Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Raízes Primitivas e Aplicações em Criptografia

Helen Alessandra Ribeiro

Orientadora: Prof[a]. Dr[a]. Grasiele Cristiane Jorge

São José dos Campos
Outubro, 2018

PROFMAT

Título: *Raízes Primitivas e Aplicações em Criptografia*

Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos
Outubro, 2018

Ribeiro, Helen Alessandra

Raízes Primitivas e Aplicações em Criptografia, Helen Alessandra Ribeiro – São José dos Campos, 2018.

viii, 94f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto de Ciência e Tecnologia. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Primitive Roots and Cryptographic Applications

1. Teoria dos Números. 2. Aritmética Modular. 3. Raízes Primitivas. 4. Criptografia. 5. Diffie-Hellman.

UNIVERSIDADE FEDERAL DE SÃO PAULO

INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe de Departamento:
Prof. Dr. Eduardo Antonelli

Coordenador do Programa de Pós-Graduação:
Prof. Dr. Angelo Calil Bianchi

HELEN ALESSANDRA RIBEIRO

RAÍZES PRIMITIVAS E APLICAÇÕES EM CRIPTOGRAFIA

Presidente da Banca: Profª. Drª. Grasiele Cristiane Jorge

Banca Examinadora:

Profª. Drª. Carina Alves Severo

Profª. Drª. Cintya Wink de Oliveira Benedito

Prof. Dr. Robson da Silva

Data da defesa: 03 de outubro de 2018

Aos meus avós, que infelizmente partiram antes de me verem concluindo essa jornada, mas que estiveram comigo em pensamento durante todos os momentos.

AGRADECIMENTOS

Agradeço os meus amigos e familiares pelo apoio, em especial à minha mãe, ao Pedro e às minhas amigas Karen e Shirley, que foram as minhas fortalezas durante todo o período em que estive estudando.

À minha orientadora, professora doutora Grasiele Cristiane Jorge, por toda disponibilidade, atenção, paciência, apoio e por me conduzir no desenvolvimento de toda a dissertação.

A todos os professores do programa PROFMAT, por compartilharem conosco os seus conhecimentos.

Aos colegas do PROFMAT, por estarem comigo nessa trajetória, compartilhando ideias, inseguranças, alegrias e conhecimento ao longo do curso.

E, por fim, agradeço ao ICT-Unifesp, por nos proporcionar toda a estrutura necessária para os nossos estudos.

RESUMO

Neste trabalho estudamos alguns tópicos relacionados à Teoria dos Números, com destaque para as raízes primitivas e algumas de suas aplicações na Criptografia: o método de troca de chaves de Diffie-Hellman e o algoritmo de criptografia ElGamal.

Como proposta didática, apresentamos uma sequência didática que tem como público alvo alunos do Ensino Médio. Tal sequência propõe atividades que objetivam ampliar a visão dos alunos sobre a Matemática, apresentando aplicações de resultados comuns à Educação Básica na Criptografia.

Palavras-chave: 1. Teoria dos Números. 2. Aritmética Modular. 3. Raízes Primitivas. 4. Criptografia. 5. Diffie-Hellman. 6. ElGamal.

ABSTRACT

In this work we study a few topics related to Number Theory, with emphasis on primitive roots and some of its applications in Cryptography: the Diffie-Hellman key exchange method and the ElGamal's cryptography algorithm.

We present a didactic sequence with focus on High School students as the target audience. This sequence suggests activities that aim to broaden students' perception of Mathematics, presenting applications of results common to Middle Education in Cryptography.

Keywords: 1. Number Theory. 2. Modular arithmetic. 3. Primitive roots. 4. Cryptography. 5. Diffie-Hellman. 6. ElGamal.

SUMÁRIO

1

INTRODUÇÃO

A Teoria dos Números é o ramo da Matemática que estuda as propriedades dos números inteiros e tem sua origem na Grécia Antiga. É possível encontrar problemas relativos a essa área no livro *Os Elementos*, escrito pelo matemático Euclides de Alexandria (325?a.C. – 285?a.C.).

Vários outros matemáticos gregos se dedicaram ao estudo de problemas relativos à Teoria dos Números, dentre eles podemos destacar Diofanto de Alexandria (200?a.C. – 284?a.C.), autor da obra *Aritmética*, que, segundo [4], é uma abordagem analítica da Teoria Algébrica dos Números que eleva o autor à condição de gênio em seu campo.

Apesar de estar presente nessas grandes obras dos gregos, a Teoria dos Números se desenvolveu muito pouco até o Século XVII, quando foi redescoberta por grandes matemáticos, como Fermat, Euler e Gauss.

O advogado francês Pierre de Fermat (1601 – 1665) se dedicava à Matemática em suas horas vagas. Sua atenção pela Teoria do Números foi despertada pelo contato com uma tradução da *Aritmética* de Diofanto. O interesse por essa área levou Fermat a umas das suas principais contribuições à Matemática: a fundação da moderna Teoria dos Números. Muitas de suas contribuições se deram por anotações no exemplar da obra de Diofanto e muitos teoremas apenas enunciados por Fermat mostraram-se verdadeiros posteriormente.

Leonhard Paul Euler (1707 – 1783) foi um matemático e físico suíço com numerosas contribuições em diversos campos da Matemática. Na Teoria dos Números, Euler apresentou importantes resultados, como o Teorema de Euler e a Função ϕ de Euler, os quais serão apresentados no Capítulo 2.

O matemático alemão, Johann Carl Friedrich Gauss (1777 – 1855), conhecido como o príncipe dos matemáticos, foi o maior matemático do Século XIX. Sua obra *Disquisitiones arithmeticae* trouxe importantes contribuições para a moderna Teoria dos Números, incluindo a notação para congruência utilizada nesse trabalho.

A maior parte das ideias apresentadas nessa dissertação são originárias ou da Grécia Antiga, ou de um dos três matemáticos citados. Para eles, o estudo das propriedades dos números inteiros era de interesse teórico apenas. As aplicações da Teoria dos Números foram surgindo posteriormente. Uma das principais áreas de aplicação da Teoria dos Números é a Criptografia.

A Criptografia é a ciência que estuda métodos para codificar mensagens de modo que apenas o seu destinatário as consiga ler. A utilização de tais métodos apresenta uma grande importância histórica quando se trata de guerras, pois, nesses períodos, conseguir transmitir mensagens a aliados sem que fossem interceptadas pelos inimigos era de extrema importância.

A necessidade de decifrar códigos impulsionou importantes avanços científicos, dentre eles a criação dos computadores. Um exemplo disso foi o *Colossus*, um computador primitivo criado pelo matemático e cientista da computação britânico Alan Turing (1912 – 1954) e utilizado para decodificar a máquina criptográfica *Lorenz*, utilizada pelos alemães durante a 2ª Guerra Mundial.

O desenvolvimento dos computadores e a utilização da internet vêm criando novos desafios para a Criptografia. A necessidade de aumentar a segurança da rede, devido a popularização de e-commerces e transações bancárias digitais, impulsiona a criação de métodos criptográficos cada vez mais seguros. Diante desses desafios, desenvolveu-se a criptografia de chave pública.

Enquanto os sistemas criptográficos antigos eram baseados em ferramentas elementares de substituição e permutação, os algoritmos de chave pública são baseados em funções matemáticas. Além disso, a criptografia de chave pública é assimétrica, ou seja, utiliza duas chaves distintas, diferente da criptografia simétrica que faz uso de uma única chave.

Introduzida pelos matemáticos estadunidenses Bailey Whitfield Diffie (1944 –) e Martin Edward Hellman (1945 –), a ideia dos códigos de chave pública apresenta uma importante mudança em relação aos códigos antigos, pois saber codificar uma mensagem utilizando um código de chave pública não necessariamente implica em saber decodificá-la. Isto se dá porque na criptografia assimétrica, uma das chaves é pública, ou seja, é conhecida por todos, enquanto a outra é mantida em sigilo. A chave pública é utilizada para criptografar a mensagem, enquanto a secreta é utilizada para descriptografar. Neste tipo de criptografia, conhecer a chave pública não é suficiente para descobrir a chave secreta. Esta ideia ficará clara no Capítulo 4, quando apresentamos o algoritmo criptográfico ElGamal, desenvolvido pelo criptógrafo egípcio Taher ElGamal(1955-).

O intuito desse trabalho é apresentar ao leitor um conceito bastante interessante da Teoria dos Números: as raízes primitivas, bem como a sua aplicação na definição dos logaritmos discretos e algumas ideias no campo da Criptografia, apresentadas no Capítulo 4. Além disso, elaboramos uma sequência didática, cujo público alvo são alunos do Ensino Médio. O objetivo dessa sequência é levar os alunos a descobrirem como o conceito de logaritmos pode ser interpretado dentro da aritmética modular e apresentar como essa ideia pode ser aplicada em um algoritmo criptográfico. Pretendemos com isso ampliar a visão dos alunos em relação à Matemática, mostrando a eles como as propriedades dos números inteiros são importantes para o desenvolvimento de algumas áreas da tecnologia.

Mais especificamente, este trabalho está detalhado como segue:

No Capítulo 1, são apresentados os conceitos preliminares de Teoria dos Números, como as ideias do Princípio da Boa Ordem e do Princípio da Indução Finita, que são importantes ferramentas para o trabalho com números inteiros. Além dos conceitos de Divisibilidade, Máximo Divisor Comum, Mínimo Múltiplo Comum e as definições de números primos e compostos e algumas propriedades.

No Capítulo 2, são introduzidas algumas ideias da Aritmética Modular, como os conceitos de congruência, congruência linear, classes de congruência. Além de alguns importantes resultados como o Pequeno Teorema de Fermat, o Teorema de Wilson, o Teorema de Euler e o Teorema Chinês dos Restos. No final deste capítulo são apresentadas algumas ideias relativas aos conceitos de grupos e subgrupos, pois esses conceitos são citados no Capítulo 4.

A intenção desses dois primeiros capítulos foi fazer um passeio pelas principais ideias dentro da Teoria dos Números.

No Capítulo 3, trazemos o conceito de raízes primitivas e algumas de suas propriedades. Essas raízes são importantes para a definição dos logaritmos discretos e a aplicação dos mesmos em um algoritmo criptográfico, denominado ELGamal, que apresentamos no Capítulo 4.

Por fim, no Capítulo 5, deixamos a proposta de uma sequência didática que trabalha algumas das ideias presentes nesse trabalho adaptadas para alunos do Ensino Médio.

2

CONCEITOS PRELIMINARES

Neste capítulo trataremos de alguns conceitos preliminares da Teoria dos Números, dentre eles o *Princípio da Boa Ordem*, o *Princípio da Indução Finita*, a *divisibilidade* no conjunto dos números inteiros, o *máximo divisor comum*, os *números primos* e *compostos* e o *Teorema Fundamental da Aritmética*. Para tanto, admitimos que o leitor esteja familiarizado com o *conjunto dos números inteiros*

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

e com as operações de adição e multiplicação e suas respectivas propriedades, além do conceito de módulo de um número inteiro.

As principais referências utilizadas neste capítulo foram [7], [9] e [11].

2.1 PRINCÍPIO DA BOA ORDEM

Para falar do Princípio da Boa Ordem, precisamos antes introduzir os conceitos de elemento mínimo e máximo de um conjunto.

Definição 2.1. *Seja A um subconjunto de $\mathbb{Z}$. Dizemos que A é limitado inferiormente se existe algum inteiro k tal que, para todo $a \in A$, $a \geq k$. Além disso, se $k \in A$, dizemos que k é elemento mínimo de A e denotamos por* $\min(A)$. *Analogamente, dizemos que A é limitado superiormente se existe algum inteiro k tal que, para todo $a \in A$, $a \leq k$. Além disso, se $k \in A$, dizemos que k é elemento máximo de A e denotamos por* $\max(A)$.

Note que se existe $k = \min(A)$, então k é único. De fato, considere que existam k e k' elementos mínimos de A, então, para todo $a \in A$, $a \geq k$ e $a \geq k'$. Como $k \in A$, temos que $k \geq k'$ e como $k' \in A$, temos que $k' \geq k$. De onde, $k = k'$. Portanto, se existe $k = \min(A)$, então k é único. De forma análoga, se existe $k'' = \max(A)$, então k'' é único.

De posse das definições de elemento mínimo e máximo de um conjunto, temos as ferramentas necessárias para demonstrar o Princípio da Boa Ordem.

Teorema 2.2. *(Princípio da Boa Ordem). Todo conjunto não vazio de inteiros não-negativos contém um elemento mínimo.*

Demonstração: Considere $S = \{0, 1, 2, 3, \ldots\}$ o conjunto dos inteiros não-negativos e considere um conjunto A, não vazio, tal que $A \subset S$. Note que se $0 \in A$, então $0 = \min(A)$, pois $0 = \min(S)$. Suponhamos que $0 \notin A$. Considere o conjunto $I_n = \{0, 1, 2, 3, \ldots, n\}$ e

$X = \{n \in \mathbb{Z}\,;\, I_n \subset S - A\}$. Note que existe um inteiro n, tal que $n \in X$ e $n+1 \notin X$. Além disso, note que se para algum $p \in A$, temos $p \leq n+1$, então $p = n+1$, pois não existe um inteiro p tal que $n \leq p \leq n+1$. Então, podemos concluir que $n+1$ é o menor elemento de A, ou seja, $n+1 = \min(A)$. ∎

O Princípio da Boa Ordem tem um importante papel em muitas demonstrações. Para ilustrar esse fato, provaremos a seguir uma importante propriedade dos números inteiros, a Propriedade Arquimediana.

