UNIVERSIDADE ESTADUAL DA PARABA
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UEPB

Alguns Métodos de Criptografia

Josemberg dos Santos Silva

Orientador: Prof. Dr. Vandenberg Lopes Vieira

Campina Grande - PB
Agosto/2016

UNIVERSIDADE ESTADUAL DA PARABA
Programa de Pós-Graduação em Matemtica
Mestrado Profissional - PROFMAT/CCT/UEPB

Alguns Métodos de Criptografia

por

Josemberg dos Santos Silva [†]

Dissertação Apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UEPB, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre em Matemática.

[†]Bolsista CAPES

S586a Silva, Josemberg dos Santos.
Alguns métodos de criptografia [manuscrito] / Josemberg dos Santos Silva. - 2016.
56 p.

Digitado.
Dissertação (Mestrado Profissional em Matemática em rede nacional) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2016.
"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática".

1. Aritmética. 2. Criptografia. 3. Teoria dos códigos. 4. Sistema RSA. I. Título.

21. ed. CDD 513

Alguns Métodosde de Criptografia

por

Josemberg dos Santos Silva

Trabalho de Conclusão de curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UEPB, modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado por:

Severino Horácio da Silva

Prof. Dr. Severino Horácio da Silva - UFCG

Maria Isabelle Silva

Profa. Dra. Maria Isabelle Silva - UEPB

Vandenberg Lopes Vieira

Prof. Dr. Vandenberg Lopes Vieira - UEPB
Orientador

Universidade Estadual da Paraba
Centro de Ciências e Tecnologia
Curso de Mestrado Profissional em Matemática em Rede Nacional

Agosto/2016

Dedicatória

Dedico este trabalho a meus pais que me deram força e determinação, aos meus familiares, minha esposa e a todos os amigos.

Agradecimentos

Agradeço primeiramente a Deus, pelo dom da vida e discernimento para concluir este trabalho.

À minha família, em especial José Pereira e Maria Marly, pelo apoio e força para conquistar essa etapa tão importante da minha vida.

À minha esposa (Luciana) que sempre esteve do meu lado, mesmo em momentos difíceis.

Aos professores do PROFMAT, pelo conhecimento adquiridos.

Aos colegas de mestrado, pela amizade que surgiu ao longo dessa caminhada, em especial, ao amigo Manoel Satiro.

Ao meu orientador, professor Dr. Vandenberg, pela paciência, dedicação e contribuição para a construção deste trabalho.

A todos que contribuíram de forma direta ou indiretamente para a construção do mesmo.

Por fim, à CAPES pela concessão da bolsa.

Resumo

Dentro do contexto de projetar esquema de comunicação digital, é necessário estabelecer um procedimento que permita o sigilo dos dados enviados por meio de mensagens eletrônicas. Nesta direção, a Teoria dos Códigos desempenha um papel central, pois seu desenvolvimento ao longo dos anos possibilitou o avanço de novas técnicas de comunicação eletrônica com maior segurança. Em particular, a Criptografia, que emprega elementos da Teoria dos Códigos, tem sido empregada cada vez mais e usada todas as vezes que se deseja transmitir uma mensagem digital, na qual apenas o remetente e o legítimo destinatário possam conhecer seu conteúdo. É neste processo que consideramos alguns conceitos da Teoria Elementar dos Números, que são base para a fundamentação matemática necessária para o desenvolvimento de elementos da Criptografia. A partir disso, apresentamos neste trabalho alguns resultados necessários da Teoria dos Números de modo a apresentar alguns métodos criptográficos.

Palavras Chaves: Aritmética. Criptografia. RSA.

Abstract

Within the context of designing a digital communication scheme, it is necessary to establish procedures to safeguard the confidentiality of data sent by electronic messages. In this sense, Coding Theory plays a central role. Since its development over the years, it has enabled the advancement of new electronic communication techniques with greater security. In particular, Cryptography that employs elements of Coding Theory has been increasingly employed and used every time a digital message is transmitted, in such a way that only the sender and the legitimate recipient may know its contents. It is within this process that we contemplate some concepts of Elementary Number Theory, which are the basis for the mathematical foundation necessary for the development of elements of Cryptography. Consequently, in this paper, we present some necessary results of the Number Theory to present some cryptographic methods.

Keywords: Arithmetic. Cryptografy. RSA.

Conteúdo

1 Introdução **1**

2 Números Inteiros e Propriedades **5**
2.1 Divisibilidade e Propriedades 5
2.2 Algoritmo da Divisão 7
2.3 Máximo Divisor Comum e Mínimo Múltiplo Comum 9
2.3.1 Máximo Divisor Comum 9
2.3.2 O Algoritmo de Euclides 11
2.3.3 Mínimo Múltiplo Comum 13
2.4 Números Primos 14
2.4.1 Teorema Fundamantal da Aritmética 14
2.4.2 O Crivo de Eratóstenes 16
2.4.3 A Infinidade dos Primos 18

3 Congruências **19**
3.1 Definição e Propriedades Básicas 19
3.2 Congruências Lineares 23
3.3 A função φ de Euler 26

4 Criptografia e Teoria dos Códigos **31**
4.1 Elementos da Criptografia 32
4.2 Cifra de César 32
4.3 Cifras Afins 35
4.4 Sistema RSA 37
4.5 Cifra de Hill 41
4.6 Considerações Finais 45

Capítulo 1

Introdução

A Teoria dos Números se dedica ao estudo dos números inteiros e suas generalizações. Em geral, esse estudo está relacionado com soluções de problemas diofantinos, ou seja, problemas que requerem solução de equação ou de sistema de equações com valores inteiros para as suas incógnitas.

O eminente teórico dos números Leonard Dickson (1874-1954) disse uma vez:

Graças a Deus que a Teoria dos Números é imaculada por qualquer aplicação.

Esta frase nos mostra que alguns teóricos dos números não se preocupavam com futuras aplicações de seus resultados na vida real. Alguns até nem acreditavam que um dia tais resultados viessem a ser usados em outras áreas da matemática, como é o caso do matemático inglês G. H. Hardy (1877-1947). Mas, atualmente, aplicações em diversas áreas tais como Física, Química, Acústica, Biologia, e, em especial, em Ciência da Computação, Codificação e Criptografia, fazem da Teoria dos Números mais atraente.

A Teoria dos Código Corretores de Erros dedica-se ao estudo das formas organizadas de se acrescentar algum dado adicional a cada informação que se deseja transmitir ou armazenar, que permita, ao recuperar a informação, detectar e corrigir erros. Essa teoria teve inicio em 1948, com os resultados obtidos pelo matemático americano Claude E. Shannon (1916-2001). Em seus resultados, Shannon mostrou que, usando códigos corretores de erros, é possível projetar sistemas de comunicações digitais com probabilidade de erro tão pequena quanto se queira. A partir daí, surgiram as pesquisas em busca dos bons códigos previstos pela teoria de Shannon.

Por outro lado, a Criptografia, que emprega resultados da Teoria dos Códigos, surge todas as vezes que se deseja enviar e receber mensagens sigilosas, de modo que apenas o rementente e o destinatário possam entender o conteúdo. Hoje em dia, a Criptografia se faz sempre presente em transações bancárias, obtenção de dados via satélite, acesso a emails, etc. É de fato um campo científico de investigação, e faz uso de resultados substanciais da Teoria dos Números.

A Criptografia se preocupava inicialmente com o fornecimento de sigilo de mensagens escritas. Seus princípios se aplicam igualmente para garantir o fluxo de dados entre computadores, a voz digitalizada, codificação do sinal de fax e televisão. Por exemplo, a maioria dos satélites rotineiramente criptografa o fluxo de dados para a partir de estações terrestres fornecer tanto privacidade quanto segurança para seus assinantes.

Criptografia (de Kryptos em grego, "oculto", e graphein. "escrever") é o estudo dos princípios e técnicas pelas quais informações podem ser escondidas em mensagens cifradas e, mais tarde, reveladas por usuários legítimos que utilizam a chave secreta, mas em que é impossível ou computacionalmente impossível para uma pessoa não autorizada a fazê-lo. Cryptanalysis (de Kryptos em grego, e analyein, "para soltar") é a ciência (e a arte) de recuperar informações de textos cifrados, sem conhecimento das chaves.

A Criptografia moderna é o estudo dos sistemas matemáticos para resolver os dois seguintes tipos principais de problemas de segurança: **privacidade** e **autenticação**. Um sistema de privacidade evita a extração de informações por partes não autorizadas de mensagens transmitidas através de um canal público e muitas vezes inseguro, assegurando, assim, ao remetente de uma mensagem que ela só vai ser lida pelo *destinatário pretendido*. Já um sistema de autenticação impede que a injeção não autorizada de mensagens em um canal público, garantindo o receptor de uma mensagem legitimidade de seu remetente. Basicamente, existem dois tipos diferentes de sistemas criptográficos: *sistemas de criptografia de chave secreta* (também chamados de sistemas de criptografia simétrica), e os *sistemas de criptografia de chave pública* (também chamados de sistemas de criptografia assimétrica).

Este trabalho tem por objetivo apresentar algumas formas de Criptografia. Não obstante o uso de resultados que, em geral, não são vistos no ensino básico (algumas propriedades dos números primos, por exemplo), a abordagem feita aqui sobre essas formas foi feita de modo mais natural possível, para que o leitor, após um contato breve com alguns resultados preliminares, possa assimilar a proposta em que o texto se insere.

O trabalho está dividido em três capítulos da seguinte forma:

No Capítulo 2, apresentamos os resultados sobre os números inteiros, destacando o conceito de divisibilidade com alguns resultados clássicos inerentes, os quais se destacam o Algoritmo da Divisão, Máximo Divisor Comum, Mínimo Múltiplo Comum e, como não poderia deixar de ser, os relacionados aos números primos, tais como a infinidade dos primos e o Teorema Fundamental da Aritmética. Esses números são os mais importantes números inteiros e são extremamente úteis para o estudo da Criptografia, em especial, a Criptografia RSA[1].

No Capítulo 3, apresentamos o conceito de congruência com suas principais propri-

[1]Representa as iniciais dos inventores do código, R.L. Rivest, A. Shamir e L. Adleman.

edades; aproveitamos este capítulo para abordar os tópicos primordiais que são usados na Criptografia, como por exemplo, os relacionados à função φ de Euler, e, é claro, o Teorema de Euler, que é uma generalização do Teorema de Fermat.

No Capítulo 4, abordamos alguns métodos utilizados desde épocas remotas até aos dias atuais, mostrando suas finalidades, bem como suas necessidades de aperfeiçoamento, até chegar no método RSA, resultado principal, que é um dos principais métodos de Criptografia de chave pública utilizados atualmente; isso se deve à sua eficiência no que tange a quebra do código. Finalizando, é apresentado o método criptográfico chamado *Cifra de Hill*, o qual consiste no uso de matrizes para codificar e decodificar uma mensagem.

Capítulo 2

Números Inteiros e Propriedades

Neste capítulo, vamos considerar alguns resultados básicos sobre os números inteiros, os quais serão úteis para o desenvolvimento do texto. Essencialmente, são resultados iniciais vistos num curso inicial de Teoria Elementar dos Números. As referências [6] e [8] abordam os tópicos aqui estudados.

2.1 Divisibilidade e Propriedades

O conjunto dos números inteiros é indicado por $\mathbb{Z}$, ou seja,

$$\mathbb{Z} = \{\ldots, \pm 3, \pm 2, \pm 1, 0\}.$$

Alguns resultados básicos relativos às operações de adição e multiplicação usuais sobre $\mathbb{Z}$, bem como os relativos à relação menor ou igual " $\leq$ ", podem ser vistos nas referências [6] e [8] . Essas propriedades serão eventualmente usadas ao longo do texto.

Dados dois números inteiros a e b, com $b \neq 0$, nem sempre a fração a/b é número inteiro, ou seja, nem sempre existe um número inteiro c tal que $a = b \cdot c$. Por exemplo, para $a = 2$ e $b = 4$, na igualdade $2 = 4 \cdot c$, $c = 1/2$. Isso motiva a definição do conceito de divisibilidade nos inteiros.

Para evitar repetições desnecessárias, as letras a, b, c, entre outras, irão representar, nesta seção, sempre números inteiros, a menos que seja mencionado o contrário.

Definição 2.1.1 *Dizemos que b **divide** a, em símbolos $b|a$, se existir um inteiro c tal que*

$$a = bc.$$

*Dizemos ainda que a é **divisível** por b, b é um **divisor** de a ou que a é um **múltiplo** de b.*

Com isso,

$$b|a \;\Leftrightarrow\; a = bc \text{ para algum } c \in \mathbb{Z}.$$

Caso contrário, dizemos que b não divide a, em símbolos $b \nmid a$. Por exemplo, $8|24$, $7 \nmid 10$.

Notemos que se b é um divisor de a, então $-b$ também o é, pois $a = bc$ implica em $a = (-b)(-c)$. Devido a isso, os divisores de um número sempre ocorrem aos pares, e, assim, para determinar todos os divisores de um número, é suficiente determinar apenas seus divisores positivos. O conjunto de divisores positivos de um inteiro a será representado por D_a, e o conjunto de seus múltiplos positivos por M_a. Daí,

$$D_a = \{n \in \mathbb{N} : n|a\} \quad \text{e} \quad M_a = \{n \in \mathbb{N} : a|n\}.$$

Notemos que, $D_a = D_{-a}$ e $M_a = M_{-a}$.

