificar ela deve seguir esses passos:

- Ana transforma a mensagem em números (1ª parte da pré-codificação) à ser enviada para Fred;
- Ana separa o grande número em blocos $a_1,\ a_2,\ .....,\ a_k$ onde cada $a_i < N$ para todo i, $1 \leq i \leq k$.
- Ana codifica cada bloco a_i usando a expressão $C(a_i) \equiv a_i^e\ (mod\ N)$, com $1 \leq i \leq k$;
- Ana envia a mensagem $b_1,\ b_2,\ ...,\ b_k$ codificada a Fred, tal que $b_i = C(a_i)$;

Exemplo 34. Ana quer enviar a mensagem "$OLA\ AMIGO$" a Fred. Seja $p = 5$ e $q = 13$.

Assim $N = 5.13 = 65$ e $= 4.12 = 48$. O número e deve ser de tal forma que $mdc\ (e,\ 48) = 1$. Vamos escolher $e = 11$.

Logo a chave pública de Fred é $(65,\ 11)$.

Ana, primeiramente, pré-codifica a seguinte mensagem à ser enviada: "$OLA\ AMIGO$"

242110361022181624

Ana separa a mensagem codificada em blocos a_i de tal forma que $a_i < N = 65$, por exemplo,

$24 - 21 - 10 - 36 - 10 - 22 - 18 - 16 - 24$.

Ana codifica cada bloco, utilizando a expressão

$C(a) \equiv a^e\ (mod\ 65)$.

$C(24) \equiv 24^{11}\ (mod\ 65)$. Sabemos que $24^2 \equiv 576 \equiv 56\ (mod\ 65)$, segue que:

$(24^2)^5 \equiv 56^5 \equiv 550731776 \equiv 36\ (mod\ 65)$, ou seja, $24^{10} \equiv 36\ (mod\ 65)$, assim temos que:

$24^{10}.24 \equiv 36.24 \equiv 864 \equiv 19\ (mod\ 65)$.Logo,

$C(24) \equiv 19\ (mod\ 65)$.

Aplicando o mesmo raciocínio para os outros blocos a_i, obtemos as codificações:

$C(21) \equiv 21^{11} \equiv 31\ (mod\ 55)$

$C(10) \equiv 10^{11} \equiv 30\ (mod\ 55)$

$C(36) \equiv 36^{11} \equiv 56\ (mod\ 55)$

$C(10) \equiv 10^{11} \equiv 30\ (mod\ 55)$

$C(22) \equiv 22^{11} \equiv 3\ (mod\ 55)$

$C(18) \equiv 18^{11} \equiv 47\ (mod\ 55)$

$C(16) \equiv 16^{11} \equiv 61\ (mod\ 55)$

$C(24) \equiv 24^{11} \equiv 19\ (mod\ 55)$

Logo, Ana envia a mensagem codificada:

$$19 - 31 - 30 - 56 - 30 - 3 - 47 - 61 - 19$$

Observação 13. Os blocos já codificados não poderão ser juntados de modo a formar um grande número.

Para decodificar, precisamos de dois números: $(N,\ d)$, onde d é o inverso de e módulo m, ou seja, $e.d \equiv 1\ (mod\ m)$ tal que $m = (p-1).(q-1)$.

Assim, para Fred decodificar, seguirá esses passos:

- Fred determina d de tal forma que $e.d \equiv 1\ (mod\ m)$;
- Fred utiliza a expressão $D(b_i) \equiv b_i^d\ (mod\ N)$ para cada i inteiro tal que $1 \leq i \leq k$;
- Fred finaliza a decodificação, obtendo os valores $a_1,\ a_2,\ .....,\ a_k$. E, após utiliza a tabela de pré-codificação para obter a mensagem em texto;

Antes de continuarmos, observe essas informações:

1) Apenas Fred deve conhecer o par $(N,\ d)$, pois esse é o segredo para decodificar uma mensagem codificada com o par $(N,\ e)$.

2) Para determinar d, basta aplicar o Algoritmo Euclidiano Estendido.

Com efeito, como $mdc\ (e,\ m) = 1$ existem pelo Teorema de Bezout x e y inteiros tais que $e.x + my = 1$ e daí $e.x \equiv 1\ (mod\ m)$, ou seja, $x \equiv d\ (mod\ m)$.