Proposição 2.3. *(Propriedade Arquimediana) Sejam a e b inteiros positivos, então existe um inteiro positivo n tal que $na > b$.*

Demonstração: Suponha que, para todo inteiro positivo n, tem-se que $b \geq na$. Então, se tomarmos o conjunto

$$S = \{b - na\,;\, n \in \mathbb{Z}, n > 0\},$$

temos que esse conjunto S é formado por inteiros não-negativos. Pelo Princípio da Boa Ordem, S apresenta elemento mínimo, ou seja, existe $m \in S$ tal que $m = \min(S)$. Como $m \in S$, m é da forma $m = b - ra$, para algum $r \in \mathbb{Z}$.

Consideremos, agora, o elemento $m' = b - (r+1)a$, que também pertence ao conjunto S. Então, temos:

$$m' = b - (r+1)a = (b - ra) - a = m - a < m,$$

pois $a > 0$. Então $m' < m = \min(S)$, uma contradição. ∎

Exemplo 2.4. *Consideremos $a = 2$ e $b = 7$. Pela Propriedade Aquimediana, Proposição 2.3, temos que existe um inteiro positivo n tal que $na > b$. De fato, para $n = 4$, temos que $2 \cdot 4 = 8 > 7$.*

2.2 PRINCÍPIO DA INDUÇÃO FINITA

Apresentaremos, agora, as duas formas do Princípio da Indução Finita, uma importante ferramenta para demostrações em diversas áreas, em especial na Teoria dos Números.

Teorema 2.5. *(Princípio da Indução Finita - 1ª forma) Seja A um conjunto não-vazio de inteiros positivos maiores ou iguais a t, com as seguintes propriedades:*

(i) $t \in A$,

(ii) Se $k \in A$, então $k+1 \in A$.

Então, A contém todos os inteiros positivos maiores ou iguais a t.

Demonstração: Suponha que A não contenha todos os inteiros positivos maiores ou iguais a t. Então, podemos tomar o conjunto

$$B = \{n \in \mathbb{Z} \, ; \, n \geq t, n \notin A\}.$$

Pelo Princípio da Boa Ordem, B possui menor elemento b, pois $B \neq \emptyset$. Note que $b \neq t$, pois $t \in A$. Então, $b-1 \in A$ e como A satisfaz (ii), o sucessor de $b-1$, que é b, também pertence a A. Por conta dessa contradição, podemos concluir que o conjunto B é vazio e, portanto, A contém todos os inteiros positivos maiores ou iguais a t. ■

Exemplo 2.6. *Utilizaremos a primeira forma do Princípio da Indução finita para provar a validade da fórmula*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2},$$

para todo inteiro n, $n \geq 1$. Perceba que a fórmula é válida para $n = 1$, pois $\frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = 1$. De acordo com essa primeira forma do Princípio da Indução Finita, devemos mostrar que se a fórmula for verdadeira para $n = k, k \in \mathbb{Z}$, $k \geq 1$, então ela também será verdadeira para $n = k + 1$. Desta forma, suponhamos que seja válida a fórmula

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Como se trata de uma igualdade, podemos adicionar $k+1$ a ambos os membros, mantendo a relação de igualdade.

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1).$$

Efetuando a adição no segundo membro, temos

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1) + 2(k+1)}{2}.$$

De onde,

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}.$$

Essa última igualdade corresponde à fórmula inicial com $n = k+1$ e nos mostra que a validade da fórmula para $n = k$ implica na validade dessa mesma fórmula pra $n = k+1$. Note que se tomarmos $k = 1$, cuja validade da fórmula já verificamos, isso implicaria a validade para $k + 1 = 2$. Então, podemos tomar $k = 2$, o que implicaria a validade da fórmula para $k + 1 = 3$ e assim sucessivamente, passando por todos os inteiros maiores ou iguais a 1. Portanto, pela primeira forma do Princípio da Indução Finita, a fórmula

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

é válida para todo $n \in \mathbb{Z}, n \geq 1$.

Há uma outra versão para o Princípio da Indução Finita, enunciada a seguir.

Teorema 2.7. *(Princípio da Indução Finita - 2^a forma). Seja A um conjunto não-vazio de inteiros positivos maiores ou iguais a t, com as seguintes propriedades:*

(i) $t \in A$

(ii) Se $t, t+1, t+2, \ldots, t+k \in A$, *então* $(t+k)+1 \in A$.

Então, A contém todos os inteiros positivos maiores ou iguais a t.

Demonstração: O argumento para a demonstração dessa segunda forma do Princípio da Indução Finita é similar ao utilizado para a demonstração da primeira forma.

Suponha que A não contenha todos os inteiros positivos maiores ou iguais a t. Então, podemos tomar o conjunto B,

$$B = \{n \in \mathbb{Z} \, ; \, n \geq t \text{ e } n \notin A\}.$$

Pelo Princípio da Boa Ordem, B possui menor elemento $t+b$, pois $B \neq \emptyset$. Note que $t+b \neq t$, pois $t \in A$. Como $b = \min(B)$, temos que $t, \ldots, t+(b-1) \in A$ e como A satisfaz (ii), o sucessor de $t+(b-1)$ que é $t+b$ também pertence a A. Por conta dessa contradição, podemos concluir que o conjunto B é vazio e, portanto, A contém todos os inteiros positivos maiores ou iguais a t. ■

Exemplo 2.8. *Considere a sequência S na qual $a_1 = 1, a_2 = 3$ e $a_n = a_{n-1} + a_{n-2}$. Então, $S = 1, 3, 4, 7, 11, 18, \ldots$. Vamos utilizar a segunda forma do Princípio da Indução Finita para provar que a propriedade*

$$a_n < \left(\frac{7}{4}\right)^n$$

é válida para todo inteiro n, $n \geq 1$.

Considere o conjunto $A = \left\{n \in \mathbb{Z}, n \geq 1 \, ; \, a_n < \left(\frac{7}{4}\right)^n, a_n \in S\right\}$. Note que $1 \in A$, pois $a_1 = 1 < \frac{7}{4} = \left(\frac{7}{4}\right)^1$. E, pela segunda forma do Princípio da Indução Finita, se $1, 2, \ldots, k \in A$ implicar que $k+1 \in A$, temos que a propriedade será válida para todo inteiro $n, n \geq 1$. Suponhamos, então, que $1, 2, \ldots, k \in A$. Em particular, $k-1$ e $k \in A$, ou seja, $a_{k-1} < \left(\frac{7}{4}\right)^{k-1}$ e $a_k < \left(\frac{7}{4}\right)^k$. Além disso, pela lei de recorrência da sequência S, temos

$$a_{k+1} = a_k + a_{k-1}.$$

De onde,

$$\begin{aligned} a_{k+1} &= \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} \\ &= \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4} + 1\right) \\ &= \left(\frac{7}{4}\right)^{k-1} \left(\frac{11}{4}\right). \end{aligned}$$

Como $\frac{11}{4} < \frac{49}{16} = \left(\frac{7}{4}\right)^2$, *temos*

$$a_{k+1} < \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^{k+1}.$$

Com isso mostramos que $k+1 \in A$ *e, pela segunda forma do Princípio da Indução Finita, temos que a propriedade* $a_n < \left(\frac{7}{4}\right)^n$ *é válida para todo* n *inteiro positivo.*

2.3 DIVISIBILIDADE

Apresentaremos, agora, a definição de divisibilidade entre dois números inteiros e suas propriedades.

Definição 2.9. *Dados* a *e* b *números inteiros, diz-se que* a *divide* b*, denotado por* $a \mid b$*, se existe um inteiro* c *tal que* $ac = b$*. Caso contrário, dizemos que* a *não divide* b *e denotamos por* $a \nmid b$*.*

Observação 2.10.

(i) Dizer que a *divide* b *é o mesmo que dizer que* a *é um divisor de* b*, ou que* b *é um múltiplo de* a*.*

(ii) Note que, para o caso $a \neq 0$ *o inteiro* c*, nas condições da definição é único. De fato, se existisse* c' *tal que* $ac' = b$*, teríamos* $ac = ac'$*, de onde* $c = c'$*, pois* $a \neq 0$*. A esse inteiro* c*, chamaremos quociente de* b *por* a *e o indicaremos por:* $c = b/a = \frac{b}{a}$*. A unicidade não acontece quando* $b = 0$ *e* $a = 0$*, pois nesse caso teríamos* $0c = 0$*, para todo* c *inteiro.*

Exemplo 2.11. *Como* $3 \cdot 7 = 21$*, dizemos que* $3 \mid 21$*. Como não existe um número inteiro* c*, tal que* $4c = 21$*, dizemos que* $4 \nmid 21$*.*

As proposições que seguem tratam de algumas propriedades importantes da divisibilidade.

Proposição 2.12. *(Reflexividade) Seja* a *um número inteiro, então* $a \mid a$*.*

Demonstração: Como $1a = a$, $\forall a \in \mathbb{Z}$, temos, pela definição de divisibilidade, que $a \mid a$.

Proposição 2.13. *(Transitividade) Dados* a, b *e* c *números inteiros. Se* $a \mid b$ *e* $b \mid c$*, então* $a \mid c$*.*

Demonstração: Como $a \mid b$, temos que existe $k \in \mathbb{Z}$ tal que $ak = b$. Do mesmo modo, temos que existe $k' \in \mathbb{Z}$ tal que $bk' = c$. Substituindo b por ak na segunda igualdade, temos: $c = (ak)k' = a(kk')$, ou seja, $a \mid c$. ∎

Proposição 2.14. *Sejam* a, b, c, m *e* $n \in \mathbb{Z}$*. Se* $c \mid a$ *e* $c \mid b$*, então* $c \mid (ma + nb)$*.*

Demonstração: Se $c \mid a$, então $a = ck$, para algum $k \in \mathbb{Z}$. Se $c \mid b$, então $b = ck'$, para algum $k' \in \mathbb{Z}$. Multiplicando as duas igualdades por m e n, respectivamente, temos:

$$ma = mck \text{ e } nb = nck'.$$

Somando membro a membro as duas igualdades, temos:

$$ma + nb = mck + nck'.$$

De onde,

$$ma + nb = (mk + nk')c,$$

ou seja,

$$c \mid (ma + nb).$$

■

Proposição 2.15. *Dados os números inteiros* $0, 1, a, b$ *e* c*, valem as seguintes propriedades para a divisão:*

(i) *Se* $a \mid b$*, então* $ac \mid bc$*, ou;*

(ii) *Se* $ab \mid ac$ *e* $a \neq 0$*, então* $b \mid c$*, ou;*

(iii) $1 \mid a$*, ou;*

(iv) $a \mid 0$*, ou;*

(v) *Se* $a \mid b$ *e* $b \neq 0$*, então* $|a| \leq |b|$*, ou;*

(vi) *Se* $a \mid b$ *e* $b \mid a$*, então* $|a| = |b|$*, ou;*

(vii) $a \mid |c| \mid ac$.

Demonstração:

(i) Se $a \mid b$, temos que existe $k \in \mathbb{Z}$ tal que $ak = b$. Multiplicando os dois lados dessa igualdade por c, temos:

$$(ak)c = bc.$$

De onde,

$$(ac)k = bc.$$

Assim, podemos concluir que $ac \mid bc$.

(ii) Se $ab \mid ac$, temos que existe $k \in \mathbb{Z}$ tal que:

$$(ab)k = ac.$$

De onde, $a(bk - c) = 0$. Como $a \neq 0$, temos:

$$bk = c.$$

De onde, podemos concluir que $b \mid c$.

(iii) Como $1a = a$, $\forall a \in \mathbb{Z}$, temos, pela definição de divisibilidade, que $1 \mid a$.

(iv) Como $0a = 0$, $\forall a \in \mathbb{Z}$, temos, pela definição de divisibilidade, que $a \mid 0$.

(v) Se $a \mid b$, temos que existe $k \in \mathbb{Z}$, tal que $ak = b$. Então,

$$|ak| = |b|.$$

De onde,

$$|a| \cdot |k| = |b|.$$

Como $b \neq 0$, temos que $|b| > 0$ e $|k| > 0$. Então, podemos concluir que:

$$|a| \leq |b|.$$

(vi) Se $a \mid b$, então existe $k \in \mathbb{Z}$, tal que $ak = b$. Por (v), temos $|a| \leq |b|$. Do mesmo modo, se $b \mid a$, temos $|b| \leq |a|$.
Das duas desigualdades anteriores, podemos concluir que:

$$|a| = |b|.$$

(vii) Se $c \geq 0$, temos que $a\,|c| = ac$, então, pela Proposição 2.12, $a\,|c| \mid ac$. Se $c < 0$, $a\,|c| = -ac$, ou seja, $-(a\,|c|) = ac$, então, $a\,|c| \mid ac$.

■

Observação 2.16. *Note que a relação de divisibilidade não é uma relação de ordem em $\mathbb{Z}$, pois apesar de ser reflexiva, Proposição 2.12, e transitiva, Proposição 2.13, ela não é antissimétrica. De fato, se $a \mid b$ e $b \mid a$, a não necessariamente é igual a b. Exemplo, $3 \mid -3$ e $-3 \mid 3$, mas $3 \neq -3$.*

Vejamos mais algumas propriedades da divisibilidade:

Proposição 2.17. *Sejam a, b, c e $d \in \mathbb{Z}$. Se $a \mid b$ e $c \mid d$ então $ac \mid bd$.*

Demonstração: Se $a \mid b$, então existe $k \in \mathbb{Z}$, tal que $ak = b$. Do mesmo modo, se $c \mid d$, então existe $k' \in \mathbb{Z}$, tal que $ck' = d$. Multiplicando os membros das igualdades anteriores, temos:

$$(ak) \cdot (ck') = bd.$$

de onde,

$$(ac) \cdot (kk') = bd.$$

Portanto, podemos concluir que $ac \mid bd$. ■

Exemplo 2.18. *Considere* $a = 2, b = -8, c = -3$ *e* $d = 6$. *Note que* $a \mid b$, *pois* $2 \cdot (-4) = -8$. *Além disso,* $c \mid d$, *pois* $-3 \cdot 2 = 6$. *De fato,* $ac \mid bd$, *pois* $ac = 2 \cdot (-3) = -6$, $bd = -8 \cdot 6 = -48$ *e* $-6 \mid -48$.