O conjunto D_a é sempre finito, pois se $b|a$, com $a \neq 0$, então $|b| \leq |a|$; e como $1|a$, $D_a \neq \varnothing$. Já o conjunto M_a é sempre infinito e contém $|a|$. Por exemplo,

$$D_{12} = \{1, 2, 3, 4, 6, 12\} \quad \text{e} \quad M_{12} = \{12, 24, 36, \ldots\}.$$

Proposição 2.1.2 *Em $\mathbb{Z}$ valem as seguintes propriedades:*

(1) *Os únicos divisores de 1 são 1 e -1.*

(2) *Se $a|b$ e $b|a$, então $a = \pm b$.*

Demonstração: (1) Se b é um divisor de 1, então $|b| \leq 1$, ou seja, $0 < |b| \leq 1$, e como não existe inteiro entre 0 e 1, segue que $|b| = 1$, isto é, $b = \pm 1$.

(2) Por hipótese, $b = c_1 \cdot a$ e $a = c_2 \cdot b$, com $c_1, c_2 \in \mathbb{Z}$. Com isso, $b = (c_1 c_2)b$ e, assim, $c_1 = c_2 = \pm 1$, isto é, $a = \pm b$. □

A seguir, apresentamos algumas propriedades elementares da divisibilidade.

Teorema 2.1.3 *A divisibilidade tem as propriedades:*

(1) *Se $a|b$ e $b|c$, então $a|c$.*

(2) *Se $a|b$ e $c|d$, então $ac|bd$.*

(3) *Se $a|b$ e $a|c$, então $a|(mb + nc)$, $\forall\ m, n \in \mathbb{Z}$.*

Demonstração: (1) Por hipótese, $b = \alpha_1 a$ e $c = \alpha_2 b$, com $\alpha_1, \alpha_2 \in \mathbb{Z}$. Substituindo o valor de b na segunda igualdade, temos $c = (\alpha_2 \alpha_1)a$, ou seja, $a|c$.

(2) Sejam $b = \beta_1 a$ e $d = \beta_2 c$, com $\beta_1, \beta_2 \in \mathbb{Z}$. Multiplicando as igualdades membro a membro, $bd = (\beta_1 \beta_2)(ac)$, ou seja, $ac|bd$.

(3) Temos que $b = a\gamma_1$ e $c = a\gamma_2$, com $\gamma_1, \gamma_2 \in \mathbb{Z}$. Por outro lado, dados $m, n \in \mathbb{Z}$, obtemos $mb = ma\gamma_1$ e $nc = na\gamma_2$. Daí, $mb + nc = ma\gamma_1 + na\gamma_2 = a(m\gamma_1 + n\gamma_2)$. Portanto, $a|(mb + nc)$. □

2.2 Algoritmo da Divisão

De acordo com o que já frisamos, nem sempre pode-se dividir um número inteiro por outro de maneira a obter um número inteiro, isto é, a divisão em questão pode não ser exata. Por exemplo, na divisão de 17 por 3,

$$17 = 3 \cdot 5 + 2.$$

Em outras palavras, ao dividir 17 objetos entre 3 pessoas, de maneira que cada uma receba sempre a mesma quantidade inteira de objetos, cada uma delas receberá 5 objetos e ainda restará 2 objetos.

O Algoritmo da Divisão é um dos resultados mais básicos e importantes da Teoria dos Números, sendo familiar para muitos desde os estudos da escola secundária. Seu resultado exprime o fato que, em $\mathbb{Z}$, é sempre possível a divisão com restos nas seguintes condições:

Teorema 2.2.1 ***(Algoritmo da Divisão)*** *Sejam a e b inteiros, com $b > 0$. Então, existem únicos inteiros q e r tais que*

$$a = bq + r, \quad com \quad 0 \leq r \leq b.$$

Demonstração: (Existência): Vamos considerar o conjunto

$$L = \{a - bq : q \in \mathbb{Z} \quad \text{e} \quad a - bq \geq 0\}.$$

Primeiramente, mostraremos que L não é vazio. Desde que $b \geq 1$, então $|a| \cdot b \geq |a|$. Com isso,

$$a - (-|a|) \cdot b = a + |a| \cdot b \geq a + |a| \geq 0.$$

Como $x = a - (-|a|) \cdot b$ é da forma $a - bq$, segue que $x \in L$. Sendo L um conjunto limitado inferiormente e não vazio, então, Pelo Princípio da Boa Ordenação[1], L possui um menor elemento r. Assim, $r \geq 0$ e

$$r = a - bq, \quad \text{com} \quad q \in \mathbb{Z}.$$

Nestas condições, temos que $r < b$, pois caso contrário, $r - b \geq 0$ e

$$r - b = a - bq - b = a - b(q + 1).$$

Logo, $r - b \in L$ e $r - b < r$, o que é um absurdo, pois r é o menor termo de L. Isso prova a existência dos inteiros q e r.
(Unicidade): Sejam $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = bq_1 + r_1, \quad \text{com} \quad 0 \leq r_1 \leq b.$$

[1]Esse princípio assegura que todo subconjunto não vazio X de $\mathbb{N}$ possui menor elemento, ou seja, existe $m \in X$ tal que $m \leq x$, para todo $x \in X$.

Dessa forma, $bq + r = bq_1 + r_1$, ou seja,

$$r - r_1 = b(q_1 - q) \;\Rightarrow\; b|(r - r_1).$$

Como $|r - r_1| < b$, segue que, $r - r_1 = 0$, isto é, $r = r_1$. Consequentemente, $q = q_1$, pois $b \neq 0$. □

Os inteiros q e r, apresentados no Teorema 2.2.1, são chamados de **quociente** e **resto** da Divisão Euclidiana de a por b, respectivamente. Às vezes, r também é chamado de **resto** de a **módulo** b.

Exemplo 2.2.2 Calcular o quociente e o resto da divisão de $a = 25$ por $b = 11$.

Solução: Utilizando o Algoritmo da Divisão, $25 = 11 \cdot 2 + 3$. Daí, o quociente é 2 e o resto é 3. △

Exemplo 2.2.3 Calcular o quociente e o resto da divisão de $a = -103$ por $b = 7$.

Solução: Utilizando o Algoritmo da Divisão, $-103 = 7 \cdot (-15) + 2$. Daí, o quociente é -15 e o resto é 2. △

Exemplo 2.2.4 Mostrar que todo quadrado perfeito é da forma $4k$ ou $4k + 1$.

Solução: Considere $a \in \mathbb{Z}$, e suponhamos que a seja um número par. Logo, $a = 2q$ e, daí, $a^2 = 4q^2 = 4k$, com $k = q^2$. Por outro lado, se a é ímpar, $a = 2q + 1$, $a^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1 = 4k + 1$, com $k = q^2 + q$. Assim, todo quadrado perfeito é da forma $4k$ ou $4k + 1$. △

Utilizando o Algoritmo da Divisão, se a é um inteiro qualquer, então ao efetuar a divisão por 2, os possiveis restos da divisão são 0 ou 1, ou seja,

$$a = 2q + r, \quad \text{com} \quad 0 \leq r \leq 1.$$

Quando $r = 0$, $a = 2k$; neste caso, dizemos que é um número **par**. Quando $r = 1$, $a = 2k + 1$, que é chamado de número **ímpar**.

Pela **paridade** de um inteiro queremos dizer que ele é par ou ímpar. Se P e I indicam os conjuntos dos números pares e ímpares, respectivamente, então

$$P = \{2k : k \in \mathbb{Z}\} \quad \text{e} \quad I = \{2k + 1 : k \in \mathbb{Z}\}.$$

É simples verificar que:

(1) $P \cap I = \varnothing$.

(2) Se $x, y \in P$, então $x \pm y \in P \quad \text{e} \quad x \cdot y \in P$.

(3) Se $x, y \in I$, então $x \pm y \in P \quad \text{e} \quad x \cdot y \in I$.

(4) Se $x \in P$ e $y \in I$, então $x \pm y \in I \quad \text{e} \quad x \cdot y \in P$.

2.3 Máximo Divisor Comum e Mínimo Múltiplo Comum

Nessa seção, consideramos os conceitos de *máximo divisor comum* (mdc) e de *mínimo múltiplo comum* (mmc). Tais conceitos são relevantes para se estabelecer propriedades da divibilidade.

2.3.1 Máximo Divisor Comum

Na educação básica, para determinar o *mdc* de dois inteiros, é natural encontrar todos os seus divisores positivos, posteriormente, verificar os divisores comuns e, finalmente, identificar o maior entre eles, que é o *mdc* entre eles. De maneira geral, dados dois inteiros não nulos a e b, tomemos

$$D_a = \{n \in \mathbb{N} : n|a\} \quad \text{e} \quad D_b = \{n \in \mathbb{N} : n|b\}.$$

Como $1|a$ e $1|b$, então $1 \in D_a \cap D_b$, ou seja, $D_a \cap D_b \neq \varnothing$. Além disso, $D_a \cap D_b$ é um conjunto finito e, por isso, possui um maior elemento, o qual é chamado de *máximo divisor comum* (mdc) de a e b, que denotaremos por

$$mdc(a, b).$$

Por exemplo, para $a = 12$ e $b = 20$, temos que $D_a = \{1, 2, 3, 4, 6, 12\}$ e $D_b = \{1, 2, 4, 5, 10, 20\}$. Assim, $D_a \cap D_b = \{1, 2, 4\}$, ou seja, $mdc(12, 20) = 4$.

Por construção, é verdade que $mdc(a, b) = mdc(b, a)$. Além disso, se $a = 0$, então o conjunto D_a é infinito, pois qualquer inteiro divide 0. Por isso, covenciona-se que $mdc(0, 0) = 0$.

Fomalmente, o conceito de máximo divisor comum é definido como segue:

Definição 2.3.1 *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{N}$ é o máximo divisor comum de a e b quando as seguintes condições são satisfeitas:*

(a) $d|a$ e $d|b$.

(b) Se $c|a$ e $c|b$, então $c|d$.

Ou seja, o máximo divisor comum de a e b é um número natural que divide a e b, bem como é divisível por todos os divisores comuns de a e b. Em alguns casos, é imediato o cálculo do *mdc* de dois inteiros. De fato,

1. $mdc(0, a) = |a|$.

2. $mdc(1, a) = 1$.

3. $mdc(a, a) = |a|$.

Segue também que, para todo $b \in \mathbb{Z}$,

$$a|b \;\Leftrightarrow\; mdc(a,b) = |a|.$$

Além disso,

$$mdc(a,b) = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b). \tag{2.1}$$

Devido a isso, vamos considerar apenas a e b positivos.

O Teorema que segue nos mostra que $mdc(a,b)$ é uma combinação linear de a e b. Tal identidade é bastante proveitosa para se estabelecer importantes resultados da Teoria dos Números.

Teorema 2.3.2 ***(Bachet-Bézout)*** *Se $d = mdc(a,b)$, então existem inteiros x_1 e y_1 tais que*

$$d = ax_1 + by_1.$$

Demonstração: Consideremos o conjunto

$$W = \{ax + by : x, y \in \mathbb{Z} \quad \text{e} \quad ax + by > 0\}.$$

Notemos que W é não vazio, pois para $x = y = 1$,

$$a \cdot 1 + b \cdot 1 = a + b > 0 \;\Rightarrow\; a + b \in W.$$

Logo, pelo Princípio da Boa Ordenação, W possui um menor elemento, $\alpha = \min W$. Mostremos que $\alpha = d$. Como $\alpha \in W$, existem $x_1, y_1 \in \mathbb{Z}$ tais que

$$\alpha = ax_1 + by_1. \tag{2.2}$$

Usando o Algoritmo da Divisão com a e α,

$$a = \alpha q + r, \quad \text{com} \quad 0 \leq r \leq \alpha. \tag{2.3}$$

Agora, substituindo o valor de α em (2.2) na expressão de (2.3),

$$\begin{aligned} a = \alpha q + r \;\Rightarrow\; r &= a - \alpha q \\ &= a - (ax_1 + by_1)q \\ &= a - ax_1 q + b(-qy_1), \end{aligned}$$

ou seja,

$$r = a(1 - x_1 q) + b(-qy_1).$$

Temos que $r = at + bs$, com $t = 1 - x_1 q$ e $s = -qy_1$. Se $r > 0$, então $r \in W$ e $r < \alpha$, contrariando o fato de $\alpha = \min W$. Logo, $r = 0$, isto é, $a = \alpha q$. O que mostra que $\alpha | a$. Analogamente, prova-se que $\alpha | b$.

Como $d = mdc(a,b)$, então $a = d\alpha_1$ e $b = d\alpha_2$. Utilizando (2.2),

$$\alpha = (d\alpha_1)x_1 + (d\alpha_2)y_1 = d(\alpha_1 x_1 + \alpha_2 y_1),$$

ou seja, $d|\alpha$. Por outro lado, $\alpha | d$, pois $d = mdc(a,b)$. Desse modo, $\alpha = d$, e, com isso, $d = ax_1 + by_1$. □

2.3.2 O Algoritmo de Euclides

O $mdc(a, b)$ pode ser calculado, sem grandes problemas, quando os números a e b são relativamente pequenos, mas se ambos forem relativamente grandes? Descrever os divisores de a e b e depois identificar o maior divisor comum entre eles não é, em geral, uma tarefa fácil. Por exemplo, calcular o $mdc(4562, 76489)$ é uma tarefa no mínimo tediosa.