Exemplo 35. Fred recebe a mensagem codificada de Ana $19-31-30-56-30-3-47-61-19$ e inicia a decodificação, sendo $N = 65$, $m = 48$ e $e = 11$.

Primeiramente, Fred deve determinar d tal que

$11.d \equiv 1\ (mod\ 48)$.

Como $mdc\ (48,\ 11) = 1$ segue que existem inteiros x e y do Teorma de Bezout tais que $48x + 11y = 1$.

Determinando y, determinamos d.

Aplicando o Algoritmo Euclidiano e o Algoritmo Euclidiano Estendido, temos:

	4	2	1	3
48	11	4	3	1
4	3	1	0	

restos	quocientes	x	y
48	*	1	0
11	*	0	1
4	4	1	-4
3	2	-2	9
1	1	3	-13

Logo, $y = -13$.

Assim $d = -13 \equiv -13 + 48 \equiv 35\ (mod\ 48)$.

Então Fred aplicará a expressão $D(b) \equiv b^{35}\ (mod\ 65)$ para decodificar cada bloco b enviado por Ana.

Assim,

$D(19) \equiv 19^{35}\ (mod\ 65)$. Vemos que $19^7 \equiv 893871739 \equiv 59\ (mod\ 65)$.

$(19^7)^5 \equiv 59^5 \equiv 714924299 \equiv 24\ (mod\ 65)$, ou seja, $19^{35} \equiv 24\ (mod\ 65)$. Logo,

$D(19) \equiv 24\ (mod\ 65)$.

Continuando o mesmo procedimento para os outros códigos obtemos:

$D(31) \equiv 31^{35} \equiv 21\ (mod\ 65)$

$D(30) \equiv 30^{35} \equiv 10\ (mod\ 65)$

$D(56) \equiv 56^{35} \equiv 36\ (mod\ 65)$

$D(30) \equiv 30^{35} \equiv 10\ (mod\ 65)$

$D(3) \equiv 3^{35} \equiv 22\ (mod\ 65)$

$D(47) \equiv 47^{35} \equiv 18\ (mod\ 65)$

$D(61) \equiv 61^{35} \equiv 16\ (mod\ 65)$

$D(19) \equiv 19^{35} \equiv 24\ 9mod\ 65)$

Logo a mensagem decodificada, em blocos, é:

$$24 - 21 - 10 - 36 - 10 - 22 - 18 - 16 - 24$$

que ao realizar a correspondência com as letras mostra o texto:

OLA AMIGO.

Veja que ao utilizar a expressão $D(b) \equiv b^d \ (mod\ N)$, sendo b o bloco da mensagem codificada, Fred retornou ao bloco original. Assim, decodificando um bloco da mensagem codificada, encontramos o bloco correspondente da mensagem original, ou seja, $D(C(a)) = a$. A seguinte proposição mostra que isto sempre ocorre.

Proposição 16. *Se* $C(a) \equiv a^e \ (mod\ N)$ *e* $D(b) \equiv b^d \ (mod\ N)$ *então*

$$D(C(a)) \equiv a \ (mod\ N),$$

onde $e.d \equiv 1 \ (mod\ m)$ *e* $m = (p-1).(q-1)$.

Demonstração. Substituindo $b = C(a)$ na expressão $D(b) \equiv b^d \ (mod\ N)$ obtemos:

$D(C(a)) \equiv (C(a))^d \ (mod\ N)$. Como $C(a) \equiv a^e \ (mod\ N)$ segue que:

$D(C(a)) \equiv (a^e)^d \ (mod\ N) \implies D(C(a)) \equiv a^{e.d} \ (mod\ N) \qquad (1).$

Mas sabemos que

$$e.d \equiv 1 \ (mod\ (p-1).(q-1))$$

ou seja,

$$(p-1).(q-1) \mid e.d - 1$$

assim, existe um inteiro t tal que:

$e.d - 1 = t.(p-1).(q-1)$, ou melhor, $e.d = t.(p-1).(q-1) + 1$. Então

$$a^{ed} = a.a^{(p-1).t.(q-1)}$$

.

Suponha primeiramente que $p \nmid a$.