Proposição 2.19. *Sejam* $a, b, c \in \mathbb{Z}$, *tais que* $a \mid (b \pm c)$. *Então,*

$$a \mid b \Leftrightarrow a \mid c.$$

Demonstração: Se $a \mid (b + c)$, então existe $k \in \mathbb{Z}$ tal que $ak = b + c$. Além disso, se $a \mid b$, então existe $k' \in \mathbb{Z}$ tal que $ak' = b$. Substituindo b por ak' na primeira igualdade, temos:

$$ak' + c = ak,$$

ou seja,

$$c = ak - ak' = a(k - k'),$$

de onde podemos concluir que $a \mid c$. A demonstração é análoga para o caso $a \mid (b - c)$. ■

2.4 O ALGORITMO DE EUCLIDES

Apresentaremos, agora, um importante resultado, conhecido como Algoritmo Euclidiano da Divisão.

Lema 2.20. *Sejam* $a, b \in \mathbb{Z}$, *com* $a \geq 0$ *e* $b > 0$. *Então, existem inteiros* q *e* r, *tais que* $a = bq + r$ *e* $0 \leq r < b$.

Demonstração: Considere o seguinte conjunto:

$$S = \{a - bx \,;\, x \in \mathbb{Z}, a - bx \geq 0\}.$$

Note que, quando $x = 0$, $a - bx \in S$, pois $a - bx = a \geq 0$. Assim, podemos concluir que $S \neq \emptyset$. Pelo Princípio da Boa Ordem, Teorema 2.2, S possui elemento mínimo. Chamaremos esse elemento de r. Como $r \in S$, $r = a - bq$ para algum $q \in \mathbb{Z}$. Resta mostrar que $r < b$. Suponha $r \geq b$, então

$$r - b \geq 0.$$

Como $r = a - bq$, temos

$$a - bq - b \geq 0,$$

de onde, $a - b(q+1) \geq 0$. Ou seja, $a - b(q+1) \in S$. Mas, $a - b(q+1) < a - bq = r$, o que é uma contradição, pois $r = min\, S$. ∎

Teorema 2.21. *(Algoritmo Euclidiano da Divisão) Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então, existem inteiros q e r, únicos, tais que $a = bq + r$ e $0 \leq r < |b|$.*

Demonstração: Vamos demonstrar inicialmente a existência de q e r, dividindo a demonstração em alguns casos:

(i) $b > 0$ e $a \geq 0$: Esse resultado pode ser constatado pelo Lema 2.20.

(ii) $b > 0$ e $a < 0$: Pelo Lema 2.20, temos que existem $q', r' \in \mathbb{Z}$, tais que $|a| = bq' + r'$ e $0 \leq r' < b$. Para $r = 0$, temos $a = -|a| = b(-q') + 0$. Portanto, as condições do teorema são satisfeitas para $q = -q'$ e $r = 0$. Para $r > 0$, temos $a = -|a| = -(bq' + r') = b(-q') - r'$. Somando e subtraindo b ao segundo membro dessa igualdade, temos:

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

Logo,

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

Como $0 < b - r' < b$, temos que as condições do teorema são satisfeitas para $q = -q' - 1$ e $r = b - r'$.

(iii) $b < 0$: Novamente, pelo Lema 2.20, temos que existem q', $r' \in \mathbb{Z}$, tais que $a = |b|q' + r'$ e $0 \leq r' < |b|$. Como $b < 0$, então $|b| = -b$. Assim,

$$a = -bq' + r' = b(-q') + r',$$

o que verifica as condições do teorema para $q = -q'$ e $r = r'$.

Por fim, vamos verificar a unicidade de q e r. Suponha que existam inteiros q' e r', satisfazendo as condições do enunciado e vamos mostrar que $q = q'$ e $r = r'$. Temos que $bq + r = a = bq' + r'$. Suponha, sem perda de generalidade, que $r' \geq r$. Então:

$$b(q - q') = r' - r.$$

Como $|b| > r'$, então $|b| > r' - r$, de onde:

$$b(q - q') < |b|.$$

Como $b(q - q') \geq 0$, podemos tomar os módulos:

$$0 \leq |b||q - q'| < |b|.$$

E, como $|b| > 0$, temos $0 \leq |q - q'| < 1$. De onde, podemos concluir que $|q - q'| = 0$, ou seja, $q = q'$. E, da igualdade $bq + r = bq' + r'$, temos $r = r'$. ∎

Definição 2.22. *O número a do Teorema 2.21 é chamado de dividendo, o número b divisor e os números q e r são chamados, respectivamente, quociente e resto da divisão de b por a.*

2.5 MÁXIMO DIVISOR COMUM

Nesta seção, apresentaremos a definição de *máximo divisor comum* e algumas propriedades relativas a esse conceito.

Definição 2.23. *Dados a e b inteiros, com $a \neq 0$ ou $b \neq 0$, o máximo divisor comum de a e b, denotado por (a, b), é o maior inteiro d, tal que $d \mid a$ e $d \mid b$. Quando $(a, b) = 1$ dizemos que a e b são primos entre si.*

Teorema 2.24. *(Teorema de Bézout) Sejam $a, b \in \mathbb{Z}$ e $d = (a, b)$. Então existem $m, n \in \mathbb{Z}$, tais que $d = ma + nb$.*

Demonstração: Seja $B = \{na + mb \ ; \ m, n \in \mathbb{Z}\}$. Tomemos $c = n_0a + m_0b$ o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c \mid a$ e $c \mid b$.

Suponha que c não divide a. Neste caso, existem $q, r \in \mathbb{Z}$ tais que $a = qc + r$, com $0 < r < c$. Portanto, $r = a - qc = a - q(n_0a + m_0b) = (1 - qn_0)a + (-qm_0)b$. Isso mostra que $r \in B$, o que é uma contradição, pois $r < c$ e c é o menor elemento de B. Portanto, $c \mid a$. E, de forma análoga, mostramos que $c \mid b$.

Como $d \mid a$ e $d \mid b$, temos, pela Proposição 2.14, que $d \mid c$. Pela Proposição 2.15, item (v), temos que $d \leq c$, pois ambos são positivos. Como d é o máximo divisor comum, temos que a única possibilidade é $d = c$, ou seja, $d = n_0a + m_0b$. ∎

Proposição 2.25. *Sejam $a, b \in \mathbb{Z}$ e seja d um inteiro positivo. Dizemos que $d = (a, b)$ se, e somente se, verifica:*

(i) $d \mid a$ e $d \mid b$,

(ii) Se $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

Demonstração: Seja $d = (a, b)$. Pela Definição 2.23, temos que d é um divisor comum de a e de b, portanto, vale (i). Além disso, pelo Teorema 2.24, existem m, $n \in \mathbb{Z}$, tais que $d = ma + nb$. Seja d' um divisor comum de a e b. Então, $d' \mid a$ e $d' \mid b$, de onde temos que existem m', $n' \in \mathbb{Z}$, tais que $a = m'd'$ e $b = n'd'$. Portanto, $d = m(m'd') + n(n'd') = d'(mm' + nn')$, o que mostra que $d' \mid d$. Agora, seja d um inteiro positivo de modo que valem (i) e (ii). Por (i), temos que d é um divisor comum de a e b. Por (ii), temos que qualquer d', divisor comum de a e b, divide d. Portanto, d é o maior dos divisores comuns de a e b. Ou seja, $d = (a, b)$. ∎

Exemplo 2.26. *Considere os números 12 e 18. Temos que os divisores de 12 são $\{1, 2, 3, 4, 6, 12\}$ e que os divisores de 18 são $\{1, 2, 3, 6, 9, 18\}$. Portanto, o maior divisor comum de 12 e 18 é o número 6. Note que 3 também é divisor comum de 12 e 18, pois $3 \mid 12$ e $3 \mid 18$. Portanto, $3 \mid 6$.*

Proposição 2.27. *Dados a, $b \in \mathbb{Z}$, se existem $m, n \in \mathbb{Z}$, tais que $am + bn = 1$, então $(a, b) = 1$.*

Demonstração: Se $(a, b) = d$, então $d \mid a$ e $d \mid b$. Logo, $d \mid (am + bn)$, pela Proposição 2.14. Portanto, $d = 1$. ■

Proposição 2.28. *Sejam a, b inteiros, $d = (a, b)$ e c um inteiro não-nulo. Então:*

(i) $(ac, bc) = d\,|c|$.

(ii) Se $c \mid a$ e $c \mid b$, então $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{d}{|c|}$.

Demonstração:

(i) Como $d = (a, b)$, temos que $d \mid a$ e então $d\,|c| \mid a\,|c|$. Como $a\,|c|$ divide ac, então $d\,|c| \mid ac$. Do mesmo modo, temos que $d\,|c| \mid bc$. Pelo Teorema 2.24, existem inteiros r e s, tais que $d = ra + sb$. Logo,

$$d\,|c| = r(a\,|c|) + s(b\,|c|).$$

Agora, se d' é um inteiro tal que $d' \mid ac$ e $d' \mid bc$, então $d' \mid a\,|c|$ e $d' \mid b\,|c|$. Da igualdade anterior, temos que $d' \mid d|c|$. Portanto, $d|c| = (ac, bc)$.

(ii) Seja $x = \left(\frac{a}{c}, \frac{b}{c}\right)$. Por (i), temos:

$$(a, b) = \left(\frac{a}{c} \cdot c, \frac{b}{c} \cdot c\right) = \left(\frac{a}{c}, \frac{b}{c}\right) \cdot |c|.$$

Assim, $d = x|c|$ e, portanto, como $c \neq 0$, $x = \frac{d}{|c|}$.

■

Corolário 2.29. *Se $(a, b) = d$, temos que* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração: Do item (ii) da Proposição 2.28, se tomarmos c o máximo divisor comum de a e b, teremos:

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{d}{|d|} = 1.$$

■

Exemplo 2.30. *Como $(18, 24) = 6$, temos que* $\left(\frac{18}{6}, \frac{24}{6}\right) = (3, 4) = 1$.

Proposição 2.31. *Dados $a, b, c \in \mathbb{Z}$, temos que $(a, b) = (a, b + ac)$.*

Demonstração: Sejam $d = (a, b)$ e $d' = (a, b + ac)$. Pelo Teorema 2.24, existem inteiros n_0 e m_0 tais que $d = n_0 a + m_0 b$, de onde:

$$d = n_0 a + m_0 b = n_0 a + acm_0 - acm_0 + m_0 b = a(n_0 - cm_0) + (b + ac)m_0,$$

ou seja, $d' \mid d$.

Agora, vamos provar que $d \mid d'$. Pela Proposição 2.14, $d \mid (b + ac)$. Então, d é divisor comum de a e $b + ac$. Logo pelo Teorema 2.25, temos que $d \mid d'$. De onde, podemos concluir que $d = d'$, pois ambos são positivos. ■

Exemplo 2.32. *Temos que* $(5, 15) = 5$. *Logo,* $(5, 15 + 1 \cdot 5) = (5, 20) = 5$; $(5, 15 + 2 \cdot 5) = (5, 25) = 5$ *e assim por diante.*

Teorema 2.33. *(Teorema de Euclides) Sejam* $a, b, c \in \mathbb{Z}$*, tais que* $a \mid bc$*. Se* $(a, b) = 1$*, então* $a \mid c$*.*

Demonstração: Como $(a, b) = 1$, pelo Teorema 2.24 existem inteiros n e m tais que $na + mb = 1$. Multiplicando-se os dois lados desta igualdade por c, temos:

$$(na)c + (mb)c = n(ac) + m(bc) = c.$$

Como $a \mid ac$ e $a \mid bc$, temos que, pela Proposição 2.14, $a \mid c$. ■

Exemplo 2.34. *Temos que* $7 \mid 84$ *e* $84 = 14 \cdot 6$*. Como* $(7, 6) = 1$*, temos que* $7 \mid 14$*.*

Proposição 2.35. *Sejam* $a, b, c \in \mathbb{Z}$*, com* $(a, b) = 1$*,* $a \mid c$ *e* $b \mid c$*. Então,* $ab \mid c$*.*

Demonstração: Se $a \mid c$, podemos escrever $c = aq$, para algum $q \in \mathbb{Z}$. Como $b \mid c$, temos $b \mid aq$ e, como $(a, b) = 1$, temos $b \mid q$. Ou seja, podemos escrever $q = br$ para algum $r \in \mathbb{Z}$. Substituindo na primeira igualdade, temos que $c = a(br) = (ab)r$, o que nos mostra que $ab \mid c$. ■

A partir da relação apresentada pelo Algoritmo Euclidiano da Divisão, podemos encontrar o importante resultado, apresentado a seguir.