O lema que segue, que é devido a Euclides, nos conduzirá a um algoritmo extremamente eficiente para o cálculo do mdc entre quaisquer dois inteiros.

Lema 2.3.3 ***(Euclides)*** *Se $a = bq + r$, então $mdc(a, b) = mdc(b, r)$.*

Demonstração: Mostremos que $D_a \cap D_b = D_b \cap D_r$, pois os conjuntos sendo iguais, seus máximos também serão. Se $d \in D_a \cap D_b$, então $d|a$ e $d|b$. Como $r = a - qb$, $d|r$, isto é, $d \in D_b \cap D_r$. Agora, para $d \in D_b \cap D_r$, $d|b$ e $d|r$. Daí, $d|(bq + r) = a$, ou seja, $d \in D_a \cap D_b$. Portanto, $D_a \cap D_b = D_b \cap D_r$, isto é, $mdc(a, b) = mdc(b, r)$. □

O resultado do lema anterior é válido mesmo que os inteiros q e r não sejam o quociente e resto da divisão de a por b. Por exemplo, $367 = 43 \cdot 8 + 23$, implica em $mdc(367, 8) = mdc(8, 23)$.

Vamos agora determinar o mdc de dois números inteiros utilizando o Lema 2.3.3.

Exemplo 2.3.4 Calcular $d = mdc(248, 102)$ e expressá-lo da forma que foi abordado no Teorema 2.3.2.

Solução: De acordo com o Teorema 2.2.1, para $a = 248$ e $b = 102$,

$$\begin{array}{rcrcrcl} 248 & = & 102 \cdot 2 + 44 & \Rightarrow & mdc(248, 102) & = & mdc(102, 44), \\ 102 & = & 44 \cdot 2 + 14 & \Rightarrow & mdc(102, 44) & = & mdc(44, 14), \\ 44 & = & 14 \cdot 3 + 2 & \Rightarrow & mdc(44, 14) & = & mdc(14, 2), \\ 14 & = & 2 \cdot 7 + 0 & \Rightarrow & mdc(14, 2) & = & mdc(2, 0). \end{array} \tag{2.4}$$

Logo, $mdc(248, 102) = mdc(2, 0) = 2$.

Determinemos agora inteiros x_1 e y_1 tais que $2 = 248 \cdot x_1 + 102 \cdot y_1$. Para tal, vamos isolar os restos não nulos das divisões no sentido inverso das igualdades (2.4). Fazendo isso sucessivamente, temos

$$\begin{array}{rcrcl} 2 & = & 44 - 3 \cdot 14 & = & 44 - 3 \cdot (102 - 2 \cdot 44) \\ & & & = & 7 \cdot 44 - 3 \cdot 102 \\ & & & = & 7 \cdot (248 - 102 \cdot 2) - 3 \cdot 102 \\ & & & = & 7 \cdot 248 - 17 \cdot 102. \end{array}$$

Logo, $x_1 = 7$ e $y_1 = -17$. △

Definição 2.3.5 *Dois inteiros a e b são ditos* ***primos entre si*** *quando $mdc(a, b) = 1$.*

Por exemplo, 4 e 15 são primos entre si, pois $mdc(4, 15) = 1$, mas 8 e 20 não são, já que $mdc(20, 8) = 4$.

Corolário 2.3.6 *Dois inteiros a e b são primos entre si se, e somente se, existem $x, y \in \mathbb{Z}$ onde $1 = ax + by$.*

Demonstração: Se $mdc(a, b) = 1$, o Teorema 2.3.2 mostra que existem inteiros x e y, em que $1 = ax + by$. Reciprocamente, suponhamos que $1 = ax + by$ com $x, y \in \mathbb{Z}$, e seja $d = mdc(a, b)$. Como $d|a$ e $d|b$, segue que $d|(ax + by) = 1$. Logo, $d = 1$, pois $d > 0$. Assim, a e b são primos entre si. □

Corolário 2.3.7 *Sejam $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração: Temos por hipótese que $bc = at$, $t \in \mathbb{Z}$. Pelo Corolário 2.3.6, $1 = ax + by$, com $x, y \in \mathbb{Z}$. Multiplicando esse última expressão por c, obtemos

$$\begin{aligned} c &= cax + cby &&= cax + aky \\ &&&= a(cx + ky). \end{aligned}$$

Ou seja, $a|c$. □

Por exemplo, $4|24$ e $24 = 8 \cdot 3$. Como $mdc(4, 3) = 1$, então $4|8$.

Corolário 2.3.8 *Sejam $a, b \in \mathbb{Z}$ tais que $mdc(a, b) = 1$. Se $a|c$ e $b|c$, então $ab|c$.*

Demonstração: Por hipótese, como $mdc(a, b) = 1$, temos

$$1 = ax + by, \quad \text{com } x, y \in \mathbb{Z}. \tag{2.5}$$

Por outro lado, existem $\theta_1, \theta_2 \in \mathbb{Z}$ tais que $c = a\theta_1$ e $c = b\theta_2$. Logo,

$$cb = ab\theta_1 \quad \text{e} \quad ca = ab\theta_2.$$

Agora, multiplicando ambos os lados da igualdade (2.5) por c, segue que

$$\begin{aligned} c &= acx + bcy &&= ab\theta_2 x + ab\theta_1 y \\ &&&= ab(\theta_2 x + \theta_1 y), \end{aligned}$$

isto é, $ab|c$. □

2.3.3 Mínimo Múltiplo Comum

Na educação básica, assim como ocorre com o *mdc*, o conceito do mínimo múltiplo comum (*mmc*) entre dois inteiros é apresentado pelo método da fatoração de dois números em fatores primos. Após isso, realiza-se o produto dos fatores para o determiná-lo.

Exemplo 2.3.9 Calcular o *mmc* dos entre os números 45 e 20.

Solução: Decompondo em fatores primos,

$$\begin{array}{r||l} 45, 20 & 2 \\ 45, 10 & 2 \\ 45, 5 & 3 \\ 15, 5 & 3 \\ 5, 5 & 5 \\ 1, 1 & \end{array}$$

ou seja, $mmc(45, 20) = 2^2 \cdot 3^2 \cdot 5 = 180$. △

O que em geral se faz é o seguinte: consideramos dois inteiros não nulos a e b, e tomamos os conjuntos

$$M_a = \{n \in \mathbb{N} : a|n\} \quad \text{e} \quad M_b = \{n \in \mathbb{N} : b|n\}.$$

É facil verificar que $|ab| \in M_a$ e $|ab| \in M_b$, isto é, $|ab| \in M_a \cap M_b \subset \mathbb{N}$. Além disso, como $M_a \cap M_b$ é limitado inferiormente, então ele possui um menor elemento, chamado de *mínimo múltiplo comum* de a e b, que é indicado por $mmc(a, b)$. Formalmente, temos:

Definição 2.3.10 *Sejam a e b inteiros não nulos. O número $m \in \mathbb{N}$ é o* ***mínimo múltiplo comum*** *de a e b quando as condições são satisfeitas:*

(a) *$a|m$ e $b|m$.*

(b) *Se $a|c$ e $b|c$, então $m|c$.*

Por exemplo,

$$mmc(3, 9) = 9, \quad mmc(4, 5) = 20.$$

Da mesma forma que temos para o *mdc*, também é válido e simples de verificar que, para quaisquer inteiros não nulos, a e b,

$$mmc(a, b) = mmc(-a, b) = mmc(a, -b) = mmc(-a, -b). \tag{2.6}$$

Com isso, é necessario calcular o *mmc* apenas entre inteiros positivos.

O próximo Teorema estabelece uma proveitosa relação entre o *mdc* e *mmc* de a e b, cuja prova pode ser encontrada em [8].

Teorema 2.3.11 *Dados dois naturais quaisquer a, b, sendo $d = mdc(a, b)$ e $m = mmc(a, b)$, temos*

$$m = \frac{ab}{d}.$$

Este Teorema nos mostra que $mmc(a, b) \leq ab$. Além disso, seu cálculo é obtido diretamente do cálculo de d.

Corolário 2.3.12 *Dados $a, b \in \mathbb{N}$, temos que $mmc(a, b) = ab$ se, e somente se, $mdc(a, b) = 1$.*

Exemplo 2.3.13 Calcular o $mmc(45, 20)$ e $mdc(12, 13)$.

Solução: Como $mdc(45, 20) = 5$, temos pelo Teorema 2.3.11,

$$m = \frac{45 \cdot 20}{5} = \frac{900}{5} = 180,$$

ou seja, $mmc(45, 20) = 180$. Também, desde que $mdc(12, 13) = 1$,

$$m = 12 \cdot 13 = 156,$$

isto é, $mmc(12, 13) = 156$. △

2.4 Números Primos

Os números primos são os principais números inteiros e, por isso, têm destaque especial na Teoria dos Números. Muitos problemas envolvendo esses inteiros já foram resolvidos, entretanto, ainda existem muitos para os quais não foram encontradas soluções e, por isso, são fontes de pesquisas científicas.

Vale ressaltar que o uso dos números primos é de fundamental importancia para o resultado principal desse trabalho, que será apresentado no Capítulo 4.

Nessa seção, vamos apresentar os resultados básicos sobre os números primos, cujo resultado principal é o Teorema Fundamental da Aritmética.

2.4.1 Teorema Fundamantal da Aritmética

O Teorema Fundamental da Aritmética (TFA) nos garante que todo inteiro $a \in \mathbb{Z} - \{0, \pm 1\}$ pode ser escrito como um produto de fatores primos, ou seja, os primos são suficientes para gerar todos os números inteiros, com exceção de 0 e ± 1. É, de fato, o principal resultado sobre esses números, sendo assim a base da Teoria dos Números.

Definição 2.4.1 *Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é chamado **primo,** quando seus únicos divisores positivos são 1 e $|p|$. Caso contrário, dizemos que p é **composto**.*

Já que o número 1 é o elemento neutro da multiplicação, ele não é primo nem composto. Além disso, temos que os números 2 e -2 são os únicos primos pares. Notemos ainda que um inteiro a é composto se, e somente se,

$$a = bc, \quad \text{com} \quad b, c \in \mathbb{Z} \quad \text{e} \quad 1 < |b|, |c| < |a|.$$

Neste caso, dizemos que b (c também) é um **divisor próprio** de a.

Já que p é primo se, e somente se, $-p$ também o é, vamos considerar apenas os primos positivos, e o conjunto desses primos será indicado por $\mathcal{P}$, que é um conjunto infinito. Os dez primeiros primos são

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots\}.$$

Vamos então para um resultado fundamental de divibilidade envolvendo números primos.

Proposição 2.4.2 *Sejam $a, b \in \mathbb{Z}$ e p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Temos que $mdc(a, p) = 1$ ou $mdc(a, p) = p$. Se $p \nmid a$, então $mdc(a, p) = 1$, que de acordo com o Corolário 2.3.7, implica em $p|b$. □

Teorema 2.4.3 ***(TFA)*** *Todo número natural $a > 1$ é escrito de forma única, a menos da ordem dos fatores, como um produto de números primos, ou seja,*

$$a = p_1 p_2 \ldots p_n,$$

onde $p_1, p_2, \ldots, p_n$ são primos.

Demonstração: Temos que mostrar a existência dos primos e a unicidade da fatoração. Consideremos o conjunto

$$A = \{a \in \mathbb{N} : a > 1 \quad \text{e} \quad a \neq p_1 p_2 \ldots p_n\}$$

onde $p_1, p_2, \ldots, p_n$ são primos. Devemos mostrar que $A = \varnothing$ para provar a existência dos primos. Por contradição, suponhamos que $A \neq \varnothing$. Logo, como A é limitado inferiormente, ele possui elemento mínimo m. Obviamente temos que m é composto, e, daí,

$$m = bc, \quad \text{com} \quad 1 < b, c < m.$$

Como $b < m$ e $c < m$, segue que $b, c \notin A$, pois $m = \min A$. Desse modo, b e c ou são primos ou produtos de primos. Por conseguinte, $m = bc$ é um produto de primos, o que é um absurdo. Com isso, $A = \varnothing$.

Para a unicidade da fatoração, admitamos que

$$a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m, \tag{2.7}$$

sendo $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m$ todos primos. Então,

$$p_1 | q_1 q_2 \ldots q_m,$$

ou seja, $p_1 | q_i$ para algum $i = 1, 2, 3, \ldots m$. Como p e q são primos, segue que $p_1 = q_i$. Sem perda de generalidade, suponhamos que $p_1 = q_1$. Pela lei do cancelamento, segue de (2.7) que

$$p_2 \ldots p_n = q_2 \ldots q_m.$$

Analogamente, temos que $p_2 = q_i$, para algum $i = 2, 3, \ldots, m$. Supondo $p_2 = q_2$, temos

$$p_3 p_4 \ldots p_n = q_3 q_4 \ldots q_m.$$

Neste processo, considerando $n > m$, resulta que

$$1 = p_{m+1} \ldots p_n,$$

o que é um absurdo. O caso $n < m$ pode ser obtido de modo análogo. Portanto, $m = n$, ou seja, $p_i = q_i$, para cada $i = 1, 2, 3, \ldots, n$. □

Na fatoração de um inteiro b, os fatores primos nem sempre são distintos. Por exemplo, $20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$. Por isso, o TFA pode ser reformulado da seguinte forma:

Corolário 2.4.4 *Todo número natural $a > 1$ pode ser escrito de modo único, a menos da ordem dos fatores, na forma*

$$a = p_1^{r_1} p_1^{r_2} \ldots p_k^{r_k}, \tag{2.8}$$

em que $p_1, p_2, \ldots, p_k$ são primos distintos e $r_1, r_2, \ldots, r_k$ são números naturais.