Dai, pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 \ (mod\ p)$, segue que

$a^{ed} \equiv a.a^{(p-1).t.(q-1)} \equiv a.(a^{(p-1)})^{t.q-1)} \equiv a.1^{t.(q-1)} \equiv a\ (mod\ p)$, portanto

$a^{ed} \equiv a\ (mod\ p)$, ou seja, $p \mid a^{ed} - a$.

No caso em que $p \mid a$ tem-se também que $p \mid a^{ed} - a$.

De forma análoga, mostra-se que:

$a^{ed} \equiv a\ (mod\ q)$, ou seja, $q \mid a^{ed} - a$.

Como $mdc\ (p,\ q) = 1$, segue que $p.q \mid a^{ed} - a$, ou seja:

$a^{ed} \equiv a\ (mod\ p.q)$

como $p.q = N$ então:

$a^{ed} \equiv a\ (mod\ N)$ para todo a inteiro.

Assim de (1) temos:

$D(C(a)) \equiv a^{ed} \equiv a\ (mod\ N)$.

Portanto $D(C(a)) \equiv a\ (mod\ N)$. □

Exemplo 36. Suponha que você recebeu a seguinte mensagem codificada $16 - 22 - 21 - 37 - 37 - 09 - 23 - 09 - 39 - 23 - 18$, sendo a chave pública $(51,\ 7)$ onde $p = 3$ e $q = 17$.

De inicio, observe que não é possível corresponder essa mensagem com um texto, pois em nossa tabela de pré-codificação não existe o símbolo representado por 09. Para decodificar, vamos precisar de d tal que $7.d \equiv 1\ (mod\ 32)$.

Como $mdc\ (32,\ 7) = 1$, pelo Teorema de Bezout, existem x e y inteiros tais que $32x + 7y = 1$. Basta determinar y.

Aplicando o Algoritmo Euclidiano e o Algoritmo Euclidiano Estendido temos que:

	4	1	1	3
32	7	4	3	1
4	3	1	0	

restos	quocientes	x	y
32	*	1	0
7	*	0	1
4	4	1	-4
3	1	-1	5
1	1	2	-9

$y = -9$.

Assim $d = -9 \equiv -9 + 32 \equiv 23 \equiv (mod\ 32)$

Aplicando a expressão decodificação $D(b) \equiv b^{23}\ (mod\ 51)$ temos que:

$D(16) \equiv 16^{23}\ (mod\ 51)$. Observe que $16^4 \equiv 65536 \equiv 1\ (mod\ 51)$. Segue que

$(16^4)^5 \equiv 1^5 \equiv 1\ (mod\ 51)$, ou seja, $16^{20} \equiv 1\ (mod\ 51)$.

Como $16^3 \equiv 16\ (mod\ 51)$, segue que $16^{20}.16^3 \equiv 1.16\ (mod\ 51)$. Logo

$16^{23} \equiv 16\ (mod\ 51)$. Então

$D(16) \equiv 16^{23} \equiv 16\ (mod\ 51)$

De forma análoga para os outros blocos obtemos:

$D(22) \equiv 22^{23} \equiv 10\ (mod\ 51)$

$D(21) \equiv 21^{23} \equiv 30\ (mod\ 51)$

$D(37) \equiv 37^{23} \equiv 28\ (mod\ 51)$

$D(37) \equiv 37^{23} \equiv 28\ (mod\ 51)$

$D(9) \equiv 9^{23} \equiv 36\ (mod\ 51)$

$D(23) \equiv 23^{23} \equiv 14\ (mod\ 51)$

$D(9) \equiv 9^{23} \equiv 36\ (mod\ 51)$

$D(39) \equiv 39^{23} \equiv 27\ (mod\ 51)$

$D(23) \equiv 23^{23} \equiv 14\ (mod\ 51)$

$D(18) \equiv 18^{23} \equiv 18\ (mod\ 51)$

Assim, a mensagem decodificada é: $16-10-30-28-36-27-14-18$. Fazendo a devida correspondência, obtemos a mensagem:

"*GAUSS É REI*"

Observação 14. Nos exemplos, consideramos primos pequenos de modo a facilitar as contas. Na prática são usados primos grandes contendo muitos dígitos para garantir a segurança das informações. Mas precisamente, o RSA Laboratory lançou desafios, que consistiam em fatorar um dado número natural N ($N = p.q$). Uma das chaves a ser fatorada corresponde ao produto dos primos:

$p = 163473364580925384844313388386509085984178367003309231 2$

$1811108523893331001045081512121181675115 79$

e

$q = 190087128166482211312685157393541397547189678996851549 3$

$6666385390880271038021044989571912614655 71.$

A segurança do RSA é baseada na seguinte afirmação: Não existe nenhum algoritmo conhecido capaz de fatorar inteiros grandes de modo realmente eficiente.