Proposição 2.36. *Sejam* $a, b \in \mathbb{Z}$*, com* $b \neq 0$ *e sejam* q, r *o quociente e o resto da divisão de* a *por* b*, respectivamente. Então,* $(a, b) = (b, r)$*.*

Demonstração: Temos que $a = bq + r$. Seja $x \in \mathbb{Z}$, tal que $x \mid a$ e $x \mid b$. Podemos reescrever a igualdade anterior como $r = a - bq$ e, portanto, $x \mid r$. Com isso mostramos que o conjunto dos divisores de a e b está contido no conjunto do divisores de b e r. Agora, considere $y \in \mathbb{Z}$ tal que $y \mid b$ e $y \mid r$. Da igualdade $a = bq + r$, temos que $y \mid a$. Assim, mostramos a inclusão contrária e podemos concluir que o conjunto dos divisores de a e b é igual ao conjunto dos divisores de b e r. Portanto, $(a, b) = (b, r)$. ■

Da proposição anterior, podemos concluir que o problema de encontrar (a, b) pode ser resumido em encontrar (b, r). Podemos repetir esse processo fazendo divisões sucessivas entre o divisor e o resto da divisão anterior, conforme descrito a seguir e obtendo em cada uma delas um quociente e um resto. Como o resto diminui a cada novo passo, em alguma

das divisões, obteremos resto nulo. Este método é conhecido como Algoritmo de Euclides e funciona da seguinte forma:

$$\begin{aligned} a &= bq_1 + r_1, 0 \leq r_1 < |b| \\ b &= r_1q_2 + r_2, 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Como, $r_n \mid r_{n-1}$, temos que $(r_{n-1}, r_n) = r_n$, O que nos leva a concluir que:

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n.$$

Portanto, o máximo divisor comum de a e b é o último resto diferente de zero obtido a partir desse processo.

Exemplo 2.37. *Vamos utilizar o processo apresentado para obter* $(1207, 300)$. *Temos que*

$$\begin{aligned} 1207 &= 300 \cdot 4 + 7 \\ 300 &= 7 \cdot 42 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6. \end{aligned}$$

Note que o último resto não nulo que obtivemos nesse processo é 1, portanto $(1207, 300) = 1$.

2.6 NÚMEROS PRIMOS

Nesta seção, apresentaremos a definição de números primos e alguns resultados que envolvem esses números.

Definição 2.38. *Um número primo é um número inteiro* n, $n > 1$, *que possui somente dois divisores positivos,* n *e 1. Se* n *não é primo, dizemos que* n *é composto.*

Proposição 2.39. *Se um número primo* p *não divide um inteiro* a, *então* $(a, p) = 1$.

Demonstração: Seja $d = (a, p)$. Então $d \mid a$ e $d \mid p$. Da relação $d \mid p$, temos, pela Definição 2.38, que $d = 1$ ou $d = p$. Como $d = p$ é impossível, pois $p \nmid a$, então, $d = 1$, isto é, $(a, p) = 1$.

Proposição 2.40. *Se* p *é um número primo e* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b$.

Demonstração: Se p não divide a, pela Proposição 2.39, $(a, p) = 1$. Então, pelo Teorema 2.33, $p \mid b$. Analogamente, $p \nmid b$ implica que $p \mid a$. ■

Corolário 2.41. *Se um número primo p divide um produto $a_1 a_2 \dots a_n$, então $p \mid a_k$, para algum k, $1 \leq k \leq n$.*

Demonstração: Demonstraremos esse resultado por indução sobre n, para todo $n \geq 2$.

Se $n = 2$, o resultado segue da Proposição 2.40. Suponha que o resultado seja válido para $n = j$.

Se $p \mid a_1 \cdot a_2 \cdots a_j a_{j+1} = (a_1 \cdot a_2 \cdots a_j) a_{j+1}$, então pela Proposição 2.40 $p \mid (a_1 a_2 \cdots a_j)$ ou $p \mid a_{j+1}$. Se $p \mid a_{j+1}$, o resultado é válido. Caso contrário, $p \mid (a_1 a_2 \cdots a_j)$ e, por hipótese de indução, $\exists\, k, 1 \leq k \leq j$, tal que $p \mid a_k$. Logo, o resultado é válido para $n = j + 1$. Portanto, esse resultado é válido para todo $n \geq 2$. ■

Teorema 2.42. *(Teorema Fundamental da Aritmética) Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração: Se n é primo não há nada a ser demonstrado. Suponhamos, então, n composto. Seja p_1, $p_1 > 1$, o menor dos divisores positivos de n diferente de 1. Podemos afirmar que p_1 é primo, caso contrário existiria p, $1 < p < p_1$, com $p \mid p_1$ e então $p \mid n$, o que seria uma contradição, pois p_1 é o menor divisor positivo de n. Logo, podemos escrever $n = p_1 n_1$, com p_1 primo.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2, $p_2 > 1$, como o menor divisor positivo de n_1. Pelo argumento anterior, p_2 é primo e podemos escrever $n = p_1 p_2 n_2$, com p_1, p_2 primos.

Repetindo esse raciocínio, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, \dots$. Como todos estes inteiros são maiores do que 1, este processo deve terminar e então $n = p_1 p_2 \cdots p_k$ para algum $k \geq 2$. Como os primos $p_1, p_2, \dots, p_k$ não são, necessariamente, distintos, n terá a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}.$$

Para mostrarmos a unicidade da fatoração usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 é primo e divide o produto $q_1 q_2 \cdots q_r$, pelo Corolário 2.41 ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \mid q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_r$. Como $1 < \frac{n}{p_1} < n$, pela hipótese de indução

temos que as duas fatorações de $\frac{n}{p_1}$ são idênticas, isto é, $s = r$ e as fatorações $p_1 p_2 \cdots p_s$ e $q_1 q_2 \cdots q_r$ são iguais. ■

Observação 2.43. *Se $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}$, o conjunto de todos os divisores positivos de n é o conjunto de todos os números da forma $p_1^{c_1} p_2^{c_2} p_3^{c_3} \cdots p_n^{c_n}$, $0 \leq c_i \leq a_i$, $i = 1, 2, \ldots, n$.*

Proposição 2.44. *Se dois inteiros positivos a e b possuem as fatorações*

$$a = \prod_{i=1}^{\infty} p_i^{a_i} \text{ e } b = \prod_{i=1}^{\infty} p_i^{b_i},$$

então o máximo divisor comum de a e b é igual a:

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i}$$

onde $c_i = min\{a_i, b_i\}$.

Demonstração: Para que o produto $\prod_{i=1}^{\infty} p_i^{c_i}$ seja um divisor comum de a e b, devemos ter $c_i \leq a_i$ e $c_i \leq b_i$, então se tomarmos $c_i = min\{a_i, b_i\}$, garantimos essa condição. ■

Teorema 2.45. *(Euclides) A sequência dos números primos é infinita.*

Demonstração: Suponhamos que a sequência dos números primos seja finita. Seja $p_1, p_2, \ldots, p_n$ a lista de todos os primos. Consideremos o número $R = p_1 p_2 \cdots p_n + 1$. É claro que R não é divisível por nenhum dos $p_i, 1 \leq i \leq n$ de nossa lista pois se fosse divisível por alguns deles, o número 1 também seria, o que não acontece. Além disso, R é maior do que qualquer $p_i, 1 \leq i \leq n$. Agora, pelo Teorema Fundamental da Aritmética, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence à nossa lista. Portanto a sequência dos números primos não é finita. ■

Proposição 2.46. *Para qualquer inteiro positivo k, existem k inteiros consecutivos todos compostos.*

Demonstração: Para demonstrarmos este resultado observamos que como $(k+1)!$ é divisível por todos os k números entre 2 e $k+1$, então a sequência

$$(k+1)! + 2, (k+1)! + 3, \ldots, (k+1)! + k, (k+1)! + (k+1)$$

é composta por k números consecutivos compostos. ■

Exemplo 2.47. *Pela Proposição 2.46, para $k = 5$, podemos encontrar 5 inteiros consecutivos, todos compostos. De fato, os números $(5+1)! + 2, (5+1)! + 3, (5+1)! + 4$, $(5+1)! + 5, (5+1)! + 6 = 722, 723, 724, 725, 726$ são todos compostos, pois $722 = 2 \cdot 19^2$, $723 = 3 \cdot 241$, $724 = 2^2 \cdot 181$, $725 = 5^2 \cdot 29$ e $726 = 2 \cdot 3 \cdot 11^2$.*

Proposição 2.48. *Se n não é primo, então n possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{n}$.*

Demonstração: Se n é um número composto, então podemos escrever $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Podemos supor, sem perda de generalidade, que $n_1 \leq n_2$. Note que $n_1 \leq \sqrt{n}$, pois, caso contrário, $n_1 > \sqrt{n}$ e $n_2 > \sqrt{n}$, o que implicaria em $n = n_1 n_2 > \sqrt{n}\sqrt{n} = n$, o que é absurdo. Tomando p um fator primo de n_1, temos que $p \leq n_1 \leq \sqrt{n}$ e, além disso, p é também um fator primo de n. ∎

2.7 MÍNIMO MÚLTIPLO COMUM

Apresentaremos, agora, a definição de *mínimo múltiplo comum* e algumas propriedades referentes a esse conceito.

Definição 2.49. *O mínimo múltiplo comum de dois inteiros positivos a e b, denotado por $[a, b]$, é o menor inteiro positivo divisível por a e por b.*

Exemplo 2.50. *Considere os números 12 e 15. Temos que os múltiplos de 12 são $\{0, 12, 24, 36, 48, 60, \ldots\}$ e que os múltiplos de 15 são $\{0, 15, 30, 60, \ldots\}$. Temos que o menor inteiro positivo que é múltiplo de 12 e de 15 e, portanto, divisível por 12 e por 15 é o número 60. Então, $[12, 15] = 60$.*

Proposição 2.51. *Se dois inteiros positivos a e b possuem as fatorações*

$$a = \prod_{i=1}^{\infty} p_i^{a_i} \text{ e } b = \prod_{i=1}^{\infty} p_i^{b_i},$$

então o mínimo múltiplo comum de a e b é igual a:

$$[a, b] = \prod_{i=1}^{\infty} p_i^{c_i},$$

onde $c_i = max\{a_i, b_i\}$.

Demonstração: Para que o produto $\prod_{i=1}^{\infty} p_i^{c_i}$ seja um múltiplo comum de a e b, devemos ter $c_i \geq a_i$ e $c_i \geq b_i$, então se tomarmos $c_i = \max\{a_i, b_i\}$, garantimos essa condição. Além disso, tomando $c_i = \max\{a_i, b_i\}$, teremos, não apenas um múltiplo comum, mas o menor possível entre todos eles. ∎

Lema 2.52. *Sejam a e b inteiros. Então, $[a, b]$ divide todo múltiplo comum de a e b.*

Demonstração: Seja $d = [a, b]$ e d' um múltiplo comum de a e b, diferente de d. Sejam,

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \text{ e } b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}; a_i \geq 0, b_i \geq 0.$$

Como d' é múltiplo de a e de b, temos que para algum $k \in \mathbb{Z}$, $d' = k p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, onde $s_i \geq max\{a_i, b_i\}$. Como,

$$d = p_1^{max\{a_1,b_1\}} p_2^{max\{a_2,b_2\}} \cdots p_n^{max\{a_n,b_n\}},$$

temos que,

$$d' = k\prod_{i=1}^{n} p_i^{s_i - max\{a_i,b_i\}} \prod_{i=1}^{n} p_i^{max\{a_i,b_i\}}.$$

Ou seja, d' é um múltiplo de d e, portanto, $d \mid d'$. ■

Proposição 2.53. *Para a e b inteiros positivos temos, $[a,b] \cdot (a,b) = a \cdot b$.*

Demonstração: Sejam a e b dados pelas seguintes fatorações:

$$a = \prod_{i=1}^{\infty} p_i^{a_i} \text{ e } b = \prod_{i=1}^{\infty} p_i^{b_i}.$$

Temos, pelo Proposição 2.44 e pela Proposição 2.51 que:

$$(a,b) = \prod_{i=1}^{\infty} p_i^{min\{a_i,b_i\}} \text{ e } [a,b] = \prod_{i=1}^{\infty} p_i^{max\{a_i,b_i\}}.$$

Note que, se x e y são números inteiros positivos e se $x < y$, temos que $max\{x,y\} = y$ e $min\{x,y\} = x$, então $max\{x,y\} + min\{x,y\} = x + y$. Usando esse fato, temos:

$$(a,b) \cdot [a,b] = \prod_{i=1}^{\infty} p_i^{min\{a_i,b_i\}} \cdot \prod_{i=1}^{\infty} p_i^{max\{a_i,b_i\}} = \prod_{i=1}^{\infty} p_i^{a_i} \cdot p_i^{b_i} = a \cdot b.$$

■

Proposição 2.54. *Sejam a e b inteiros positivos, tais que $(a,b) = 1$. Então, se d é divisor positivo de ab, existe um único par de divisores positivos d_1 de a e d_2 de b tais que $d = d_1 d_2$. Reciprocamente, se d_1 e d_2 são divisores positivos de a e b, respectivamente, então $d = d_1 d_2$ é um divisor positivo de ab.*

Demonstração: Consideremos as fatorações de a e b dadas por

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \text{ e } b = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}.$$

Como $(a,b) = 1$, os conjuntos $\{p_1, p_2, \ldots, p_n\}$ e $\{q_1, q_2, \ldots, q_m\}$ são disjuntos. Portanto, a fatoração de ab é dada por

$$ab = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}.$$

Se d é um divisor positivo de ab, então

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m},$$

para $0 \leq \alpha_i \leq a_i, i = 1, 2, \ldots, n$ e $0 \leq \beta_j \leq b_j, j = 1, 2, \ldots, m$. Se definirmos

$$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \text{ e } d_2 = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m},$$

teremos $(d_1, d_2) = 1$ e $d_1 d_2 = d$, o que mostra a primeira parte da proposição. Para demonstrar a recíproca, considere d_1 e d_2 divisores positivos de a e b, respectivamente. Logo,

$$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, 0 \leq \alpha_i \leq a_i, i = 1, 2, \ldots, n$$

e

$$d_2 = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}, 0 \leq \beta_j \leq b_j, j = 1, 2, \ldots, m.$$

Tomando

$$d = d_1 d_2 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m},$$

temos que d é um divisor de ab. ■

Seja $b > 1$ inteiro, o Teorema a seguir mostra que podemos escrever qualquer número inteiro positivo n em qualquer base b, ou seja, n pode ser escrito como uma adição de parcelas que são múltiplas de potências de b.