A representação em (2.8) é chamada de **fatoração canônica** de a em fatores primos.

Exemplo 2.4.5 A fatoração canônica de $a = 340$ é $2^2 \cdot 5 \cdot 17$.

2.4.2 O Crivo de Eratóstenes

É bem comum nos depararmos com o seguinte questionamento: dado um número inteiro, como verificar se ele é primo ou não? Para responder este questionamento, vamos utilizar um método bem clássico da Teoria dos Números, o Teste de Primalidade, o qual serve de base para um algoritmo, chamado de Crivo de Eratóstenes, que pode ser usado para determinar todos os números primos menores ou iguais a um número natural dado.

Teorema 2.4.6 ***(Teste de Primalidade)*** *Se $n > 1$ for composto, então n possui necessariamente, um divisor primo p tal que $p \leq \sqrt{n}$. Ou seja, se n não possui divisores diferentes de 1, menores ou iguais a $\sqrt{n}$, então n é primo.*

Demonstração: Seja n um número composto. Logo,

$$n = a \cdot b, \quad \text{com} \quad 1 < a, b < n.$$

Se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n,$$

o que é impossivel. Dessa forma, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Suponhamos que $a \leq \sqrt{n}$. Como $a > 1$, existe um primo p, com $p|a$. Já que $a|n$, segue que $p|n$ e $p \leq a \leq \sqrt{n}$. □

O Teorema 2.4.6 nos garante que para verificar se um inteiro $a > 1$ é primo, basta verificar sua divisibilidade pelos primos menores ou iguais a $\sqrt{a}$. Entretanto, esse processo quando aplicado em números relativamente grandes torna-se uma tarefa árdua, pois à medida que n cresce, sua raiz também cresce, mesmo que em proporções menores, ou seja,

$$\lim_{x \to \infty} \frac{x}{\sqrt{x}} = \infty.$$

Isto mostra a ineficiência desse teste para inteiros arbitrários. Por exemplo, para $a = 6478398479$, temos que $\left[\sqrt{6478398479}\right] = 80488$, ou seja, para verificar se a é primo através desse teste, teremos que determinar todos os primos menores ou iguais a 80448, o que não é nada prático. Do ponto de vista computacional, ainda não existe um algoritmo que seja eficiente para se testar a primalidade de um inteiro.

Exemplo 2.4.7 Dado o número $a = 131$, segue que $\left[\sqrt{131}\right] = 11$. Os primos menores ou iguais a 11 são $2, 3, 5, 7, 11$. Realizando os cálculos, temos que 131 não é divisivel por nenhum desses primos. Assim, 131 é primo.

O método de Eratóstenes para listar todos o primos menores ou iguais a n, consiste nos seguintes passos:

Passo 1: Descrever os números de forma ordenada a partir do 2,

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 \ldots, n. \tag{2.9}$$

Passo 2: Como 2 é primeiro primo que aparece em (2.9), vamos excluir todos os seus múltiplos maiores que 2:

$$2, 3, 5, 7, 9, 11, 13, 15, 17, 19, \ldots, n. \tag{2.10}$$

Passo 3: O primeiro número, cujos múltiplos não foram excluídos, que aparecem em (2.10), é 3. Como 3 é primo, então excluímos todos os seus múltiplos, exceto ele próprio:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 25, \ldots, n. \tag{2.11}$$

	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~~

Tabela 2.1: Primos Menores do que 100.

Passo 4: O primeiro número,cujos múltiplos não foram excluídos, que aparecem em (2.11), é 5; daí, excluindo todos os seus múltiplos, exceto ele próprio, obtemos

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots, n.$$

Todo esse processo é realizado até que o primeiro número não excluído seja maior do que $\sqrt{n}$. Na Tabela 2.1, temos os primos menores do que 100, obtidos através do Crivo de Eratóstenes. Vale ressaltar que foi necessário excluir apenas os múltiplos de 7, pois $\left[\sqrt{100}\right] = 10$.

2.4.3 A Infinidade dos Primos

Os números primos, assim como os compostos, são infinitos. A prova desse fato foi apresentada primeiro por Euclides (cerca de 300 a.C), o qual fez uso do método da redução ao absurdo.

Teorema 2.4.8 *O conjunto $\mathcal{P}$ dos números primos é infinito.*

Demonstração: Vamos supor por absurdo que o conjunto $\mathcal{P}$ seja finito, e sejam $p_1, p_2, \ldots, p_n$ todos os primos. Consideremos $a \in \mathbb{N}$ dado pelo produto dos $p_i's$ somado ao número 1, ou seja,

$$a = p_1 p_2 \ldots p_n + 1.$$

Como $a > 1$, então existe um primo p tal que $p|a$. Como $p_1, p_2, \ldots, p_n$ são os únicos primos, $p = p_i$ para algum $i = 1, 2, \ldots, n$. Sem perda de generalidade, vamos considerar $p = p_1$. Dessa forma,

$$p|(pp_2 \ldots p_n + 1),$$

ou seja, $p|1$, o que é uma contradição. Com isso, temos que $\mathcal{P}$ é infinito. □

Capítulo 3

Congruências

As congruências são, de maneira geral, uma grande ferramenta para mostrar importantes resultados da Teoria dos Números. A Teoria das Congruências ou Aritmética Modular tem aplicações em diversas áreas. A partir do conceito de congruência módulo m, obtemos a relação de equivalência " $\equiv (\mathrm{mod}\, m)$ ", a mais importante da Teoria dos Números, que gera o conjunto quociente $\mathbb{Z}_m$, o conjunto base da aritmética modular.

3.1 Definição e Propriedades Básicas

Consideremos m um número natural e a e b inteiros quaisquer. Dizemos que a é **congruente** a b **módulo** m, em símbolos,

$$a \equiv b \ (\mathrm{mod}\, m) \quad \text{ou} \quad a \equiv_m b,$$

quando m divide $a - b$. O inteiro m é chamado **módulo** da congruência.

Por exemplo, $7 \equiv 2 \ (\mathrm{mod}\, 5)$ e $11 \equiv 3 \ (\mathrm{mod}\, 4)$, pois, $5|(7-2)$ e $4|(11-3)$, respectivamente.

Se m não divide $a - b$, dizemos que a **não é congruente** a b módulo m ou que a é **incongruente** a b módulo m, representado por

$$a \not\equiv b \ (\mathrm{mod}\, m).$$

O fato $a \equiv b \ (\mathrm{mod}\, m)$ implica que

$$a = b + mk, \quad \text{com } k \in \mathbb{Z}.$$

A congruência $a \equiv b \ (\mathrm{mod}\, 1)$ sempre é satisfeita, pois 1 divide qualquer número inteiro. Por isso, na congruência $a \equiv b \ (\mathrm{mod}\, m)$, vamos sempre considerar $m \geq 2$.

Proposição 3.1.1 *Dados a, b, c inteiros quaisquer, temos que as seguintes propriedades são satisfeitas:*

(1) $a \equiv a (\mathrm{mod}\, m)$. ($\equiv_m$ ***é reflexiva***)

(2) *Se* $a \equiv b(\mathrm{mod}\, m)$*, então* $b \equiv a \,\mathrm{mod}\, m$*.* ($\equiv_m$ ***é simétrica***)

(3) *Se* $a \equiv b(\mathrm{mod}\, m)$ *e* $b \equiv c(\mathrm{mod}\, m)$*, então* $a \equiv c(\mathrm{mod}\, m)$*.* ($\equiv_m$ ***é transitiva***)

Demonstração: (1) Para qualquer inteiro a, $a - a = 0 = 0 \cdot m$, ou seja, $a \equiv a \pmod{m}$.

(2) Se $a \equiv b \,\mathrm{mod}\, m$, então $a - b = mk$, com $k \in \mathbb{Z}$. Com isso, $b - a = m(-k)$ e $-k \in \mathbb{Z}$, isto é, $b \equiv a \pmod{m}$.

(3) Como que $a \equiv b(\mathrm{mod}\, m)$ e $b \equiv c(\mathrm{mod}\, m)$, existem $k_1, k_2 \in \mathbb{Z}$, tais que

$$a - b = mk_1 \quad \text{e} \quad b - c = mk_2.$$

Somando membro a membro estas igualdades,

$$a - b + b - c = a - c = m(k_1 + k_2),$$

ou seja, $a \equiv c(\mathrm{mod}\, m)$. □

Este resultado mostra que " $\equiv_m$" é uma relação de equivalência[1] sobre $\mathbb{Z}$, chamada **relação de congruência módulo** m. Através do algoritmo da divisão, pode-se mostrar que o conjunto quociente de $\mathbb{Z}$ por " $\equiv_m$", denotado por $\mathbb{Z}_m$, contém m classes de equivalências. Especificamente,

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}.$$

Por exemplo, para $m = 3$, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, em que

$$\begin{aligned} \bar{0} &= \{3k : k \in \mathbb{Z}\}, \\ \bar{1} &= \{3k + 1 : k \in \mathbb{Z}\}, \\ \bar{2} &= \{3k + 2 : k \in \mathbb{Z}\}. \end{aligned}$$

Teorema 3.1.2 *Dados* a, b, c, d *inteiros quaisquer, temos que:*

(1) *Se* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$*, então*

$$(a + c) \equiv (b + d) \pmod{m} \quad e \quad ac \equiv bd \pmod{m}.$$

(2) *Se* $a \equiv b \pmod{m}$*, então*

$$(a + c) \equiv (b + c) \pmod{m} \quad ac \equiv bc \pmod{m}.$$

(3) *Se* $a \equiv b \pmod{m}$*, então* $a^k \equiv b^k \pmod{m}$ *para qualquer* $k \in \mathbb{N}$.

[1]Na referência [8], o leitor poderá estudar os conceitos e resultados básicos sobre *relação de equivalência* e *classe de equivalência*.

(4) *Se* $(a+c) \equiv (b+c) \pmod{m}$*, então* $a \equiv b \pmod{m}$.

Demonstração: Vamos provar (1), (2) e (3).

(1) Por hipótese,

$$a = b + k_1 m \quad \text{e} \quad c = d + k_2 m. \tag{3.1}$$

Somando membro a membro estas igualdades, temos

$$a + c = b + d + (k_1 + k_2)m,$$

ou seja, $(a+c) \equiv (b+d) \pmod{m}$. Por outro lado, multiplicando (3.1) membro a membro, temos

$$ac = (b + k_1 m)(d + k_2 m) = bd + (bk_2 + dk_1 + k_1 k_2 m)m.$$

Isto é, $ac \equiv bd \bmod m$.

(2) Temos que $c \equiv c \pmod{m}$. Dessa forma, segue de (1) que

$$(a+c) \equiv (b+c) \pmod{m} \quad \text{e} \quad ac \equiv bc \pmod{m}.$$

(3) Provemos por indução que $a^k \equiv b^k \pmod{m}$ para todo inteiro $k \geq 1$. Por hipótese, $a \equiv b \pmod{m}$. Logo, o resultado é válido para $k = 1$. Suponhamos, por hipótese de indução, que $a^k \equiv b^k \pmod{m}$, com $k \geq 1$. Como $a \equiv b \pmod{m}$, então segue do item (1) que $a^{k+1} \equiv b^{k+1} \pmod{m}$. Portanto, $a^k \equiv b^k \pmod{m}$ para todo $k \geq 1$. □

Vejamos a seguir algumas aplicações das propriedades anteriores.

Exemplo 3.1.3 Mostrar que $10^{2n} \equiv 1 \pmod{11}$ e $10^{2n+1} \equiv (-1) \pmod{11}$, para todo $n \in \mathbb{N}$.

Solução: Como, $10^2 = 100 \equiv 1 \pmod{11}$, então elevendo ambos os lados desta congruência a n, temos

$$\left(10^2\right)^n = 10^{2n} \equiv 1^n \pmod{11}.$$

Por outro lado, multiplicando membro a membro esta congruência com $10 \equiv 10 \pmod{11}$,

$$10^{2n} \cdot 10 = 10^{2n+1} \equiv 10 \equiv -1 \pmod{11}.$$ △

Exemplo 3.1.4 Determinar o digito das unidades do número 3^{28}.