Observação 15. Sabendo os valores dos primos p e q, fica possível a decifração, por isso, esses números devem ser mantidos em sigilo. Mas se alguém conhece N e também o valor de $m = (p-1).(q-1)$, então ele consegue descobrir os valores de p e q.

De fato, resolvendo $(p-1)(q-1) = pq - p - q + 1 = m$. Substituindo $N = pq$ segue que

$N - (p+q) + 1 = m$, ou seja,

$p + q = N - m + 1$.

Logo, para descobrir p e q, basta resolver a equação $x^2 - (N - m + 1).x + N = 0$.

Esta observação faz sentido, pois de fato $m = (p-1).(q-1)$ é o valor de $\phi(n) = \phi(p.q)$ onde ϕ indica a Função de Euler.

A função ϕ:$\mathbb{N}^* \to \mathbb{N}$ é definida como, $\phi(n)$ = quantidade de números naturais, menores do que n, e que são primos com n.

Assim se alguém descobrir um modo de calcular $\phi(n)$, sem decompor o n, determinará os valores de p e q.

Capítulo 4

CONSIDERAÇÕES FINAIS

Concluímos que é possível aplicar alguns conceitos da Teoria dos Números nas salas de aula do Ensino Médio.

Com o Algoritmo Euclidiano Estendido, o aluno poderá determinar, de forma ágil e eficaz, uma solução particular das Equações Diofantinas Lineares.

A inserção da Criptografia na sala de aula poderá despertar o interesse discente pela área, muito utilizada atualmente na segurança de dados nas comunicações via internet. Somado a isso, poderá motivar a curiosidade sobre os números primos, tão fundamentais e misteriosos na matemática.

Enfim, acreditamos que esse trabalho possa servir como um material de apoio para o docente de matemática da educação básica, especialmente o que atua no Ensino Médio, com vistas a sanar algumas dificuldades na área de Aritmética. E, também, que possa servir de motivação e inspiração para que o mesmo busque se aperfeiçoar em cursos de pós-graduação, melhorando sua própria prática, podendo assim surgir contribuições a esse trabalho e de novas propostas de aplicações em sala de aula.

Apêndice A

Microsoft Excel

Para facilitar o processo das contas, utilizamos o software Microsoft Excel, pois nele é possível a implementação de fórmulas aritméticas em sua planilha eletrônica.

A.1 Algoritmo Euclidiano

Para determinarmos o $mdc\ (a,\ b)$, usamos a seguinte fórmula no Excel, onde nas células A2 e B2 entram o valores de a e b.

	A	B	C	D
1		=TRUNCAR(A2/B2)	=TRUNCAR(B2/C2)	=TRUNCAR(C2/D2)
2			=SE(A3=0;" $\leftarrow mdc$";A3)	=SE(B3=0;" $\leftarrow mdc$";B3)
3	=(A2-B1*B2)	=SE(A3=0;"FIM";(B2-C1*C2)	=SE(B3=0;"FIM";(C2-D1*D2))	=SE(C3=0;"FIM";(D2-E1*E2))

Observação 16. A célula A1 deve ficar em branco.

A.2 Algoritmo Euclidiano Estendido

Para resolver a equação $40x + 7y = 1$, primeiramente aplicamos o Algoritmo Euclidiano:

	5	1	2	2
40	7	5	2	1
5	2	1	0	

Após, completamos no Excel, o procedimento normal do Algoritmo Euclidiano Estendido e finalizamos com as seguintes fórmulas.

	A	B	C	D
1	restos	quocientes	x	y
2	40	*	1	0
3	7	*	0	1
4	5	5	=(C2-B4*C3)	=(D2-B4*D3)
5	2	1	=(C3-B5*C4)	=(D3-B5*D4)
6	1	2	=(C4-B6*C5)	=(D4-B6*D5)

Assim obtemos $x = 3$ e $y = -17$.