Exemplo 2.55. *Considere os números* 18 *e* 25. *As fatorações desses números são* $18 = 2 \cdot 3^2$ *e* $25 = 5^2$. *Como* $(18, 25) = 1$, *temos que esses números não apresentam números primos em comum em suas fatorações. Portanto, a fatoração de* $18 \cdot 25 = 450$ *é dada por* $450 = 2 \cdot 3^2 \cdot 5^2$. *Se* 15 *é um divisor positivo de* 450, *temos que existe* 3, *tal que* $3 \mid 12$ *e que existe* 5 *tal que* $5 \mid 25$, *de modo que* $3 \cdot 5 = 15$.

Teorema 2.56. *Seja b um inteiro maior do que 1. Então todo inteiro positivo n pode ser representado de maneira única da seguinte forma:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0,$$

onde $k \geq 0$, $a_i \in \mathbb{Z}, i = 0, 1, \ldots, k$, $a_k \neq 0$ *e* $0 \leq a_i < b$.

Demonstração: Para provar a existência, começamos pela divisão de n por b, obtendo o quociente q_0 e o resto a_0. Em seguida, dividimos q_0 por b, obtendo o quociente q_1 e o resto r_1. Repetimos esse processo até obter um quociente $q_k = 0$, como mostra a sequência a seguir:

$$\begin{aligned}
n &= bq_0 + a_0 \\
q_0 &= bq_1 + a_1 \\
q_1 &= bq_2 + a_2 \\
q_2 &= bq_3 + a_3 \\
&\vdots \\
q_{k-2} &= bq_{k-1} + a_{k-1} \\
q_{k-1} &= b \cdot 0 + a_k,
\end{aligned}$$

onde $0 \leq a_j < b, j = 0, 1, 2, \ldots, k$.

Agora, substituímos na primeira equação a expressão para q_0 obtida na segunda equação. Em seguida, substituímos na equação obtida a expressão de q_1 obtida na terceira equação, e assim sucessivamente, obtendo:

$$\begin{aligned} n &= bq_0 + a_0 \\ &= b(bq_1 + a_1) + a_0 \\ &= b^2q_1 + a_1b + a_0 \\ &= b^2(bq_2 + a_2) + a_1b + a_0 \\ &= b^3q_2 + a_2b^2 + a_1b + a_0 \\ &= b^3(bq_3 + a_3) + a_2b^2 + a_1b + a_0 \\ &= b^4q_3 + a_3b^3 + a_2b^2 + a_1b + a_0 \\ &\vdots \\ &= b^kq_{k-1} + a_{k-1}b^{k-1} + \cdots + a_2b^2 + a_1b + a_0 \\ &= a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0. \end{aligned}$$

Agora, nos resta mostrar a unicidade dessa representação. Considere $d_b(n)$ o número de representações de n na base b. Queremos, portanto, mostrar que $d_b(n)$ é sempre igual a 1. Como alguns dos coeficientes a_j podem ser nulos podemos supor, excluindo tais termos, que n possa ser representado na forma

$$n = a_kb^k + a_{k-1}b^{k-1} + \cdots + a_sb^s,$$

onde a_k e a_s são não nulos. Logo

$$\begin{aligned} n - 1 &= a_kb^k + a_{k-1}b^{k-1} + \cdots + a_sb^s - 1 \\ &= a_kb^k + a_{k-1}b^{k-1} + \cdots + (a_s - 1)b^s + b^s - 1. \end{aligned}$$

Como $(b-1)\sum_{j=0}^{s-1} b^j = b^s + b^{s-1} + \cdots + b - b^{s-1} - \cdots - b - 1 = b^s - 1$, podemos escrever:

$$n - 1 = a_kb^k + a_{k-1}b^{k-1} + \cdots + (a_s - 1)b^s + (b-1)\sum_{j=0}^{s-1} b^j,$$

o que nos mostra que é possível encontrar, para cada representação de n na base b, uma representação para $n-1$ na base b. Logo $d_b(n) \leq d_b(n-1)$. Dado $m \in \mathbb{Z}$ com $m \geq n$, ou seja, $n = m - k$ para algum $k \in \mathbb{Z}, k \geq 0$, essa desigualdade nos diz que,

$$d_b(m) \leq d_b(m-1) \leq d_b(m-2) \leq \cdots \leq d_b(m-k) = d_b(n).$$

Logo, como $n > 1$ e $d_b(n) \geq 1$, obtemos $1 \leq d_b(n) \leq d_b(1) = 1$. Esta última série de desigualdades nos garante que $d_b(n) = 1$, o que conclui a demonstração. ∎

Exemplo 2.57. *Vamos escrever o número 470 na base 3. Temos que*

$$\begin{aligned} 470 &= 3 \cdot 156 + 2 \\ 156 &= 3 \cdot 52 + 0 \\ 52 &= 3 \cdot 17 + 1 \\ 17 &= 3 \cdot 5 + 2 \\ 5 &= 3 \cdot 1 + 2 \\ 1 &= 3 \cdot 0 + 1. \end{aligned}$$

Fazendo as substituições, temos:

$$\begin{aligned} 470 &= 3 \cdot 156 + 2 \\ &= 3 \cdot (3 \cdot 52 + 0) + 2 \\ &= 3 \cdot (3 \cdot (3 \cdot 17 + 1) + 0) + 2 \\ &= 3 \cdot (3 \cdot (3 \cdot (3 \cdot 5 + 2) + 1) + 0) + 2 \\ &= 3 \cdot (3 \cdot (3 \cdot (3 \cdot (3 \cdot 1 + 2) + 2) + 1) + 0) + 2 \\ &= 3 \cdot (3 \cdot (3 \cdot (3 \cdot (3 \cdot (3 \cdot 0 + 1) + 2) + 2) + 1) + 0) + 2 \\ &= 1 \cdot 3^5 + 2 \cdot 3^4 + 2 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3^1 + 2 \cdot 3^0. \end{aligned}$$

Definição 2.58. *Denotamos a representação de um número n na base b por $(a_k \cdots a_1 a_0)_b$, onde $a_0, a_1, \ldots, a_k$ são obtidos de acordo com o Teorema 2.56.*

Exemplo 2.59. *A partir do resultado do Exemplo 2.57, podemos escrever* $470 = (122102)_3$.

3

ARITMÉTICA MODULAR E GRUPOS

De posse dos conceitos preliminares apresentados no Capítulo 1, podemos apresentar algumas das definições e propriedades relativas à aritmética modular, como as definições de *congruência*, *congruência linear*, *equações diofantinas* e os importantes *Teoremas de Fermat, Wilson e Euler*. Além disso, ao final deste capítulo, apresentamos as definições de *grupos* e *subgrupos* e algumas propriedades, pois tais conceitos aparecem no *algoritmo criptográfico ElGamal*, apresentado no Capítulo 4.

As principais referências utilizadas neste capítulo foram [6], [7], [9] e [11].

3.1 CONGRUÊNCIA

Definição 3.1. *Dado um número inteiro m maior do que 1, dizemos que dois números inteiros a e b são congruentes módulo m se a e b possuírem mesmo resto quando divididos por m e simbolizaremos por:*

$$a \equiv b \,(mod\, m).$$

Quando a e b não forem congruentes módulo m, ou seja, forem incongruentes módulo m, simbolizaremos por:

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

Exemplo 3.2. *Seja $m = 6$. Temos que a divisão de 10 por 6 resulta em um resto 4, pois $10 = 1 \cdot 6 + 4$. Além disso, a divisão de 16 por 6 resulta em resto 4, pois $16 = 2 \cdot 6 + 4$. Então, 10 e 16 são congruentes módulo 6, ou seja, $10 \equiv 16 \,(mod\, 6)$. Já $15 \not\equiv 10 \,(mod\, 6)$, pois $15 = 2 \cdot 6 + 3$.*

No que segue, consideraremos m um número inteiro maior do que 1, a menos que se diga o contrário.

Para mostrar que $a \equiv b \,(mod\, m)$, basta mostrar que m divide $a - b$, como provamos na Proposição 3.3.

Proposição 3.3. *Sejam a e b dois números inteiros. Temos que $a \equiv b \,(mod\, m)$ se, e somente se, m divide $a - b$.*

Demonstração: De fato, pelo Algoritmo Euclidiano da Divisão, podemos escrever

$$a = mq_1 + r_1 \text{ e } b = mq_2 + r_2,$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor $r_2 \leq r_1$ (caso contrário, basta considerar $b - a$ ao invés de $a - b$ na equação a seguir). Assim, temos

$$a - b = m(q_1 - q_2) + r_1 - r_2.$$

Note que se $r_1 = r_2$, temos que $a - b$ é um múltiplo de m, ou seja, $m \mid a - b$. Do mesmo modo, se $a - b$ é múltiplo de m, isto é, $a - b = km$ para algum $k \in \mathbb{Z}$, então $km = m(q_1 - q_2) + r_1 - r_2$. Logo $m(k - q_1 + q_2) = r_1 - r_2$. Como $m > r_1 - r_2 \geq 0$, temos que $r_1 = r_2$. ■

Exemplo 3.4. *Vamos verificar se 15 é congruente a 39 módulo 8. Pela Proposição 3.3, isso ocorre se, e somente se,* $8 \mid (39 - 15)$. *Como* $39 - 15 = 24$ *e* $8 \mid 24$, *podemos afirmar que* $15 \equiv 39 \,(mod\, 8)$. *De fato,* $15 = 1 \cdot 8 + 7$ *e* $39 = 4 \cdot 8 + 7$.

Apresentaremos a seguir algumas propriedades dessa relação de congruência.

Proposição 3.5. *Se* a *e* b *são inteiros, temos que* $a \equiv b \,(mod\, m)$ *se, e somente se, existir um inteiro* k *tal que* $a = b + km$.

Demonstração: Se $a \equiv b \,(mod\, m)$, então $m \mid (a - b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. Por outro lado, se existe k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, $m \mid (a - b)$ isto é, $a \equiv b \,(mod\, m)$. ■

Proposição 3.6. *Para todo* a, b *e* c *inteiros, temos que:*

(i) $a \equiv a \,(mod\, m)$ *(propriedade reflexiva).*

(ii) se $a \equiv b \,(mod\, m)$, *então* $b \equiv a \,(mod\, m)$ *(propriedade simétrica).*

(iii) se $a \equiv b \,(mod\, m)$ *e* $b \equiv c \,(mod\, m)$, *então* $a \equiv c \,(mod\, m)$ *(propriedade transitiva).*

Demonstração:

(i) Como $m \mid 0$, então $m \mid (a - a)$, o que implica $a \equiv a \,(mod\, m)$.

(ii) Se $a \equiv b \,(mod\, m)$, então $a = b + km$ para algum inteiro k. Logo $b = a + (-km)$, o que implica, pela Proposição 3.5, $b \equiv a \,(mod\, m)$.

(iii) Se $a \equiv b \,(mod\, m)$ e $b \equiv c \,(mod\, m)$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - c = k_2 m$. Somando, membro a membro, estas últimas equações, obtemos $a - c = (k_1 + k_2)m$, de onde, $a = c + (k_1 + k_2)m$ o que implica pela Proposição 3.5 que $a \equiv c \,(mod\, m)$. ■

Proposição 3.7. *Se* a, b, c *e* m *são inteiros tais que* $a \equiv b \,(mod\, m)$, *então:*

(i) $a + c \equiv b + c \,(mod\, m)$.

(ii) $a - c \equiv b - c \,(mod\, m)$.

(iii) $ac \equiv bc \,(mod\, m)$.

Demonstração: Como $a \equiv b \,(mod\, m)$, temos que $a - b = km$, para algum $k \in \mathbb{Z}$.

(i) Como $a-b=(a+c)-(b+c)$, temos $a+c \equiv b+c\,(mod\, m)$.

(ii) Como $(a-c)-(b-c)=a-b=km$, temos que $a-c \equiv b-c\,(mod\, m)$.

(iii) Como $a-b=km$ então $ac-bc=ckm$ o que implica $m \mid (ac-bc)$ e, portanto, $ac \equiv bc\,(mod\, m)$. ■

Proposição 3.8. *Se a, b, c, d e m são inteiros tais que $a \equiv b\,(mod\, m)$ e $c \equiv d\,(mod\, m)$, então:*

(i) $a+c \equiv b+d\,(mod\, m)$.

(ii) $a-c \equiv b-d\,(mod\, m)$.

(iii) $ac \equiv bd\,(mod\, m)$.

Demonstração: Como $a \equiv b\,(mod\, m)$ e $c \equiv d\,(mod\, m)$, temos que existem $k, k_1 \in \mathbb{Z}$ tais que $a-b=km$ e $c-d=k_1m$.

(i) Somando-se membro a membro as igualdades anteriores, obtemos $(a+c)-(b+d)=(k+k_1)m$ e isto implica $a+c \equiv b+d\,(mod\, m)$.

(ii) Basta subtrair membro a membro $a-b=km$ e $c-a=k_1m$, obtendo $(a-c)-(b-d)=(k-k_1)m$ o que implica $a-c \equiv b-d\,(mod\, m)$.