Solução: O problema equivale a determinar o inteiro a tal que

$$3^{28} \equiv a \pmod{10},$$

com $0 \leq a \leq 9$. Vamos determinar uma congruência base favorável para os cálculos e, assim, aplicar as propriedades de modo a chegarmos no que queremos. Um bom início é a congruência

$$3^2 \equiv 9 \equiv -1 \pmod{10}.$$

Elevando os membros dessa congruência a 14, obtemos

$$(3^2)^{14} = 3^{28} \equiv (-1)^{14} \pmod{10}.$$

Como $(-1)^{14} = 1$, segue que o dígito das unidades de 3^{28} é 1. △

Definição 3.1.5 *Se h e k são inteiros e $h \equiv k \pmod{m}$, dizemos que k é um* ***resíduo*** *de h* ***módulo*** *m.*

Vale ressaltar que um resíduo nem sempre é o resto de uma divisão. De fato, $10 \equiv 6 \pmod{4}$, mas $10 = 4 \cdot 2 + 2$, isto é, 6 é um resíduo de 10 módulo 4, mas o resto da divisão de 10 por 4 é 2.

Consideremos um inteiro a, e sejam q e r o quociente e resto da divisão de a por m, respectivamente,

$$a = qm + r, \quad \text{onde} \quad 0 \leq r \leq m - 1.$$

Como os elementos do conjunto $r \in \{1, 2, 3, \ldots, m-1\}$ são dois a dois incongruentes módulo m, segue que cada inteiro a é congruente a apenas um desse valores. Com isso, dizemos que o conjunto $\{1, 2, 3, \ldots, m-1\}$ é um *sistema completo de resíduos módulo m*. De uma maneira geral,

Definição 3.1.6 *Um conjunto de inteiros $\{a_1, a_2, \ldots, a_r\}$ é um* ***sistema completo de resíduos módulo*** *m quando*

(a) $a_i \not\equiv a_j \pmod{m}$ para $i \neq j$.

(b) Para todo inteiro b, existe a_i de modo que $b \equiv a_i \pmod{m}$.

Exemplo 3.1.7 O conjunto $\{6, 13, 20, 27, 28, 35\}$ é um sistema completo de resíduos módulo 6, pois além de seus inteiros serem incongruentes dois a dois módulo 6, temos sob a congruência módulo 6,

$$6 \equiv 0, \quad 13 \equiv 1, \quad 20 \equiv 2, \quad 27 \equiv 3, \quad 28 \equiv 4, \quad 35 \equiv 5.$$

Por outro lado, se b é um inteiro qualquer, então ele é da forma $b = 6q + r$, com $0 \leq r \leq 5$, ou seja, $b \equiv a_i \pmod{6}$, onde $a_i \in \{6, 13, 20, 27, 28, 35\}$. Assim, $\{6, 13, 20, 27, 28, 35\}$ é um sistema completo de resíduos módulo 6.

Teorema 3.1.8 *Se $\{a_1, a_2, \ldots, a_k\}$ é um sistema completo de resíduos módulo m, então $k = m$.*

Demonstração: Já vimos que $\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m. Assim, cada $a_i \in \{a_1, a_2, \ldots, a_k\}$ é congruente a exatamente um $r_i \in \{0, 1, 2, \ldots, m-1\}$. Isso implica que $k \leq m$. Por outro lado, como $\{a_1, a_2, \ldots, a_k\}$ é um sistema completo de resíduos módulo m, então cada r_i é congruente a exatamente um $a_i \in \{a_1, a_2, \ldots, a_k\}$. Por isso, $m \leq k$, ou seja, que $k = m$. □

Teorema 3.1.9 *Sejam a, b, c inteiros quaisquer. Então,*

$$ac \equiv bc \pmod{m} \;\Leftrightarrow\; a \equiv b \pmod{m/d},$$

com $d = mdc(c, m)$.

Demonstração: Se $ac \equiv bc \pmod{m}$, então

$$ac - bc = c(a - b) = km, \quad \text{com} \quad k \in \mathbb{Z}. \tag{3.2}$$

Sendo $d = mdc(c, m)$, $m = dk_1$ e $c = dk_2$. Com $mdc(k_1, k_2) = 1$. Substituindo m e c em (3.2),

$$dk_2(a - b) = kdk_1 \;\Rightarrow\; k_2(a - b) = kk_1 \;\Rightarrow\; k_1 | k_2(a - b),$$

ou seja, $k_1|(a - b)$. Desse modo, $a \equiv b \pmod{k_1}$, ou melhor, $a \equiv b \pmod{m/d}$.

Reciprocamente, consideremos $c = dk_3$ e $m = dk_4$. Como $a \equiv b \pmod{m/d}$, isto é, $a \equiv b \pmod{k_4}$, segue que $a - b = k_4k_5$, com $k_5 \in \mathbb{Z}$. Portanto

$$c(a - b) = k_4k \cdot dk_3 = mkk_3,$$

o que mostra que $ac \equiv bc \pmod{m}$. □

Como consequência direta, temos a lei do cancelamento, bastante útil no estudo de congruências.

Corolário 3.1.10 ***(Lei do Cancelamento)*** *Suponhamos $ac \equiv bc \pmod{m}$, com $mdc(c, m) = 1$. Então, $a \equiv b \pmod{m}$.*

3.2 Congruências Lineares

Consideramos nesta seção congruências lineares, que muito se assemelham com as equações lineares da Álgebra Linear.

Definição 3.2.1 *Dados a e b inteiros, com $a \neq 0$, uma congruência da forma*

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

é chamada ***congruência linear****, em que x é uma incognita.*

O objetivo então é determinar todas as soluções inteiras de $ax \equiv b \pmod{m}$, ou seja, todos os inteiros x_0 para os quais

$$ax_0 \equiv b \pmod{m}.$$

Por exemplo, $x_0 = 4$ é uma solução da congruência linear $6x = 3 \pmod{7}$, pois $6 \cdot 4 = 24 \equiv 3 \pmod{7}$. Já a congruêncaia $6x \equiv 1 \pmod{4}$, não tem solução inteira. De fato,

se $x_0 \in \mathbb{Z}$ é solução desta congruência, então $4|(6x_0 - 1)$, o que não é possivel, pois $6x_0 - 1$ é ímpar.

Um caso particular da situação anterior é a congruência dada por

$$ax \equiv 1 \pmod{m}.$$

Se x_0 é solução desta congruência, dizemos então que a é **invertível** módulo m, ou que a **admite inverso** módulo m.

Vejamos como identificar se um número inteiro a é invertível módulo m.

Proposição 3.2.2 *Um inteiro a é invertível módulo m se, e somente se, $mdc(a, m) = 1$. Qualquer outro inverso de a é congruente a ele módulo m.*

Demonstração: Se a é invertível módulo m, existe um inteiro b tal que $ab \equiv 1 \pmod{m}$. Logo, existe $c \in \mathbb{Z}$, com $ab = 1 + cm$, ou seja, $ab + (-c)m = 1$, que pelo Corolário 2.3.6, implica em $mdc(a, m) = 1$. Reciprocamente, se $mdc(a, m) = 1$, então pelo Teorema 2.3.2, existem inteiros x, y tais que $ax + my = 1$, isto é, $ax \equiv 1 (\mathrm{mod}\, m)$, o que mostra que a é invertível módulo m.

Para concluir, suponhamos que a tenha dois inversos módulo m, x_1 e x_2. Assim, $ax_1 \equiv 1 \pmod{m}$ e $ay_1 \equiv 1 \pmod{m}$. Por transitividade, $ax_1 \equiv ay_1 \pmod{m}$. Como $mdc(a, m) = 1$, então do Corolário 3.1.10, $x_1 \equiv y_1 \pmod{m}$. □

Exemplo 3.2.3 Vamos determinar os inversos de 5 e 7 módulo 8. Como $mdc(5, 8) = mdc(7, 8) = 1$, então 5 e 7 admitem inversos módulo 8, e como $5 \cdot 5 \equiv 25 \equiv 2 \pmod{8}$, $7 \cdot 7 \equiv 49 \equiv 1 \pmod{8}$, então o inverso de 5 é o próprio 5, e o de 7 é o proprio 7.

Vale ressaltar que se x_0 é solução de $ax \equiv b \pmod{m}$ e $x_0 \equiv y_0 \pmod{m}$, então y_0 também é solução. Portanto,

$$x = x_0 + km$$

é solução para cada inteiro k. Isso significa que uma congruência linear ou não tem solução ou tem inifinitas soluções.

Teorema 3.2.4 *A congruência linear $ax \equiv b \pmod{m}$ tem solução inteira se, e somente se, $d|b$, em que $d = mdc(a, m)$.*

Demonstração: Suponhamos que x_0 seja solução de $ax \equiv b \pmod{m}$ e tomemos $d = mdc(a, m)$. Dessa forma, $ax_0 - b = km$, ou seja, $b = ax_0 - km$. Como $d|a$ e $d|m$, segue que $d|b$.

Para a recíproca, suponhamos que $d|b$. Pelo Teorema 2.3.2, existem inteiros t e u, tais que

$$d = at + um. \tag{3.3}$$

Como $d|b$, então $b = dv$, com $v \in \mathbb{Z}$. Logo, de (3.3),

$$b = (at + um)v = avt + muv,$$

ou seja, $a(vt) \equiv b \pmod{m}$. Isso implica dizer que $x_0 = vt$ é uma solução de $ax \equiv b \pmod{m}$. □

Corolário 3.2.5 *A congruência* $ax \equiv 1 \pmod{m}$ *tem solução se, se somente se,* $mdc(a, m) = 1$.

O próximo Teorema caracteriza as soluções de uma congruência linear.

Teorema 3.2.6 *Se* x_0 *é uma solução da congruência linear* $ax \equiv b \pmod{m}$, *então todas as outras soluções são da forma*

$$x = x_0 + \frac{m}{d}k, \quad com \quad k \in \mathbb{Z}.$$

Demonstração: Inicialmente, vamos mostrar que $x_0 + (m/d)k$ é uma solução. Temos

$$ax = a\left(x_0 + \frac{m}{d}k\right) = ax_0 + a\frac{m}{d}k = b + m\left(\frac{ak}{d}\right),$$

ou seja, $ax \equiv b \pmod{m}$, pois $ak/d \in \mathbb{Z}$. Agora, seja $x_1 \in \mathbb{Z}$, com $ax_1 \equiv b \pmod{m}$. Como $ax_0 \equiv b \pmod{m}$, então por transsitividade, $ax_0 \equiv ax_1 \pmod{m}$, e, consequentemente, pelo Teorema 3.1.9, $x_0 \equiv x_1 \pmod{m/d}$, isto é,

$$x_1 = x_0 + \frac{m}{d}k, \quad \text{com } k \in \mathbb{Z}.$$ □

Existem soluções que são incongruente duas a duas módulo m, e estas são em quantidade finita, como mostramos a seguir.

Corolário 3.2.7 *Considere a congruência* $ax \equiv b \pmod{m}$. *Se* $d|b$, *onde* $d = mdc(a, m)$, *então a congruência possui* d *soluções incongruentes, duas a duas módulo* m, *dadas por*

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

em que x_0 *é uma solução particular qualquer de* $ax \equiv b \pmod{m}$.

Particularmente, como consequência do Corolário 3.2.7, a congruência linear

$$ax \equiv 1 \pmod{m},$$

tem apenas uma solução incongruente módulo m.

Exemplo 3.2.8 Determinar a(s) soluções de $2x \equiv 6 \pmod{8}$.

Solução: Inicialmente, $mdc(2, 8) = 2$ e $2|6$. Temos que $x_0 = 3$ é uma solução desta congruência. Portanto, sua solução geral é

$$x = 3 + 4t, \quad k \in \mathbb{Z}.$$

As soluções incongruentes são 3 e 7. △

De um modo geral, a demonstração do Teorema 3.2.4 nos fornece um modo de se determinar uma solução particular x_0 de $ax \equiv b \pmod{m}$.

3.3 A função φ de Euler

Nesta seção, apresentamos umas das mais importantes funções Aritméticas (uma função $f : \mathbb{N} \to \mathbb{R}$ é chamada **função Aritmética**). A função φ de Euler definida a seguir é parte central do teorema que generaliza o Teorema de Fermat, o qual estabelece uma congruência base importante com módulo primo. Especificando, o Teorema de Fermat afirma que, dados dois inteiros a e p, com p primo e $p \nmid a$, então

$$a^{p-1} \equiv 1 \pmod{p}.$$

O Teorema de Euler amplia este resultado com módulo m, sendo m um inteiro composto.

Definição 3.3.1 *Para cada inteiro $n \geq 1$, indicamos por $\varphi(n)$ o número de inteiros positivos menores ou iguais a n que são primos com n. A função $\varphi(n)$ assim definida é chamada de* ***função φ de Euler****.*

Por exemplo, o conjunto $\{1, 2, 4, 5, 7, 8\}$ contém todos os inteiros positivos menores do que e primos com 9, ou seja, $\varphi(9) = 6$.