A.3 Solução Geral da Equação Diofantina Linear

Vamos usar como exemplo a equação já resolvida no Problema 1: $8j + 5c = 500$, onde $a = 8$, $b = 5$, $mdc\ (8,\ 5) = 1$, $j_0 = 1000$ e $c_0 = -1500$. Assim, colocamos os dados conhecidos na linha 2 e implantamos as fórmulas que aparecem a seguir:

	A	B	C	D	E
1	a	b	$mdc\ (a,\ b)$	j_0	c_0
2	8	5	1	1000	-1500
3					
4	valores t	-199	=(B4+1)	=(C4+1)	=(D4+1)
5	j	=(D2+((B2/C2)*B4))	=(D2+((B2/C2)*C4))	=(D2+((B2/C2)*D4))	=(D2+((B2/C2)*E4))
6	c	=(E2-((A2/C2)*B4))	=(E2-((A2/C2)*C4))	=(E2-((A2/C2)*D4))	=(E2-((A2/C2)*E4))

Observação 17. A linha 4 deve ser preenchida a partir das restrições encontradas para o

inteiro t.

A.4 Criptografia de Cifras Afins

A.4.1 Codificar

Na codificação dos códigos na Criptografia de Cifras Afins, colocamos os dados das chaves m e n, juntamente com os blocos da pré-codificação e usamos as fórmulas na coluna D. Para facilitar o entedimento, utilizamos o exemplo 28.

	A	B	C	D
1	chave m	chave n	blocos	Bloco Codificado
2	5	2	14	=((A2*C2+B2)-TRUNCAR((A2*C2+B2)/26)*26)
3	5	2	01	=((A3*C3+B3)-TRUNCAR((A3*C3+B3)/26)*26)
4	5	2	12	=((A4*C4+B4)-TRUNCAR((A4*C4+B4)/26)*26)
5	5	2	04	=((A5*C5+B5)-TRUNCAR((A5*C5+B5)/26)*26)
6	5	2	15	=((A6*C6+B6)-TRUNCAR((A6*C6+B6)/26)*26)

Assim, obtemos os códigos $20 - 07 - 10 - 22 - 25$

A.4.2 Decodificar

Colocamos os dados conhecidos nas primeiras colunas, m^{-1},a chave n e os códigos do bloco codificado. Assim, implantamos as fórmulas, como mostram na coluna D. Para exemplificar, observe a aplicação do exemplo 29.

	A	B	C	D
1	m^{-1}	chave n	bloco codif.	Bloco Decodificado
2	9	7	23	=(A2*(C2-B2)-TRUNCAR((A2*(C2-B2)/26))*26)
3	9	7	10	=(A3*(C3-B3)-TRUNCAR((A3*(C3-B3)/26))*26)
4	9	7	17	=(A4*(C4-B4)-TRUNCAR((A4*(C4-B4)/26))*26)
5	9	7	19	=(A5*(C5-B5)-TRUNCAR((A5*(C5-B5)/26))*26)
6	9	7	00	=(A6*(C6-B6)-TRUNCAR((A2*(C6-B6)/26))*26)

Observação 18. Em alguns casos pode ocorrer de o bloco decodificado aparecer negativo. Basta somar o bloco decodificado por 26. Veja a linha 6:

	A	B	C	D
6	9	7	00	-11

$$-11 + 26 \equiv 15 \ (mod\ 26).$$

A.5 Criptografia RSA

A.5.1 Codificar

Nessa parte foi importante usar as propriedades de congruência. Para clarear as ideias, vejamos o exemplo 33.

$C(24) \equiv 24^{11} \ (mod\ 65)$. Sabemos que $24^2 \equiv 576 \equiv 56 \ (mod\ 65)$ então:

$(24^2)^5 \equiv 56^5 \equiv 550731776 \equiv 36 \ (mod\ 65)$, ou seja, $24^{10} \equiv 36 \ (mod\ 65)$, assim temos que:

$24^{10}.24 \equiv 36.24 \equiv 864 \equiv 19 \ (mod\ 65)$.Logo,

$C(24) \equiv 19 \ (mod\ 65)$.