(iii) Multiplicamos ambos os lados de $a-b=km$ por c e ambos os lados de $c-d=k_1m$ por b, obtendo $ac-bc=ckm$ e $bc-bd=bk_1m$. Basta, agora, somarmos membro a membro estas últimas igualdades obtendo $ac-bc+bc-bd=ac-bd=(ck+ck_1)m$, o que implica $ac \equiv bd\,(mod\, m)$. ■

Proposição 3.9. *Se a, b, c e m são inteiros e $ac \equiv bc\,(mod\, m)$, então $a \equiv b\,(mod\, \frac{m}{d})$, onde $d=(c,m)$.*

Demonstração: De $ac \equiv bc\,(mod\, m)$, temos que existe $k \in \mathbb{Z}$ tal que $ac-bc=c(a-b)=km$. Se dividirmos os dois membros por d, teremos $\left(\frac{c}{d}\right)(a-b)=k\left(\frac{m}{d}\right)$. Logo $\left(\frac{m}{d}\right) \mid \left(\frac{c}{d}\right)(a-b)$ e, como $\left(\frac{m}{d}, \frac{c}{d}\right)=1$, Corolário 2.29, então $\left(\frac{m}{d}\right) \mid (a-b)$, o que implica $a \equiv b\,\left(mod\, \frac{m}{d}\right)$. ■

Proposição 3.10. *Se a, b, k e m são inteiros com $k>0$ e $a \equiv b\,(mod\, m)$, então $a^k \equiv b^k\,(mod\, m)$.*

Demonstração: A partir da igualdade:

$$a^k-b^k=(a-b)(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\ldots+ab^{k-2}+b^{k-1})$$

e do fato de $a \equiv b\,(mod\, m)$, podemos concluir que:

$$a^k-b^k=mk(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\ldots+ab^{k-2}+b^{k-1}), \text{ para algum } k \in \mathbb{Z}.$$

Logo, $a^k \equiv b^k \,(mod\, m)$. ∎

Proposição 3.11. *Se* $a \equiv b \,(mod\, m_1)$, $a \equiv b \,(mod\, m_2)$, ..., $a \equiv b \,(mod\, m_k)$ *onde* a, b, $m_1, m_2, \ldots, m_k$ *são inteiros e* $m_i > 0$, $i = 1, 2, \ldots, k$, *então:*

$$a \equiv b \,(mod\, [m_1, m_2, \ldots, m_k])$$

onde $[m_1, m_2, \ldots, m_k]$ *é o mínimo múltiplo comum de* $m_1, m_2, \ldots, m_k$.

Demonstração: Seja p_n o maior primo que aparece nas fatorações de $m_1, m_2, \ldots, m_k$. Cada $m_i, i = 1, 2, \ldots, k$ pode, então, ser expresso como

$$m_i = p_1^{\alpha_{1i}} p_2^{\alpha_{2i}} \cdots p_n^{\alpha_{ni}},$$

onde $\alpha_{ji} \geq 0$ para $j = 1, \ldots, n$ e $i = 1, \ldots, k$.

Como $m_i \mid (a-b), i = 1, 2, \ldots, k$ temos que $p_j^{\alpha_{ji}} \mid (a-b), i = 1, 2, \ldots, k, j = 1, 2, \ldots, n$. Logo, se tomarmos $\alpha_j = \max\limits_{1 \leq i < k} \{\alpha_{ji}\}$ teremos que

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \mid (a-b)$$

mas

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = [m_1, m_2, \ldots, m_k],$$

o que implica $a \equiv b \,(mod\, [m_1, m_2, \ldots m_k])$. ∎

Exemplo 3.12. *Como* $16 \equiv 4 \,(mod\, 2)$, $16 \equiv 4 \,(mod\, 3)$ *e* $16 \equiv 4 \,(mod\, 4)$, *temos, pela Proposição 3.11 que* $16 \equiv 4 \,(mod\, [2, 3, 4])$, *ou seja,* $16 \equiv 4 \,(mod\, 12)$. *De fato,* $12 \mid (16 - 4)$.

Como vimos, dois números inteiros a e b são congruentes módulo um inteiro m se apresentam os mesmos restos na divisão por m. Apresentaremos, agora as definições de *resíduo* e *sistema completo de resíduos.*

Definição 3.13. *Se* h *e* k *são dois inteiros com* $h \equiv k \,(mod\, m)$, *dizemos que* h *é um resíduo de* k *módulo* m.

Definição 3.14. *O conjunto de inteiros* $\{r_1, \cdots, r_s\}$ *é chamado um sistema completo de resíduos módulo* m *se:*

(i) $r_i \not\equiv r_j \,(mod\, m)$ *para* $i \neq j$;

(ii) para todo inteiro n *existe um* r_i *tal que* $n \equiv r_i \,(mod\, m)$.

Exemplo 3.15. *O conjunto {0,1,2,3,4} é um sistema completo de resíduos módulo 5, pois apresenta todos os possíveis restos de uma divisão por 5.*

Proposição 3.16. *Se* k *inteiros* $r_1, r_2, \ldots, r_k$ *formam um sistema completo de resíduos módulo* m, *então* $k = m$.

Demonstração: Primeiramente demonstramos que os inteiros $t_0, t_1, \ldots, t_{m-1}$, com $t_i = i$ formam, de fato, um sistema completo de resíduos módulo m. Pelo Teorema 2.21 sabemos que, para cada n, existe um único par de inteiros q e s, tal que $n = mq + s$, $0 \leq s < m$. Logo $n \equiv s \,(mod\, m)$, sendo s um dos t_i. Como $|t_i - t_j| \leq m-1$, temos que $t_i \not\equiv t_j \,(mod\, m)$ para $i \neq j$. Portanto, o conjunto $t_0, t_1, \ldots t_m - 1$ é um sistema completo de resíduos módulo m. Disto concluímos que cada r_i é congruente a exatamente um dos t_i, o que nos garante $k \leq m$. Como o conjunto $r_1, r_2, \ldots, r_k$ forma, por hipótese, um sistema completo de resíduos módulo m, cada t_i é congruente a exatamente um dos r_i e portanto $m \leq k$. Desta forma $k = m$. ∎

Observação 3.17. *O conjunto* $\{0, 1, ..., m-1\}$ *é um sistema completo de resíduos módulo* m.

Proposição 3.18. *Se* $r_1, r_2, \ldots, r_m$ *é um sistema completo de resíduos módulo* m *e* a *e* b *são inteiros com* $(a, m) = 1$, *então*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

também é um sistema completo de resíduos módulo m.

Demonstração: Considerando-se o resultado do teorema anterior, será suficiente mostrar que quaisquer dois inteiros do conjunto $ar_1 + b, ar_2 + b, \ldots, ar_m + b$, são incongruentes módulo m. Para isso vamos supor que $ar_i + b \equiv ar_j + b \,(mod\, m)$. Logo, pela Proposição 3.7, temos $ar_i \equiv ar_j \,(mod\, m)$. Mas, como $(a, m) = 1$, a Proposição 3.9 nos diz que $r_i \equiv r_j \,(mod\, m)$. O fato de $r_i \equiv r_j \,(mod\, m)$ implica $i = j$, uma vez que, $r_1, r_2, \ldots, r_m$ formam um sistema completo de resíduos módulo m, o que completa a demonstração. ∎

3.2 CONGRUÊNCIA LINEAR

Nesta seção, apresentaremos a definição de *congruência linear* e investigaremos em quais condições esse tipo de congruência possui solução.

Definição 3.19. *Uma congruência linear em uma variável é uma congruência da forma* $ax \equiv b \,(mod\, m)$ *onde* x *é uma incógnita.*

Exemplo 3.20. *Dada a congruência* $3x \equiv 2 \,(mod\, 8)$, *temos que as suas soluções são os valores de* x *tais que* $8 \mid (3x - 2)$. *Note que* $x = 6$ *e* $x = 14$ *são exemplos de soluções para essa congruência linear.*

Observação 3.21. *Note que se* x_0 *é solução para uma congruência do tipo* $ax \equiv b \,(mod\, m)$ *e* $x_1 \equiv x_0 \,(mod\, m)$, *então* x_1 *também é solução para* $ax \equiv b \,(mod\, m)$. *De fato, se* $x_1 \equiv x_0 \,(mod\, m)$, *temos que* $ax_1 \equiv ax_0 \equiv b \,(mod\, m)$.

Acabamos de mostrar que, caso exista uma solução x_0 para uma dada congruência linear, todos os inteiros congruentes a x_0 módulo m também serão solução dessa congruência linear.

Vamos, então, investigar quando uma congruência linear possui solução e, caso possua solução, quantas são as soluções incongruentes dessa congruência linear. Para tanto, vamos antes definir *equação diofantina* e provar os teoremas a respeito das soluções desse tipo de equação.

Definição 3.22. *Denomina-se equação diofantina a toda equação da forma $ax + by = c$, em que a, b e c são números inteiros, e a e b não são ambos nulos e x e y assumem valores inteiros.*

Resolver uma equação desse tipo, é encontrar um par de inteiros x e y, de modo que a igualdade $ax + by = c$ seja satisfeita. O nome "diofantina" remete a Diophanto de Alexandria, que foi o primeiro a buscar soluções para esse tipo de equação.

Observação 3.23. *Algumas equações diofantinas não apresentam solução como, por exemplo, a equação $2x + 8y = 11$. Nesta equação, para qualquer par de inteiros x e y temos que o primeiro membro resultará sempre em um número par, enquanto o segundo membro apresenta um número ímpar, o que nos mostra que não existe uma solução inteira que satisfaça a igualdade.*

No teorema a seguir, vamos verificar uma condição para a existência de soluções para esse tipo de equação.

Teorema 3.24. *Sejam a, b e c inteiros e $d = (a, b)$. A equação diofantina $ax + by = c$ tem soluções se, e somente se, $d \mid c$.*

Demonstração: Se $d \nmid c$, então a equação $ax + by = c$ não possui solução, pois $d \mid a$ e $d \mid b$. Então, vamos supor que $d \mid c$. Pelo Teorema 2.24, temos que existem $m, n \in \mathbb{Z}$, tais que $d = ma + nb$. Como $d \mid c$, existe $k \in \mathbb{Z}$ tal que $c = kd$. Assim, podemos escrever $c = kd = kma + knb$, o que nos mostra que o par $x = km$ e $y = kn$ é uma solução para a equação $ax + by = c$. ■

Exemplo 3.25. *Dada a equação diofantina $15x + 18y = 36$. Note que $(15, 18) = 3$ e $3 \mid 36$. Portanto, essa equação possui solução. De fato, uma solução desta equação é $x = 0$ e $y = 2$.*

Agora, vamos investigar quantas são as soluções para esse tipo de equação.

Teorema 3.26. *Sejam a, b e c inteiros e $d = (a, b)$, tal que $d \mid c$.*

(i) Escrevendo d na forma $d = ma + nb$, com $m, n \in \mathbb{Z}$, temos que o par (x_0, y_0), no qual $x_0 = m \cdot \frac{c}{d}$ e $y_0 = n \cdot \frac{c}{d}$ é uma solução da equação

$$ax + by = c.$$

(ii) Se (x_0, y_0) é uma solução particular de $ax + by = c$, então todas as outras soluções são da forma (x, y), na qual:

$$x = x_0 + \frac{b}{d} \cdot t \text{ e } y = y_0 - \frac{a}{d} \cdot t, \text{ com } t \in \mathbb{Z}.$$

Demonstração:

(i) Vamos verificar que $(x_o = m \cdot \frac{c}{d}, y_0 = n \cdot \frac{c}{d})$ é solução. De fato $a\left(m \cdot \frac{c}{d}\right) + b\left(n \cdot \frac{c}{d}\right) = (am + bn)\frac{c}{d} = d \cdot \frac{c}{d} = c$.

(ii) Vamos verificar que se (x_0, y_0) é uma solução particular, os pares da forma (x, y) com

$$x = x_0 + \frac{b}{d} \cdot t \text{ e}$$
$$y = y_0 - \frac{a}{d} \cdot t$$

são soluções. Temos que:

$$ax + by = a\left(x_0 + \left(\frac{b}{d}\right)t\right) + b\left(y_0 - \left(\frac{a}{d}\right)t\right) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = ax_0 + by_0 = c.$$

Falta mostrar que toda solução (x, t) da equação $ax + by = c$ é da forma $x = x_0 + \left(\frac{b}{d}\right)t$, $y = y_0 - \left(\frac{a}{d}\right)t$, para algum $t \in \mathbb{Z}$. Suponha que (x, y) seja uma solução para a equação, então $ax + by = c$. Mas, como $ax_0 + by_0 = c$, temos:

$$ax + by - (ax_0 + by_0) = ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0.$$

De onde, temos que $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$, segue, pela Proposição 2.28, que

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Dividindo-se os membros da última igualdade por d, temos:

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Portanto, pelo Teorema 2.33, $\left(\frac{b}{d}\right) \mid (x - x_0)$. E, portanto, existe um inteiro t satisfazendo $x - x_0 = t\left(\frac{b}{d}\right)$, ou seja, $x = x_0 + \left(\frac{b}{d}\right)t$. Substituindo-se este valor de x na equação acima, obtemos $y = y_0 - \left(\frac{a}{d}\right)t$. ■

Observação 3.27. *A partir do Teorema 3.26, temos que toda solução (x, y) de uma equação do tipo $ax + by = c$ pode ser escrita como:*

$$(x, y) = \left(m \cdot \frac{c}{d} + \frac{b}{d}t, n \cdot \frac{c}{d} - \frac{a}{d}t\right), \text{ com } t \in \mathbb{Z},$$

onde d, m e n podem ser obtidos a partir da relação $d = ma + nb$.

Utilizando os teoremas referentes às equações diofantinas, podemos avaliar quando uma congruência linear $ax \equiv b\,(mod\, m)$ possui solução e, caso possua, quantas são as soluções incongruentes, como veremos a seguir.