Existe uma dificuldade de calcular $\varphi(n)$ para inteiros relativamente grandes. No entanto, de acordo com o Teorema 3.3.4, o cálculo de $\varphi(n)$ é facilmente feito desde que se conheça a fatoração canônica de $n \in \mathbb{N}$. Antes disso, apresentamos o seguinte:

Teorema 3.3.2 *Se p é primo e $k \geq 1$, temos,*

$$\varphi(p^k) = p^k \left(1 - \frac{1}{p}\right).$$

Demonstração: É evidente que $mdc(n, p) = 1$ se, e somente se, $p \nmid n$. Por outro lado, entre 1 e p^k, existem p^{k-1} múltiplos de p, que são

$$p, 2p, 3p, 4p, \ldots, \left(p^{k-1}\right) p,$$

pois $p\alpha \leq p^k$ se, e somente se, $\alpha = 1, 2, 3, \ldots, p^{k-1}$. Com isso, o conjunto $\{1, 2, \ldots, p^k\}$ contém exatamente $p^k - p^{k-1}$ números que são primos com p. Logo, por definição, $\varphi(n) = p^k\,(1 - 1/p)$. □

Por exemplo,

$$\varphi(27) = \varphi\left(3^3\right) = 3^3 - 3^2 = 27 - 9 = 16.$$

Particularmente, $\varphi(p) = p - 1$ se, e somente se, p é primo.

O resultado a seguir nos mostra uma propriedade significativa da função φ.

Teorema 3.3.3 ***(A função φ é multiplicativa)*** *Se m e n são números naturais, onde $mdc(m, n) = 1$, segue que*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

A demostração do Teorema 3.3.3 é muito técnica e longa e, por isso, não será aqui apresentada. Para o leitor interessado na sua prova sugerimos a referência [8].

Vale destacar que a propriedade multiplicativa de φ pode ser estendida da seguinte forma: se $m_1, m_2, \ldots, m_k$ são inteiros positivos primos aos pares, ou seja, $mdc(m_i, m_j) = 1$, com $i \neq j$, então

$$\varphi(m_1 m_2 \ldots m_k) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_k). \tag{3.4}$$

Provemos agora o resultado que generaliza o Teorema 3.3.2.

Teorema 3.3.4 *Se $n > 1$ e $n = p_1^{k_1} p_1^{k_2} \ldots p_k^{k_r}$ é a fatoração canônica de n, então*

$$\begin{aligned}\varphi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\ldots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= n\left(1 - 1/p_1\right)\left(1 - 1/p_2\right)\ldots\left(1 - 1/p_r\right).\end{aligned}$$

Demonstração: Desde que φ é multiplicativa e $mdc\left(p_i^{k_i}, p_j^{k_j}\right) = 1$, com $i \neq j$, segue de (3.4) que

$$\varphi(n) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)\ldots\varphi\left(p_r^{k_r}\right).$$

Agora, pelo Teorema 3.3.2,

$$\varphi\left(p_i^{k_i}\right) = p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i}\left(1 - \frac{1}{p_i}\right),$$

para cada $i = 1, 2, \ldots r$. Logo,

$$\begin{aligned}\varphi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\ldots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= p_1^{k_1} p_2^{k_2}\ldots p_2^{k_2}\left(1 - 1/p_1\right)\left(1 - 1/p_2\right)\ldots\left(1 - 1/p_r\right) \qquad (3.5)\\ &= n\left(1 - 1/p_1\right)\left(1 - 1/p_2\right)\ldots\left(1 - 1/p_r\right).\end{aligned}$$

□

Notemos que,

$$p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i-1}\left(p_i - 1\right).$$

A expressão apresentada em (3.5) pode ser reescrita como

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1}\ldots p_r^{k_r-1}\left(p_1 - 1\right)\left(p_2 - 1\right)\ldots\left(p_r - 1\right).$$

Exemplo 3.3.5 Calcular $\varphi(280)$.

Solução: Como $280 = 2^3 \cdot 5 \cdot 7$, segue que

$$\begin{aligned}\varphi(280) = \varphi(2^3 \cdot 5 \cdot 7) &= \varphi\left(2^3\right)\varphi(5)\varphi(7)\\ &= 2^2(5-1)(7-1)\\ &= 4 \cdot 4 \cdot 6\\ &= 96.\end{aligned}$$

Lema 3.3.6 *Seja a um inteiro tal que $mdc(a,m) = 1$. Se $a_1, a_2, \ldots, a_{\varphi(m)}$ são os inteiros positivos menores do que m e relativamente primos com m, então*

$$aa_1, aa_2, \ldots, aa_{\varphi(m)}$$

são congruentes módulo m a $a_1, a_2, \ldots, a_{\varphi(m)}$, em alguma ordem.

Demonstração: Mostremos primeiramente que $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ são dois a dois incongruentes módulo m. De fato, se $aa_i \equiv aa_j \pmod m$ para $i \neq j$, então como $mdc(a,m) = 1$, podemos cancelar o fator a desta congruência e, assim, $a_i \equiv a_j \pmod m$, ou seja, $m \mid a_i - a_j$, o que é uma impossibilidade, pois $1 \leq a_i, a_j \leq m-1$ e $a_i \neq a_j$. Além disso, como $mdc(a,m) = 1$ e $mdc(a_i,m) = 1$ para todo $i = 1, \ldots, \varphi(m)$, então $mdc(aa_i,m) = 1$. Desde que $\{0, 1, \ldots, m-1\}$ é um sistema completo de resíduos módulo m, então para cada aa_i, existe único inteiro b, com $0 \leq b < m$, tal que $aa_i \equiv b \pmod m$. Como

$$mdc(b,m) = mdc(aa_i,m) = 1,$$

então b deve necessariamente ser um dos inteiros $a_1, a_2, \ldots, a_{\phi(m)}$. Logo, $aa_i \equiv a_j \pmod m$ para algum $j = 1, \ldots, \varphi(m)$. □

Por exemplo, ,para $m = 12$, temos que $\varphi(12) = 4$, ou seja, existem 4 números inteiros que são primos com 12 e menores do que 12, que são

$$a_1 = 1, \quad a_2 = 5, \quad a_3 = 7, \quad a_4 = 11.$$

Considerando $a = 11$, temos

$$11 \cdot 1 \equiv 11 \pmod{12},$$
$$11 \cdot 5 \equiv 7 \pmod{12},$$
$$11 \cdot 7 \equiv 5 \pmod{12},$$
$$11 \cdot 11 \equiv 1 \pmod{12}.$$

Ou seja, são congruentes aos inteiros que são primos com 12.

O teorema a seguir é de fundamental importância para o estudo da Criptografia RSA.

Teorema 3.3.7 ***(Euler)*** *Sejam a e m inteiros, com $m \geq 1$ e $mdc(a,m) = 1$, então*

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Demonstração: O caso $m = 1$ é imediato, pois $\varphi(1) = 1$. Por isso, vamos considerar $m > 1$. Sejam $a_1, a_2, \ldots, a_{\varphi(m)}$ os inteiros positivos menores do que m que são relativamente primos com m. Desde que $mdc(a_i,m) = 1$ para cada $i = 1, \ldots, \varphi(m)$, segue que

$aa_1, aa_2, \ldots, aa_{\varphi(m)}$ são congruentes módulo m a $a_1, a_2, \ldots, a_{\varphi(m)}$, em alguma ordem. Desse modo,

$$\begin{aligned} a \cdot a_1 &\equiv b_1 \pmod{m}, \\ a \cdot a_2 &\equiv b_2 \pmod{m}, \\ \vdots &\equiv \vdots \\ a \cdot a_{\varphi(m)} &\equiv b_{\varphi(m)} \pmod{m}, \end{aligned}$$

em que $b_1, b_2, \ldots, b_{\varphi(m)}$ são os inteiros $a_1, a_2, \ldots, a_{\varphi(m)}$, não necessariamente nesta ordem. Multilicando estas congruências, segue que

$$(aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \equiv b_1 b_2 \cdots b_{\varphi(m)} \pmod{m},$$

de modo que

$$a^{\varphi(m)}(a_1 a_2 \cdots a_{\varphi(m)}) \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}.$$

Como $mdc(a_i, m) = 1$ para todo $i = 1, \ldots, \varphi(m)$, então $mdc(a_1 a_2 \ldots a_{\varphi(m)}, m) = 1$. Por isso, podemos cancelar o fator $a_1 a_2 \ldots a_{\varphi(m)}$ da última congruência e, assim,

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \qquad \square$$

Notemos que quando m for um número primo, $m = p$, como $\varphi(p) = p - 1$, segue que

$$a^{p-1} \equiv 1 \mod p,$$

ou seja, o Teorema de Fermat é um caso particular do Teorema de Euler.

Exemplo 3.3.8 Determiner o resto da divisão de

(a) 7^{299} *por* 30.

(b) 4^{100} *por* 19.

Solução: Para (a), temos que $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = \varphi(2)\varphi(3)\varphi(5) = 2 \cdot 4 = 8$, e como $mdc(7, 30) = 1$, segue do Teorema de Euler que

$$7^8 \equiv 1 \pmod{30}.$$

Elevando ambos os membros desta congruência por 37, temos

$$\left(7^8\right)^{37} = 7^{296} \equiv 1 \pmod{30}. \tag{3.6}$$

Por outro lado,

$$7^3 \equiv 13 \pmod{30}, \tag{3.7}$$

Multiplicando as congruências (3.6) e (3.7),

$$7^{299} \equiv 13 \pmod{30},$$

ous seja, o resto da divisão de 7^{299} por 30 é 13.

Para (b), $\varphi(19) = 19 - 1 = 18$, pois 19 é primo. Assim,

$$4^{18} \equiv 1 \pmod{19}.$$

Elevendo ambos os membros da congruência por 5,

$$\left(4^{18}\right)^5 = 4^{90} \equiv 1 \pmod{19}. \tag{3.8}$$

Por outro lado,

$$4^{10} \equiv 4 \pmod{19}. \tag{3.9}$$

Multiplicando as congruências (3.8) e (3.9),

$$4^{100} \equiv 4 \pmod{19},$$

ou seja, o resto da divisão de 4^{100} por 19 é 4. △

Capítulo 4

Criptografia e Teoria dos Códigos

Não é de hoje a necessidade do envio e recebimento de mensagens sigilosas, de modo que apenas a pessoa que enviou e a que seja o destinatário legítimo possam entender o conteúdo, dificultando a leitura da informação, caso seja inteceptada.

A palavra Criptografia deriva-se do grego; kryptos, significa secreto, oculto; graphein significa escrita, ou seja, escrita secreta, muito utilizada ao longo da história, sejam para assuntos ligados às guerras, ao amor, diplomacias, entre outros, onde havia a necessidade das informações não caírem em mãos erradas. Trata-se de um conjunto de regras a fim de codificar uma informação de modo que apenas o emissor e o receptor consigam decodificar, lendo a informação com facilidade. Para isso, são usadas varias técnicas, que ao longo do tempo, são modificadas, aperfeiçoadas e surgem outras maneiras, aumentando ainda mais a segurança das informações. Vale ressaltar que um dos métodos mais famosos de sistemas criptográficos da antiguidade foi um sistema utilizado por Júlio César, conhecido como cifra de César, em que consistia em substituir cada letra do alfabeto por outra letra, seguindo um determinado padrão.

A Teoria Moderna da Criptografia está baseada nas ciências exatas, e os estudos científicos sobre a Criptografia estão ficando cada vez mais avançados, pelo fato da sua importância na atualidade, sendo um dos tópicos do conhecimento mais antigos.

As formas de enviar mensagens foram mudando durante séculos, formas como tatuagens nos corpos de escravos, pinturas, figuras, criação de sinais, entre outros. Entretanto, o desenvolvimento das tecnologias causou grandes mudanças nas formas de transmitir informações. Vale salientar que a Segunda Guerra Mundial foi muito importante para o avanço da Criptografia, onde se fez necessário decodificar as mensagens dos inimigos. Atualmente, decifrar mensagens interceptadas é de grande utilidade no combate ao terrorismo e ao tráfico de drogas, por exemplo. Isso mostra a importância da Criptografia na vida cotidiana.

Nas referências [3], [5] e [7], o leitor poderá fazer uma leitura abrangente sobre os conceitos apresentados na seção seguinte.

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

Tabela 4.1: Tabela da Cifra de César.

4.1 Elementos da Criptografia

Existe uma maneira bastante simples para codificar uma mensagem do remetente para um destinatário, usando letras do alfabeto de várias línguas, como inglês, português, italiano e espanhol. Para isso, podemos permutar as letras e gerar uma cifra, ou, obedecendo a uma ordem, trocar as letras de posição. Temos então um caso simples de gerar cifra, conhecido a muitos séculos, atribuído a Júlio César.

Primeiramente, vamos definir alguns elementos da Criptografia que serão utilizandos ao longo do texto. **Codificar** é tonar a mensagem secreta; **decodificar** é tornar a mensagem pronta para leitura, utilizando a chave de decodificação; **decifrar** é a quebra do código, ou seja, quando não estamos de posse da chave para decodificação.

Em alguns métodos de Criptografia, devemos realizar a **pré-codificação**, que consiste em substituir a letra do alfabeto por um número já pré-determinado.

4.2 Cifra de César

A cifra de César é uma das técnicas mais simples de Criptografia, conhecida por cifra de substituição, onde cada letra do texto é substituída por outra, deslocando um número fixo de vezes o alfabeto. Nesse caso, o deslocamento são três casas crescentes.

Observe que na primeira linha da Tabela 4.1, estão dispostas as letras do alfabeto da língua portuguesa, e na segunda linha estão as letras com troca de três posições. Em geral, nenhuma letra está acentuada; isso é realizado quando se faz necessário no processo de codificação/decodificação.