Assim, utilizamos as potências 2, 5 e após, multiplicamos por 24, pois:

$24^{11} = (24^2)^5.24$

	A	B	C	D	E	F
1	N	pot. 1	pot. 2	Código	Resto Parcial	Resto
2	65	2	5	24	=((D2^B2)-TRUNCAR(D2^B2)-A2)*A2)	=(((E2^C2)*D2)-TRUNCAR(((E2^C2)*D2)/A2)*A2)
3	65	2	5	21	=((D3^B3)-TRUNCAR(D3^B3)-A3)*A3)	=(((E3^C3)*D3)-TRUNCAR(((E3^C3)*D3)/A3)*A3)

A.5.2 Decodificar

Da mesma forma, foi necessário determinar as potências. Usaremos o exemplo 34.

$D(19) \equiv 19^{35}\ (mod\ 65)$. Vemos que $19^7 \equiv 893871739 \equiv 59\ (mod\ 65)$.

$(19^7)^5 \equiv 59^5 \equiv 714924299 \equiv 24\ (mod\ 65)$, ou seja, $19^{35} \equiv 24\ (mod\ 65)$. Logo,

$D(19) \equiv 24\ (mod\ 65)$.

Dessa forma, aplicamos as fórmulas com as potências 7 e 5, pois $(19^7)^5 = 19^{35}$.

	A	B	C	D	E	F
1	N	pot. 1	pot. 2	Código	Resto 1	Resto
2	65	7	5	19	=((D2^B2)-TRUNCAR((D2^B2)/A2)*A2)	=((E2^C2)-TRUNCAR((E2^C2)/A2)*A2)
3	65	7	5	31	=((D3^B3)-TRUNCAR((D3^B3)/A3)*A3)	=((E3^C3)-TRUNCAR((E3^C3)/A3)*A3)

Referências Bibliográficas

[1] CABRAL e QUEIROZ. André Luis e Lenisa Morais. A Criptografia ao Longo dos Tempos. Monografia de Conclusão de Curso. Centro Universitário Claretiano.

[2] CAMPELLO e LEAL. Antonio Carlos e Isabel. Teoria Aritmética dos Números e Criptografia RSA.

[3] CIDADE. Cleice de Cássia Franco. Sistema de Congruências - Algoritmo Chinês do Resto. Monografia de Conclusão de Curso. UFSM.

[4] COUTINHO, S.C. Números Inteiros e Criptografia RSA. Rio de Janeiro. IMPA/SBM, 2000.

[5] COUTINHO. S. C.. Criptografia. (Programa de Iniciação Científica OBMEP. Sociedade Brasileira de Matemática).

[6] DOMINGUES. José Sérgio. Algoritmos de Primalidade na Criptografia RSA.UNIMONTES.

[7] FREIRE. Benedito. Notas de Aula. Teoria dos Números.

[8] FREITAS e OLIVEIRA. Elisabete e José. Introdução à Teoria dos Números e Criptografia. (Caderno de Minicurso. II Colóquio de Matemática da Região Centro-Oeste).

[9] HEFEZ. A. Elementos de Aritmética. (Série Textos Universitários. Sociedade Brasileira de Matemática).

[10] HEFEZ. A. Iniciação à Aritmética. (programa de Iniciação Científica OBMEP. Sociedade Brasileira de Matemática).

[11] LEMOS. Manoel. Criptografia, Números Primos e Algoritmos.Publicações Matemáticas. UFPE.

[12] OLGIN, GROENWALD e FRANKE. Clarissa, Claudia e Rosvita. Criptografia no Ensino Médio. ULBRA.

[13] OLIVEIRA. Filipe. Introdução à Teoria dos Números. Universidade Nova de Lisboa.

[14] PELLEGRINI. Jerônimo. Introdução à Criptografia e seus Fundamentos. Notas de Aula.

[15] PIMENTEL. Elaine Gouvêa. Teoria dos Números e Criptografia RSA. Monografia de Conclusão de Curso.

[16] POMMER. Wagner Marcelo. Equações Diofantinas Lineares: Um Desafio Motivador para Alunos do Ensino Médio. Dissertação de Mestrado. PUC/SP.

[17] POSTAL. Tannery. Criptografia RSA. Monografia de Conclusão de Curso. UFMT.

[18] SAUTOY. Marcus du. A Música dos Números Primos: A História de um Problema Não Resolvido na Matemática. Tradução: Diego Alfaro. 2007.

[19] SHOKRANIAN. Salahoddin. Criptografia para Iniciantes. 2. ed. Editora Ciência Moderna.

[20] http://www.tabelaaascii.com/: acessado em 09\01\2013.