Teorema 3.28. *Sejam a, b e m inteiros e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b\,(mod\, m)$ não possui nenhuma solução e quando $d \mid b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração: Pela Proposição 3.5, x inteiro é solução de $ax \equiv b\,(mod\, m)$ se, e somente se, existe um inteiro y tal que $ax = b + my$, ou seja, $ax - my = b$. Pelo Teorema 3.26, sabemos que se d não divide b, esta equação não possui solução, e se $d \mid b$, ela possui infinitas soluções dadas por

$$x = x_0 - \left(\frac{m}{d}\right) k \text{ e } y = y_0 - \left(\frac{a}{d}\right) k,$$

onde (x_0, y_0) é uma solução particular de $ax - my = b$.

Para determinar as soluções incongruentes, vamos tentar descobrir as condições para que $x_1 = x_0 - \left(\frac{m}{d}\right) k_1$ e $x_2 = x_0 - \left(\frac{m}{d}\right) k_2$ sejam congruentes módulo m. Se x_1 e x_2 são congruentes então

$$x_0 - \left(\frac{m}{d}\right) k_1 \equiv x_0 - \left(\frac{m}{d}\right) k_2\,(mod\, m).$$

Isto implica

$$\left(\frac{m}{d}\right) k_1 \equiv \left(\frac{m}{d}\right) k_2\,(mod\, m),$$

e como $\left(\frac{m}{d}\right) \mid m$, temos $\left(\frac{m}{d}, m\right) = \frac{m}{d}$. Assim, pela Proposição 3.9, temos $k_1 \equiv k_2\,(mod\, d)$.

Observe que m foi substituído por $d = \frac{m}{\frac{m}{d}}$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - \left(\frac{m}{d}\right) k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. ∎

Definição 3.29. *Dizemos que uma solução x_0 de $ax \equiv b\,(mod\, m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.*

Corolário 3.30. *A congruência linear $ax \equiv 1\,(mod\, m)$ tem solução se, e somente se, $(a, m) = 1$. E quando $(a, m) = 1$, a solução é única.*

Demonstração: Segue direto do Teorema 3.28. ∎

Definição 3.31. *Uma solução a_0 de $ax \equiv 1\,(mod\, m)$ é chamada de um inverso de a módulo m.*

Proposição 3.32. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1\,(mod\, p)$ ou $a \equiv -1\,(mod\, p)$.*

Demonstração: Se a é o seu próprio inverso, então $a^2 \equiv 1\,(mod\, p)$, de onde, $p \mid (a^2 - 1)$. Mas se $p \mid (a-1)(a+1)$, sendo p primo, $p \mid (a-1)$ ou $p \mid (a+1)$, o que implica $a \equiv 1\,(mod\, p)$ ou $a \equiv -1\,(mod\, p)$.

Reciprocamente, se $a \equiv 1\,(mod\, p)$ ou $a \equiv -1\,(mod\, p)$, temos que $p \mid (a-1)(a+1)$, o que significa que $p \mid (a^2 - 1)$, ou seja, $a^2 \equiv 1\,(mod\, p)$. ∎

Exemplo 3.33. *Considere $p = 7$ e $a = 6$. Temos que $a \equiv -1\,(mod\, 7)$ e $6^2 = 36 \equiv 1\,(mod\, 7)$.*

3.3 PEQUENO TEOREMA DE FERMAT E TEOREMA DE WILSON

Nesta seção, apresentaremos dois importantes resultados envolvendo números primos, conhecidos como Teorema de Wilson e Pequeno Teorema de Fermat.

Teorema 3.34. *(Teorema de Wilson) Se p é primo, então $(p-1)! \equiv -1\,(mod\,p)$.*

Demonstração: Como $(2-1)! = 1$ e $1 \equiv -1\,(mod\,2)$, pois $2 \mid (1-(-1))$, o resultado é válido para $p = 2$.

Pelo Corolário 3.30, a congruência $ax \equiv 1\,(mod\,p)$ apresenta uma única solução para todo $a \in \{1, 2, 3, \ldots, p-1\}$. No conjunto $\{1, 2, 3, \ldots, p-1\}$ somente 1 e $p-1$ são seus próprios inversos módulo p. Então, podemos agrupar os números $2, 3, 4, \ldots, p-2$ em pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos,

$$2 \cdot 3 \cdot 4 \cdot 5 \cdots (p-2) \equiv 1\,(mod\,p).$$

Multiplicando-se ambos os lados desta congruência por $p-1$ teremos

$$2 \cdot 3 \cdot 4 \cdots (p-2)(p-1) \equiv (p-1)\,(mod\,p),$$

isto é, $(p-1)! \equiv p-1\,(mod\,p)$, ou seja, $(p-1)! \equiv -1\,(mod\,p)$. ∎

Exemplo 3.35. *Tomemos $p = 5$, então, pelo Teorema 3.34, $4! \equiv -1\,(mod\,5)$. De fato, $4! = 24$ e $24 \equiv -1\,(mod\,5)$, pois $5 \mid (24-(-1))$.*

O teorema que segue nos mostra que, quando um número satisfaz a relação do Teorema de Wilson, esse número é primo.

Teorema 3.36. *Se n é um inteiro tal que $(n-1)! \equiv -1\,(mod\,n)$, então n é primo.*

Demonstração: Suponhamos que $(n-1)! \equiv -1\,(mod\,n)$, isto é, $n \mid ((n-1)!+1)$ e que n não seja primo, ou seja, $n = rs$, $1 < r < n$ e $1 < s < n$. Note que $r \mid (n-1)!$, pois $r < n$ e $(n-1)!$ é o produto de todos os inteiros positivos menores do que n. Além disso, como $r \mid n$, temos que $r \mid ((n-1)!+1)$. Portanto, $r \mid ((n-1)!+1-(n-1)!) = 1$, porém $r > 1$, o que é uma contradição. Assim, podemos concluir que n é um número primo. ∎

Teorema 3.37. *(Pequeno Teorema de Fermat) Seja p primo. Se p não divide a, então $a^{p-1} \equiv 1\,(mod\,p)$.*

Demonstração: Vimos que o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ constitui um sistema completo de resíduos módulo p (Observação 3.17). Pela Proposição 3.18, como $(a, p) = 1$ e considerando $b = 0$, temos que o conjunto $\{0, a, 2a, 3a, \ldots, (p-1)a\}$ é também um sistema completo de resíduos módulo p. Tomando o conjunto $\{a, 2a, 3a, \ldots, (p-1)a\}$ temos que nenhum destes números $ia, 1 \leq i \leq p-1$ é congruente

a zero módulo p. Temos, portanto, um conjunto de $p-1$ elementos dois a dois incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um elemento do conjunto $\{1, 2, 3, \ldots, p-1\}$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a)\cdots(p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \,(mod\, p)$$

ou seja, $a^{p-1}(p-1)! \equiv (p-1)! \,(mod\, p)$. Mas, como $((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

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

o que conclui a demonstração. ■

Exemplo 3.38. *Tomemos $p = 3$ e $a = 4$. Então, pelo Pequeno Teorema de Fermat, $4^{3-1} \equiv 1 \,(mod\, 3)$. De fato, $4^2 = 16$ e $16 = 5 \cdot 3 + 1$, o que implica que $16 \equiv 1 \,(mod\, 3)$.*

Corolário 3.39. *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \,(mod\, p)$.*

Demonstração: Se $p \mid a$, então $p \mid (a(a^{p-1} - 1))$ e, portanto, $a^p \equiv a \,(mod\, p)$. Se $p \nmid a$, pelo Teorema 3.37 $p \mid (a^{p-1} - 1)$ e, portanto, $p \mid (a^p - a)$. Logo, em ambos os casos, $a^p \equiv a \,(mod\, p)$. ■

3.4 FUNÇÃO ϕ DE EULER E TEOREMA DE EULER

Apresentaremos nesta seção a *função aritmética* conhecida como *função ϕ de Euler* e um importante resultado que envolve essa função, conhecido como *Teorema de Euler*.

Definição 3.40. *Se n é um inteiro positivo, a função ϕ de Euler, denotada por $\phi(n)$, é definida como o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.*

Exemplo 3.41. *Considerando $n = 12$, então os números inteiros positivos menores do que ou iguais a 12 que são relativamente primos com 12 são: 1, 5, 7 e 11. Então, $\phi(12) = 4$.*

As proposições a seguir apresentam duas propriedades da função ϕ de Euler.

Proposição 3.42. *Para p primo e a um inteiro positivo temos*

$$\phi(p^a) = p^a - p^{a-1}$$

Demonstração: Por definição, sabemos que $\phi(p^a)$ é o número de inteiros positivos não-superiores a p^a e relativamente primos com p^a.

Os números não relativamente primos com p^a e menores do que ou iguais a p^a são os múltiplos de p menores ou iguais a p^a. Note que esses múltiplos são $\{p \cdot 1, p \cdot 2, \ldots, p \cdot p^{a-1}\}$, ou seja, a quantidade de múltiplos de p menores ou iguais a p^a corresponde a p^{a-1}. Assim, $\phi(p) = p^a - p^{a-1}$. ■

Exemplo 3.43. *Temos que* $\phi(27) = \phi(3^3)$. *No conjunto* $\{1, 2, 3, \ldots, 27\}$, *os números que não são relativamente primos com* 27 *são os múltiplos de* 3 *menores ou iguais a* 27, *ou seja,* $\{3, 6, 9, 12, 15, 18, 21, 24, 27\}$. *Note que temos* 9 *múltiplos de* 3 *menores ou iguais a* 27, *quantidade que corresponde a* 3^2. *Assim,* $\phi(3^3) = 3^3 - 3^{3-1} = 27 - 9 = 18$.

Proposição 3.44. *Para qualquer inteiro positivo* n *temos* $\sum_{d|n} \phi(d) = n$.

Demonstração: Considere o conjunto $A = \{1, 2, 3, \ldots, n\}$. Podemos separar A em subconjuntos A_d para cada divisor positivo d de n da seguinte forma:

$$A_d = \{m \in A\,;\, (m, n) = d\}.$$

Note que os subconjuntos A_d são dois a dois disjuntos e que $\bigcup_{d|n} A_d = A$. Seja $m \in A_d$. Pelo Corolário 2.29, temos:

$$(m, n) = d \Leftrightarrow \left(\tfrac{m}{d}, \tfrac{n}{d}\right) = 1.$$

Então, $m \in A_d$ se, e somente se, $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Como $m \leq n$, temos que $\frac{m}{d} \leq \frac{n}{d}$. Portanto, A_d possui $\phi\left(\frac{n}{d}\right)$ elementos.

Como os subconjuntos A_d são disjuntos e a união desses subconjuntos resulta no conjunto A, temos:

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = n.$$

Como para cada divisor d de n, temos que $\frac{n}{d}$ também é divisor de n, pois $n = \frac{n}{d} \cdot d$, temos que, $\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$, ou seja, $\sum_{d|n} \phi(d) = n$. ∎

Exemplo 3.45. *Seja* $n = 24$. *Os divisores positivos de* n *são* $1, 2, 3, 4, 6, 8, 12$ *e* 24. *Temos que,*

$$\begin{aligned}
A_1 &= \{1, 5, 7, 11, 13, 17, 19, 23\} \\
A_2 &= \{2, 10, 14, 22\} \\
A_3 &= \{3, 9, 15, 21\} \\
A_4 &= \{4, 20\} \\
A_6 &= \{6, 18\} \\
A_8 &= \{8, 16\} \\
A_{12} &= \{12\} \\
A_{24} &= \{24\}.
\end{aligned}$$

Então, denotando por $\#A_i$ *a cardinalidade (número de elementos) do subconjunto* A_i, *temos:*

$$\begin{aligned}
\#A_1 &= \phi\left(\frac{24}{1}\right) = \phi(24) = 8\\
\#A_2 &= \phi\left(\frac{24}{2}\right) = \phi(12) = 4\\
\#A_3 &= \phi\left(\frac{24}{3}\right) = \phi(8) = 4\\
\#A_4 &= \phi\left(\frac{24}{4}\right) = \phi(6) = 2\\
\#A_6 &= \phi\left(\frac{24}{6}\right) = \phi(4) = 2\\
\#A_8 &= \phi\left(\frac{24}{8}\right) = \phi(3) = 2\\
\#A_{12} &= \phi\left(\frac{24}{12}\right) = \phi(2) = 1\\
\#A_{24} &= \phi\left(\frac{24}{24}\right) = \phi(1) = 1.
\end{aligned}$$

Note que $\left\{\frac{n}{d}\,;\, d \mid n\right\} = \left\{\frac{24}{1}, \frac{24}{2}, \frac{24}{3}, \frac{24}{4}, \frac{24}{6}, \frac{24}{8}, \frac{24}{12}, \frac{24}{24}\right\} = \{24, 12, 8, 6, 4, 3, 2, 1\} = \{d\,;\, d \mid n\}$. *Além disso,* $\sum_{d|n} \phi(d) = 8 + 4 + 4 + 2 + 2 + 2 + 1 + 1 = 24 = n$.

Definição 3.46. *Um sistema reduzido de resíduos módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \pmod m$.*

Exemplo 3.47. *O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ é um sistema completo de resíduos módulo 10 e $\{1, 3, 7, 9\}$ é um sistema reduzido de resíduos módulo 10.*

Note que, para obter o sistema reduzido de resíduos módulo m, basta excluir de um sistema completo de resíduos módulo m os elementos que não são relativamente primos com m.

Observação 3.48. *Para p primo, $\phi(p) = p - 1$. Considerando o sistema completo de resíduos $\{0, 1, 2, \ldots, p-1\}$, o único elemento desse conjunto que não é relativamente primo com p é o 0, então o conjunto $\{1, 2, 3, \ldots, p-1\}$ é um sistema reduzido de resíduos módulo p.*

Proposição 3.49. *Seja a um inteiro positivo tal que $(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \ldots, ar_{\phi(m)}$ é também, um sistema reduzido de resíduos módulo m.*

Demonstração: Como $(a, m) = 1$ e $(r_i, m) = 1$, temos $(ar_i, m) = 1$. De fato, ar_i e m não possuem fatores primos em comum, pois m não possui fatores primos em comum com a, nem com r_i. Logo, $(ar_i, m) = 1$ pela Proposição 2.27. Logo, temos que todos os elementos do conjunto $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ são relativamente primos com m. Portanto, resta mostrar que os elementos desse conjunto são, dois a dois, incongruentes módulo m.