Por outro lado, vamos chamar as letras da primeira e terceira linhas de **alfabeto-texto**, ou simplesmente **texto**, já na segunda e quarta linhas, de **alfabeto-cifra**, ou **cifra**. Desse modo, uma pessoa escreve as mensagens utilizando as cifras e envia para o destinatário. Ao receber a mensagem, o destinatário utiliza a Tabela 4.1 para transformar a cifra em texto. Esse processo recebe o nome de **decodificação**.

Vamos considerar a seguinte mensagem codificada utilizando a Tabela 4.1:

WHRULDGRVQXPHURV

A pessoa que receber esta mensagem não terá dificuldades de entender se, a priori, conhecer a chave para decodificar, que nesse caso, será a Tabela 4.1. Logo, a mensagem

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

Tabela 4.2: Pré-codificação.

de forma clara é:

teoria dos números.

O fato é que temos muitas limitações recorrendo apenas às letras. Por isso, podemos associar as letras com números de dois algarismos. Como o alfabeto tem 26 letras, os números irão variar de 0 a 25, como pode ser visto na Tabela 4.2. Assim, utilizamos uma congruência com módulo 26.

Visto que na Cifra de César a cifra é deslocada três casas crescentes em relação ao texto, podemos utilizar a congruência

$$C \equiv (T + 3) \pmod{26}, \tag{4.1}$$

onde C é o termo numérico que representa a cifra e T é o termo numérico que representa o texto, utilizando a Tabela 4.2. Esta congruência representa as cifras na Criptografia de Júlio César. Por outro lado, para determinar o texto, precisamos decodificar a mensagem, que é equivalente a

$$T \equiv (C - 3) \pmod{26}. \tag{4.2}$$

Desse modo, precisamos primeiro fazer a pré-codificação, que consiste em transformar a mensagem original em números, de acordo com a Tabela 4.2; em seguida, utilizar (4.1) para codificar a mensagem. É comum o agrupamento em conjuntos de quatro algarismos.

Exemplo 4.2.1 Utilizando a cifra de César e a Tabela 4.2, codificar a palavra: MATEMATICA.

Solução: Primeiro, vamos transformar essa palavra em números. Usando a Tabela 4.2, temos:

1200 1904 1200 1908 0200.

A	14,63%	H	1,28%	O	10,73%	V	1,67%
B	1,4%	I	6,18%	P	2,52%	W	0,01%
C	3,88%	J	0,4%	Q	1,2%	X	0,21%
D	4,99%	K	0,02%	R	6,53%	Y	0,01%
E	12,57%	L	2,78%	S	7,81%	Z	0,47%
F	1,02%	M	4,74%	T	4,34%		
G	1,3%	N	5,5%	U	4,63%		

Tabela 4.3: Ocorrência das letras do alfabeto na Língua Portuguesa

Agora, por (4.1), temos:

$$C \equiv 12 + 3 \equiv 15 \pmod{26},$$
$$C \equiv 00 + 3 \equiv 03 \pmod{26},$$
$$C \equiv 19 + 3 \equiv 22 \pmod{26},$$
$$C \equiv 04 + 3 \equiv 07 \pmod{26},$$
$$C \equiv 08 + 3 \equiv 11 \pmod{26},$$
$$C \equiv 02 + 3 \equiv 05 \pmod{26}.$$

Consequentemente,

$$1503\ 2207\ 1503\ 2211\ 0503,$$

é a mensagem codificada numericamente, que corresponde a

$$\text{PDXHPDXLFD.} \qquad \triangle$$

No exemplo anterior, pudemos perceber que precisamos conhecer apenas a Tabela 4.2 para realizar todo o processo. Vale ressaltar que para casos onde conhecemos a cifra, utilizamos o mesmo processo de pré-codificação e utilizamos (4.2) para encontrar os algarismos correspondentes ao texto e consequentemente, o texto claro. Às vezes, decifrar uma frase longa que utiliza esse modelo de Criptografia pode não ser uma tarefa muito difícil, pelo fato de que, na língua portuguesa, algumas letras aparecem com mais frequência que as demais, tornando algumas cifras repetitivas, abrindo espaço para que um interceptador consiga êxito no entendimento da mensagem. Na Tabela 4.3, apresentamos a frequência com que as letras aparecem nas palavras da lingua portuguesa.

Diante da fragilidade desse método, vamos abordar um método um pouco mais complexo, que utiliza as cifras afins.

4.3 Cifras Afins

Como vimos na sessão anterior, a cifra de César é determinada pela congruência $C \equiv (T + 3) \pmod{26}$. Utilizando a mesma idéia de deslocamento do alfabeto, podemos determinar um método criptográfico alterando apenas o deslocamento da cifra em relação ao texto, ou seja, alterando a chave. A congruência a seguir, representa a cifra de César generalizada.

$$C \equiv (T + k) \pmod{26} \tag{4.3}$$

em que $0 \leq k \leq 25$. Vale salientar que quando $k = 3$, temos a cifra de César, $k = 0$, segue que a cifra corresponde exatamente ao texto da mensagem.

O valor de k, chamado **chave de codificação**, representa a escolha da quantidade de casas que o alfabeto irá se deslocar é uma questão particular.

Exemplo 4.3.1 Considerando a cifra de César generalizada, com chave $k = 10$, decodifique a mensagem: NSKNOZBYFK.

Solução: Fazendo a pré-codificação, temos

$$1318\ 1013\ 1425\ 0124\ 0510.$$

Utilizando (4.3) e substituindo a chave, obtemos $C \equiv (T + 10) \pmod{26}$, que é equivalente à congruência $T \equiv (C - 10) \pmod{26}$. Dessa forma, decodificando o texto temos:

$$T \equiv 13 - 10 \equiv 03 \pmod{26},$$
$$T \equiv 18 - 10 \equiv 08 \pmod{26},$$
$$T \equiv 10 - 10 \equiv 00 \pmod{26},$$
$$T \equiv 14 - 10 \equiv 04 \pmod{26},$$
$$T \equiv 25 - 10 \equiv 15 \pmod{26},$$
$$T \equiv 01 - 10 \equiv 17 \pmod{26},$$
$$T \equiv 24 - 10 \equiv 14 \pmod{26},$$
$$T \equiv 05 - 10 \equiv 21 \pmod{26}.$$

Logo, a mensagem decodificada, representada por números, é

$$0308\ 0003\ 0415\ 1714\ 2100,$$

que utilizando a Tabela 4.2, representa a mensagem:

$$\text{DI AD EP RO VA},$$

ou seja, dia de prova. △

Agora, vamos definir uma cifra um pouco mais robusta. Primeiro, consideremos dois inteiros a e b tais que

$$0 \leq a, b \leq 25, \quad mdc(a, 26) = 1$$

Definição 4.3.2 *Chamamos de cifra afim a congruência*

$$C \equiv (aT + b) \pmod{26}, \tag{4.4}$$

onde os números a e b são chamados de ***chaves da cifra****.*

Para decodificar a cifra afim, devemos determinar o valor de T. De (4.4), temos:

$$aT \equiv (C - b) \pmod{26}.$$

Como por hipótese, $mdc(a, 26) = 1$, então existe um inteiro a^{-1} tal que $aa^{-1} \equiv 1 \pmod{26}$. Assim, da última congruência, obtemos

$$a^{-1}aT \equiv a^{-1}(C - b) \pmod{26},$$

ou melhor,

$$T \equiv a^{-1}(C - b) \pmod{26}. \tag{4.5}$$

Temos que (4.5) determina o texto claro da mensagem.

Salientamos que, quando $a = 1$, temos simplesmente a cifra de César generalizada, que foi apresentada em (4.3). Por isso, existem 26 cifras de César generalizadas e 312 cifras afins, pois nas cifras afins, temos 12 possibilidades de escolha para a, $\varphi(26) = 12$, e 26 possibilidades para b, ou seja, $12 \cdot 26 = 312$.

Exemplo 4.3.3 Utilizando a cifra afim, codifique a palavra Criptografia com as chaves $a = 3$ e $b = 4$.

Solução: Primeiramente, vamos realizar a pré-codificação. De acordo com a Tabela 4.2, temos

$$0217\ 0815\ 1914\ 0617\ 0005\ 0800.$$

Usando (4.4), e substituindo as chaves, obtemos,

$$C \equiv (3T + 4) \pmod{26}.$$

Assim, codificando, segue que

$$C \equiv 3 \cdot 02 + 4 \equiv 10 \pmod{26},$$
$$C \equiv 3 \cdot 17 + 4 \equiv 03 \pmod{26},$$
$$C \equiv 3 \cdot 08 + 4 \equiv 02 \pmod{26},$$
$$C \equiv 3 \cdot 15 + 4 \equiv 23 \pmod{26},$$
$$C \equiv 3 \cdot 19 + 4 \equiv 09 \pmod{26},$$
$$C \equiv 3 \cdot 14 + 4 \equiv 20 \pmod{26},$$
$$C \equiv 3 \cdot 06 + 4 \equiv 22 \pmod{26},$$
$$C \equiv 3 \cdot 00 + 4 \equiv 04 \pmod{26},$$
$$C \equiv 3 \cdot 05 + 4 \equiv 19 \pmod{26}.$$

A palavra codificada é representada numericamente como

$$1003\ 0223\ 0920\ 2203\ 0419\ 0204,$$

que utilizando a tabela 4.2, representa o código

KDCXJUWDETCE. △

4.4 Sistema RSA

Nessa seção, vamos abordar o mais conhecido e seguro dos métodos de Criptografia de chave pública, a Criptografia RSA, a qual representa as iniciais dos inventores do código, R.L. Rivest, A. Shamir e L. Adleman. Existem vários códigos de chaves públicas, entretanto, o RSA é o mais utilizado atualmente. Ele é usado em comunicações eletrônicas, como o uso de cartão de credito, compras pela internet, entre outros tipos de comunicações onde se faz necessário a utilização de assinaturas eletrônicas. A matemática necessária para definir o sistema RSA tem como base conceitos elementares da Teoria dos Números, conceitos esses abordados nos Capítulos 2 e 3, onde, em ocasião oportuna, estaremos apenas citando.

Veremos então os passos para a utilização de método RSA, mostrando por que ele é bastante eficiente. Para tal, precisamos de dois parâmetros, que são dois números primos, os quais, indicaremos por p e q. Para codificar uma mensagem, devemos conhecer o produto dos dois primos, que vamos chamar de n. Por outro lado, para decodificar uma mensagem, deve-se conhecer os primos p e q. Cada usuário tem sua própria chave de codificação (n), que é a chave pública; todos podem saber, entretanto, os primos p e q devem ficar em segredo, que é a **chave de decodificação**, pois uma vez expostos, comprometerá a segurança do método. O código é basicamente isso, porém, pode-se perguntar: Se o valor de n é conhecido, então pode-se simplesmente fatorá-lo,

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

Tabela 4.4: Conversão Numérica RSA.

descobrir p e q, e então decifrar a mensagem. Mas não é bem assim, pois usando chaves de codificação com números extremamente grandes, demoraria muito tempo para concluir, pois no RSA, além de os primos p e q serem grandes, com no mínimo 100 dígitos cada um, eles são escolhidos convenientemente, ou seja, são números com uma distância considerável um do outro. Portanto, levaria muito tempo para fatorar n (caso isso ocorra), mesmo usando um computador avançado. Esse é o ponto forte do método RSA, devido à complexidade de se obter a fatoração canônica de inteiros arbitrários.

Primeiramente, para utilizar esse método, devemos converter a mensagem em números, ou seja, a pré-codificação, utilizando para isso a Tabela 4.4. Feita a pré-codificação, usa-se 99 entre cada espaço das palavras.

Em seguida, teremos que escolher os parâmetros do sistema que iremos utilizar, os primos distintos, p e q, com $n = pq$. O próximo passo é quebrar a pré-codificação em blocos, de modo que eles sejam menores do que n.

Por exemplo, para os primos $p = 13$ e $q = 17$, os blocos formados devem ser menores do que $221 = n = pq$. Por outro lado, deve-se ter cuidado para que os blocos não se iniciem em 0, pois do contrário, pode-se ter problema no processo de decodificação. Ressaltamos também que a forma de quebra dos blocos não é única, fica a critério do usuário do método.

Feita a pré-codificação, inicia-se a codificação propriamente dita, precisando para isso, do valor de n e de um inteiro positivo e, com $mdc(e, \varphi(n)) = 1$. De posse dos primos p e q, calculamos $\varphi(n)$, com $n = pq$, através da igualdade

$$\varphi(n) = (p-1)(q-1).$$

O par (n, e) é chamado de **chave de codificação** do sistema RSA.

A codificação é feita com cada bloco, formando um sequência de blocos codificados, não podendo reuní-los para formar um novo número, pois, dessa forma, seria impossível realizar a decodificação.

Seja b um bloco da pré-codificação. Para codificar esse bloco, temos que usar a chave de codificação (n, e). A codificação do bloco b, representado por $C(b)$, é o resto da divisão de b^e por n, ou seja,

$$C(b) \equiv b^e \pmod{n}. \tag{4.6}$$

Por outro lado, para realizar a decodificação, precisamos conhecer um número, que chamaremos de d, que é o inverso de e módulo $\varphi(n)$. Assim, temos a **chave de decodificação,** o par (d, n). Considerando a como sendo um bloco de números codificado, $D(a)$ é o resultado da decodificação, que é obtido por

$$D(a) \equiv a^d \pmod{n}. \tag{4.7}$$

Descobrir a chave de decodificação é de fato complicado, pois isso consiste em obter a fatoração canônica de n, bem como o valor de d, inverso de e módulo $\varphi(n)$. A segurança desse método é a dificuldade de encontrar d conhecendo apenas n e e. Pode-se calcular d usando o algoritmo de euclides com $\varphi(n)$ e e, enquanto $\varphi(n)$ só pode ser calculado fatorando os primos p e q. Portanto, a segurança do método depende da magnitude de n e da escolha dos primos p e q, pois se $|p-q|$ for pequeno, então pode-se facilmente fatorar n através processo conhecido como Fatoração de Fermat[1].

Para uma simples aplicação de como o método funciona, vamos fazer um exemplo para primos pequenos, visando apenas a fixação do que foi exposto, não pela dificuldade da fatoração de n.

Exemplo 4.4.1 Utilizando o método RSA, e tomando os primos 11 e 13, vamos codificar o a seguinte mensagem: "A VIDA É BELA."

Solução: Utilizando a Tabela 4.4, vamos realizar a pré-codificação, não esquecendo de colocar 99 nos espaços entre palavras, dessa forma, obtemos:

$$10993118131099149911142110.$$

Na sequência, serão quebrados em blocos de modo que sejam menores que $n = 11.13 = 143$. Uma quebra de blocos pode ser

$$109 - 93 - 118 - 13 - 10 - 99 - 14 - 9 - 91 - 114 - 2 - 110.$$

[1]Para detalhes, sugerimos a referência [3].

Feita a pré-codificação, iremos então, determinar o valor de e. Como $\varphi(11 \cdot 13) = 10 \cdot 12 = 120 = 2^3 \cdot 3 \cdot 5$, consideremos $e = 7$, pois $mdc(7, 120) = 1$, o que satisfaz a condição. Realizando a codificação de cada bloco, obtemos[2]:

$$\begin{aligned}
109^7 &\equiv 21 \pmod{143},\\
93^7 &\equiv 102 \pmod{143},\\
118^7 &\equiv 79 \pmod{143},\\
13^7 &\equiv 117 \pmod{143},\\
10^7 &\equiv 10 \pmod{143},\\
99^7 &\equiv 44 \pmod{143},\\
14^7 &\equiv 53 \pmod{143},\\
9^7 &\equiv 48 \pmod{143},\\
91^7 &\equiv 130 \pmod{143},\\
114^7 &\equiv 49 \pmod{143}.\\
2^7 &\equiv 128 \pmod{143}\\
110^7 &\equiv 33 \bmod 143.
\end{aligned}$$

Logo, a mensagem codificada é

$$21 - 102 - 79 - 117 - 10 - 44 - 53 - 48 - 130 - 49 - 128 - 33. \qquad \triangle$$

Podemos observar que não acontece repetição numérica, não havendo margem a suposições de letras que apresentam uma maior frequência em nosso alfabeto.

No próximo exemplo, iremos fazer o processo inverso, decodificar uma mensagem. Vamos utilizar a mesma frase anterior.

Exemplo 4.4.2 Decodificar a mensagem do Exemplo 4.4.1.

Solução: Para decodificar a mensagem, precisamos encontrar o número d, que é o inverso de $e = 7$ módulo $\varphi(n) = 120$. Pelo Algoritmo de Euclides,

$$\begin{aligned}
120 &= 17 \cdot 7 + 1,\\
1 &= 120 + (-17) \cdot 7,
\end{aligned}$$

assim, $(-17) \cdot 7 \equiv 1 \pmod{120}$, e como $(-17) \equiv 103 \pmod{120}$, então $103 \cdot 7 \equiv 1$

[2]Os resultados destas congruências envolvem longos cálculos. Devido a isso, eles não foram descritos no texto. Foram realizados fazendo uso das propriedades descritas no Capítulo 3.

(mod 120). Desse modo, $d = 103$. Agora, decodificando, temos

$$21^{103} \equiv 109 \pmod{143},$$
$$102^{103} \equiv 93 \pmod{143},$$
$$79^{103} \equiv 118 \pmod{143},$$
$$117^{103} \equiv 13 \pmod{143},$$
$$10^{103} \equiv 10 \pmod{143},$$
$$44^{103} \equiv 99 \pmod{143},$$
$$53^{103} \equiv 14 \pmod{143},$$
$$48^{103} \equiv 9 \pmod{143},$$
$$130^{103} \equiv 91 \pmod{143},$$
$$49^{103} \equiv 114 \pmod{143},$$
$$128^{103} \equiv 2 \pmod{143},$$
$$33^{103} \equiv 110 \pmod{143}.$$

Logo, a decodificação é

$$10993118131099149911142110,$$

que resulta na mensagem original do Exemplo 4.4.1, "A VIDA É BELA". △

4.5 Cifra de Hill

Nesta seção, fazemos uso de resultados elementares sobre álgebra matricial, os quais podem ser vistos nas referências [1] e [2].

A Cifra de Hill é um método criptográfico que consiste na codificação e decodificação de mensagens por meio de matrizes. A segurança do método está ligada ao sigilo da matriz de codificação.

Para o uso das matrizes, precisamos representar as letras do alfabeto por números inteiros, conforme tabela abaixo:

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

Para utilização da Cifra de Hill, usamos um procedimento que consiste em transformar cada par sucessivo de letras do texto em um par cifrado, através dos seguintes passos:

Passo 1: Escolher uma matriz 2x2 com números inteiros

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

para efetuar a codificação.

Passo 2: Agrupar as letras sucessivas do texto em pares; caso seja uma quantidade ímpar, adicionar uma letra fictícia para completar o último par. Posteriormente, substituir cada letra pelo número corresponde.

Passo 3: Colocar cada par de letras, p_1 e p_2, em um vetor coluna

$$\mathbf{P} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix},$$

determinando o produto $A\mathbf{P}$. Chamaremos $\mathbf{P}$ de vetor comum e $A\mathbf{P}$, o vetor **cifrado**.

Passo 4: Coverter cada vetor cifrado em seu equivalente alfabético.

A matriz de codificação deve apresentar inversa módulo 26 para que a Cifra seja útil, pois caso contrário, será impossível decodificar a mensagem.

De maneira formal, dizemos que uma matriz A com entradas em $\mathbb{Z}_{26}$ é invertível módulo m se existir uma matriz B com entradas em $\mathbb{Z}_{26}$ tal que

$$AB = I \pmod{26}.$$

Sejam A uma matriz invertível módulo 26, $\mathbf{P}$ o vetor comum, formado pelas letras consecultivas da mensagem. Então, o vetor cifrado é determinado por

$$\mathbf{C} = A\mathbf{P} \pmod{26}.$$

Consequentemente, o vetor comum é obtido por

$$\mathbf{P} = A^{-1}\mathbf{C} \pmod{26}.$$

Em resumo:

Teorema 4.5.1 *Uma matriz quadrada A com entradas em $\mathbb{Z}_{26}$ é invertível módulo* 26 *se, e somente se, o resíduo de* $\det(A)$ *não é divisível por* 2 *ou* 13.

Dada a matriz

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

com entradas em $\mathbb{Z}_{26}$, sua inversa é dada por

$$A^{-1} = (a_{11} \cdot a_{22} - a_{12} \cdot a_{21})^{-1} \cdot \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \pmod{26}, \tag{4.8}$$

em que $(a_{11} \cdot a_{22} - a_{12} \cdot a_{21})^{-1}$ é o inverso de $(a_{11} \cdot a_{22} - a_{12} \cdot a_{21}) \pmod{26}$.

Exemplo 4.5.2 Utilizando a Cifra de Hill, codificar a palavra: datilografia.

Solução: Primeiramente, consideremos

$$A = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$$

como nossa matriz de codificação, pois $\det(A) = 7$, ou seja, A tem inversa módulo 26. Agora, separemos as letras consecultivas em pares,

$$\text{d a} \quad \text{t i} \quad \text{l o} \quad \text{g r} \quad \text{a f} \quad \text{i a}.$$

Logo, a correpondência numérica é

$$4\ 1 \quad 20\ 9 \quad 12\ 15 \quad 7\ 18 \quad 1\ 6 \quad 9\ 1.$$

Multiplicando cada vetor coluna pela matriz de codificação, obtemos

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 14 \\ 21 \end{bmatrix},$$
$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 9 \end{bmatrix} = \begin{bmatrix} 0 \\ 21 \end{bmatrix},$$
$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 15 \end{bmatrix} = \begin{bmatrix} 14 \\ 19 \end{bmatrix},$$
$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 18 \end{bmatrix} = \begin{bmatrix} 5 \\ 14 \end{bmatrix},$$
$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 6 \end{bmatrix} = \begin{bmatrix} 15 \\ 8 \end{bmatrix},$$
$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 15 \end{bmatrix}.$$

Observemos que as entradas dos vetores cifrados estão em $\mathbb{Z}_{26}$. Assim, a palavra cifrada correspondente é nuzunsenco. △

Vejamos agora o processo inverso.

Exemplo 4.5.3 Decodificar a palavra do Exemplo 4.5.2.

Solução: Separando as letras ao pares, obtemos

$$\text{n u} \quad \text{z u} \quad \text{n s} \quad \text{e n} \quad \text{co}.$$

A correspondncia numérica é

$$14\ 21 \quad 0\ 21 \quad 14\ 19 \quad 5\ 14 \quad 15\ 8 \quad 3\ 15.$$

Vamos determinar a matriz inversa de A, que será a nossa matriz de decodificação. Pela expressão (4.8), a inversa de A é

$$A^{-1} = 7^{-1} \cdot \begin{pmatrix} 5 & -2 \\ -4 & 3 \end{pmatrix} \pmod{26}.$$

Notemos que $15 \cdot 7 \equiv 1 \pmod{26}$, isto é, 15 é o inverso de 7 módulo 26. Daí,

$$A^{-1} = \begin{pmatrix} 23 & 22 \\ 18 & 19 \end{pmatrix} \pmod{26}.$$

Mutiplicando a matriz inversa pelo vetor cifrado, temos

$$\begin{bmatrix} 23 & 22 \\ 18 & 19 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 21 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \end{bmatrix},$$

$$\begin{bmatrix} 23 & 22 \\ 18 & 19 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 21 \end{bmatrix} = \begin{bmatrix} 20 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 23 & 22 \\ 18 & 19 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 19 \end{bmatrix} = \begin{bmatrix} 12 \\ 15 \end{bmatrix},$$

$$\begin{bmatrix} 23 & 22 \\ 18 & 19 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 7 \\ 18 \end{bmatrix},$$

$$\begin{bmatrix} 23 & 22 \\ 18 & 19 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 8 \end{bmatrix} = \begin{bmatrix} 1 \\ 6 \end{bmatrix},$$

$$\begin{bmatrix} 23 & 22 \\ 18 & 19 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 9 \\ 1 \end{bmatrix}.$$

Substituindo as letras correspondentes, a palavra “datilografia”. △

4.6 Considerações Finais

Em virtude da grande aplicabilidade da Teoria dos números, que é frequentemente vista nos anos iniciais do ensino básico, mesmo que de maneira informal, apresentamos este trabalho com os principais resultados elementares para o estudo da Teoria Elementar dos Números, os quais foram aplicados em alguns métodos Criptográficos. As aplicações, mesmo em níveis elementares, podem oferecer uma visão diferenciada para os leitores. Acreditamos que os resultados aqui apresentados possam ser úteis a todo leitor que deseja estudar algumas aplicações de tópicos abstratos dessas teoria.

Acreditamos também que o trabalho possa servir de apoio para professores do ensino básico, especificamente, a todos aqueles que buscam enriquecer suas aulas com aplicações práticas da matemática em problemas do cotidiano, tomando por base os exemplos aqui apresentados, uma vez que eles podem ser base para que outros possam ser elaborados dentro do contexto de cada tópico. A referência [4] poderá ajudar neste sentido.

Bibliografia

[1] ATON, H.; RORRES, C. *Álgebra Linear com Aplicações*. Tradução técnica de Claus Ivo Doering. 10^a ed. Porto Alegre: Bookman, 2012.

[2] BOLDRINI, J. L. [et al]. – *Álgebra Linear* ($7^{\underline{a}}$ edição), Ed. Harbra Ltda., São Paulo, 1986.

[3] COUTINHO, S. C. *Números Inteiros Criptografia e RSA*. 2^a ed. Rio de Janeiro: IMPA, 2011.

[4] GAUDINO, U. A. *Teoria dos Números e Criptografia com Aplicações Básicas*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional). UEPB, Campina Grande, 2014.

[5] EVARISTO, J.; PERDIGÃO, E. *Introdução à Algebra Abstrata*. Maceió: Edufal, 2002.;

[6] MILIES, C.P.; COELHO, S. P. *Números: Uma Introdução à Matemática*. 3^a ed. São Paulo: Edusp, 2006.

[7] SHOKRANIAN, S. *Criptografia para Iniciantes*. 2^a ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2012.

[8] VIEIRA, V. L. *Um Curso Básico em Teoria dos Números*. Campina Grande/São Paulo: EDUEPB (Co-edição: LF Editorial), 2015.