Como $(a, m) = 1$, temos que $ar_i \equiv ar_j \,(mod\, m)$ implica $r_i \equiv r_j \,(mod\, m)$, ou seja, $i = j$, pois o conjunto $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ é um sistema reduzido de resíduos módulo m. Portanto, o conjunto $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ é um sistema reduzido de resíduos módulo m. ■

Teorema 3.50. *(Euler) Se m é um inteiro positivo e a um inteiro com $(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1 \,(mod\, m).$$

Demonstração: Na Proposição 3.49 mostramos que se $(a, m) = 1$ e o conjunto $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ for um sistema reduzido de resíduos módulo m, o conjunto $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ constitui, também, um sistema reduzido de resíduos módulo m. Então, esses conjuntos possuem os mesmos elementos e, portanto, o produto dos ar_i deve ser congruente ao produto dos r_j módulo m, isto é,

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 \cdots r_{\phi(m)} \,(mod\, m)$$

ou seja,

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \,(mod\, m).$$

Se r_i pertence a um sistema reduzido de resíduos módulo m, então $(r_i, m) = 1$. Ou seja, r_i e m não possuem fatores primos em comum. Portanto, $\prod_{i=1}^{\phi(m)} r_i$ não possui fatores primos em comum com m. Ou seja, $\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1$. Então, podemos cancelar $\prod_{i=1}^{\phi(m)} r_i$ em ambos os lados. Assim, $a^{\phi(m)} \equiv 1 \,(mod\, m)$. ■

Exemplo 3.51. *Considere $a = 16$ e $m = 3$. Como $(16, 3) = 1$, temos, pelo Teorema de Euler, que $16^{\phi(3)} \equiv 1 \,(mod\, 3)$. De fato, $\phi(3) = 2$ e $16^2 = 256 \equiv 1 \,(mod\, 3)$.*

Como vimos, para p primo, $\phi(p) = p - 1$. Então, o teorema anterior é uma generalização do Pequeno Teorema de Fermat.

3.5 TEOREMA CHINÊS DOS RESTOS

Neste ponto veremos o Teorema do Resto Chinês, que recebe esse nome pelo fato de seu resultado já ser conhecido na antiguidade, pelos matemáticos chineses.

Teorema 3.52. *(O Teorema Chinês dos Restos) Sejam a_i, m_i, c_i inteiros para $i = 1, \ldots, r$, com $m_i \geq 1$ para todo i. Se $(a_i, m_i) = 1$ e $(m_i, m_j) = 1$ para $i \neq j$, então o sistema*

$$\begin{aligned}
a_1 x &\equiv c_1 \,(mod\, m_1) \\
a_2 x &\equiv c_2 \,(mod\, m_2) \\
a_3 x &\equiv c_3 \,(mod\, m_3) \\
&\vdots \\
a_r x &\equiv c_r \,(mod\, m_r)
\end{aligned}$$

possui solução e a solução é única módulo M, onde $M = m_1 m_2 \cdots m_r$.

Demonstração: Do fato de $(a_i, m_i) = 1$, o Teorema 3.28 nos diz que $a_i x \equiv c_i \,(mod\, m_i)$ possui uma única solução que denotamos por b_i. Se definirmos $y_i = \frac{M}{m_i}$ onde, $M = m_1 m_2 \cdots m_r$, teremos $(y_i, m_i) = 1$, uma vez que $(m_i, m_j) = 1$ para $i \neq j$. Novamente, o Teorema 3.28 nos garante que cada uma das congruências $y_i x \equiv 1 \,(mod\, m_i)$ possui uma única solução que denotamos por y_i^*. Logo, $y_i y_i^* \equiv 1 \,(mod\, m_i)$, $i = 1, 2, \ldots, r$. Afirmamos que o número x dado por

$$x = b_1 y_1 y_1^* + b_2 y_2 y_2^* + \cdots + b_r y_r y_r^*,$$

é uma solução simultânea para o nosso sistema de congruências. De fato,

$$\begin{aligned} a_i x &= a_i b_1 y_1 y_1^* + a_i b_2 y_2 y_2^* + \cdots + a_i b_i y_i y_i^* + \cdots + a_i b_r y_r y_r^* \\ &\equiv a_i b_i y_i y_i^* \equiv a_i b_i \equiv c_i \,(mod\, m_i), \end{aligned}$$

uma vez que y_j é divisível por m_i para $i \neq j$, $y_i y_i^* \equiv 1 \,(mod\, m_i)$ e b_i é solução de $a_i x \equiv c_i \,(mod\, m_i)$. Provamos, a seguir, que esta solução é única módulo M. Se x^* é uma outra solução para o nosso sistema, então $a_i x^* \equiv c_i \equiv a_i x \,(mod\, m_i)$ e, sendo $(a_i, m_i) = 1$ obtemos $x^* \equiv x \,(mod\, m_i)$, $i = 1, 2, \ldots, r$. Mas, como $(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, \ldots, m_r] = m_1 m_2 \cdots m_r.$$

Portanto, pela Proposição 3.11, $x^* \equiv x \,(mod\, M)$, o que conclui a demonstração. ∎

Corolário 3.53. *Uma solução x de um sistema de congruências do tipo:*

$$\begin{aligned} a_1 x &\equiv c_1 \,(mod\, m_1) \\ a_2 x &\equiv c_2 \,(mod\, m_2) \\ a_3 x &\equiv c_3 \,(mod\, m_3) \\ &\vdots \\ a_r x &\equiv c_r \,(mod\, m_r), \end{aligned}$$

pode ser obtida da seguinte forma: $x = y_1^* y_1 a_2^{-1} c_1 + y_2^* y_2 a_2^{-1} c_2 + \cdots + y_r^* y_r a_r^{-1} c_r$, onde $y_i = \frac{M}{m_i}$ e y_i^* é solução de $y_i y_i^* \equiv 1 \,(mod\, m_i)$, $i = 1, \ldots, r$.

Demonstração: Se $x = y_1^* y_1 a_1^{-1} c_1 + y_2^* y_2 a_2^{-1} c_2 + \cdots + y_r^* y_r a_r^{-1} c_r$, então

$$a_1 x = a_1 (y_1^* y_1 a_1^{-1} c_1 + y_2^* y_2 a_2^{-1} c_2 + \cdots + y_r^* y_r a_r^{-1} c_r) \equiv a_1 y_1^* y_1 a_1^{-1} c_1 \,(mod\, m_1),$$

pois $y_2, y_3, \ldots, y_r$ são múltiplos de m_1. Então, $a_1 x \equiv a_1 y_1^* y_1 a_1^{-1} c_1 \equiv a_1 a_1^{-1} y_1^* y_1 c_1 = y_1^* y_1 c_1 \,(mod\, m_1)$. E como $y_1^* y_1 \equiv 1 \,(mod\, m_1)$, podemos concluir que $a_1 x \equiv c_1 \,(mod\, m_1)$. Fazendo o mesmo para as demais congruências, podemos verificar que $a_i x \equiv c_i \,(mod\, m_i)$, para $i = 1, \ldots, r$. ∎

Exemplo 3.54. *Considere o seguinte sistema:*

$$x \equiv 0\,(mod\,7)$$
$$x \equiv 1\,(mod\,12)$$
$$x \equiv 15\,(mod\,17).$$

Pelo Teorema 3.52, esse sistema possui uma única solução módulo $M = 7 \cdot 12 \cdot 17 = 1428$. *Pela Proposição 3.53, podemos obter uma solução desse sistema calculando* $x = y_1^* y_1 a_1^{-1} c_1 + y_2^* y_2 a_2^{-1} c_2 + \cdots + y_r^* y_r a_r^{-1} c_r$, *onde* $y_1 = \frac{M}{m_1}$ *e* y_i^* *é solução de* $y_i y_i^* \equiv 1\,(mod\,m_i)$, $i = 1, \ldots, r$.

Como, $y_1 = 204$, $y_2 = 119$ *e* $y_3 = 84$, *podemos calcular:*

$$204y_1^* \equiv 1\,(mod\,7) \Rightarrow y_1^* = 1$$
$$119y_2^* \equiv 1\,(mod\,12) \Rightarrow y_2^* = 11$$
$$84y_3^* \equiv 1\,(mod\,17) \Rightarrow y_3^* = 16.$$

Note que $a_1 = a_2 = a_3 = 1$, *então* $a_1^{-1} = a_2^{-1} = a_3^{-1} = 1$. *Assim,*

$$x = 1 \cdot 204 \cdot 1 \cdot 0 + 11 \cdot 119 \cdot 1 \cdot 1 + \cdots + 16 \cdot 84 \cdot 1 \cdot 15 = 21469.$$

Pelo Teorema 3.52, $21469 \equiv 49\,(mod\,1428)$ *é a única solução módulo* $M = 1428$.

3.6 TEOREMA DE LAGRANGE

Apresentaremos, agora, o *Teorema de Lagrange*, que trata do número de soluções de uma relação de congruência do tipo $f(x) \equiv 0\,(mod\,p)$, onde $f(x)$ é um polinômio com coeficientes inteiros.

Teorema 3.55. *(Lagrange) Seja* $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0$ *um polinômio com coeficientes inteiros tal que* $(c_n, p) = 1$, *onde* p *é primo. Nestas condições a congruência*

$$f(x) \equiv 0\,(mod\,p),$$

tem no máximo n *soluções incongruentes módulo* p. *É claro que quando* $n > p$ *a congruência acima não tem mais do que* p *soluções distintas módulo* p.

Demonstração: Faremos a demonstração por indução em n, sendo n o grau do polinômio $f(x)$.

Para $n = 1$, temos a congruência linear

$$f(x) = c_1 x + c_0 \equiv 0\,(mod\,p).$$

Por hipótese, $(c_1, p) = 1$. Pelo Teorema 3.28, temos que $c_1 x \equiv -c_0\,(mod\,p)$ tem exatamente uma solução. Com isso temos que a propriedade é válida para $n = 1$.

Suponhamos que a propriedade seja válida para todo polinômio de grau $n-1$. Faremos uma prova por contradição. Suponhamos que a congruência $f(x) \equiv 0\,(mod\,p)$, onde $f(x)$ é um polinômio de grau n, tenha $n+1$ soluções incongruentes módulo p. Sejam $x_0, x_1, x_2, \ldots, x_n$ estas $n+1$ soluções. Como $(x^i - x_0^i)$ é divisível por $x - x_0$ para todo inteiro $i, i = 1, 2, \ldots, n$, temos:

$$\begin{aligned} f(x) - f(x_0) &= c_n(x^n - x_0^n) + c_{n-1}(x^{n-1} - x_0^{n-1}) + \cdots + c_1(x - x_0) \\ &= (x - x_0)h(x), \end{aligned}$$

onde $h(x)$ é um polinômio de grau $n-1$ tendo c_n como coeficiente de x^{n-1}. Como $f(x_k) \equiv f(x_0)\,(mod\,p)$, temos

$$f(x_k) - f(x_0) = (x_k - x_0)h(x_k) \equiv 0\,(mod\,p),$$

ou seja, $p \mid (x_k - x_0)h(x)$. Como p é primo, $p \mid (x_k - x_0)$ ou $p \mid h(x)$. Como $x_k \not\equiv x_0\,(mod\,p)$, para $k \neq 0$, $h(x_k) \equiv 0\,(mod\,p)$. Isso nos mostra que a congruência $h(x) \equiv 0\,(mod\,p)$ possui n soluções incongruentes módulo p, o que é uma contradição, pois $h(x)$ tem grau $n-1$, $(c_n, p) = 1$ e, pela hipótese de indução, todo polinômio nessas condições possui no máximo $n-1$ soluções. Portanto, $f(x)$ não pode ter mais do que n soluções incongruentes módulo p. ■

Exemplo 3.56. *Sejam $p = 13$ e $n = 6$. Seja $f(x) = 2x^6 + x^3 + x + 1$. A congruência $f(x) \equiv 0\,(mod\,13)$ tem como soluções incongruentes módulo 13: 6 e 9.*

Exemplo 3.57. *Sejam $p = 5$ e $n = 4$. Seja $f(x) = 10x^4 + 5x^2 + 5$. A congruência $f(x) \equiv 0\,(mod\,5)$ tem como soluções incongruentes módulo 5: 0, 1, 2, 3, e 4.*

3.7 CLASSES DE CONGRUÊNCIA

Nesta seção, apresentaremos o conceito de *classe de congruência* e algumas de suas propriedades.

Definição 3.58. *Seja a um inteiro. Chama-se classe de congruência de a módulo m o conjunto formado por todos os inteiros que são congruentes a a módulo m. Denotamos esse conjunto por $\overline{a}$, ou seja:*

$$\overline{a} = \{x \in \mathbb{Z}\ ;\ x \equiv a\,(mod\,m)\}.$$

Observação 3.59. *Como vimos, se $x \equiv a\,(mod\,m)$, então $x - a = mk$, para algum $k \in \mathbb{Z}$. Ou seja, podemos escrever $x = a + mk$ e, portanto: $\overline{a} = \{a + mk\ ;\ k \in \mathbb{Z}\}$.*

Exemplo 3.60. *O cojunto $\overline{1} = \{1 + 0 \cdot 2, 1 + 2 \cdot 2, 1 + 3 \cdot 2, \ldots\} = \{1, 3, 5, 7, \ldots\}$ corresponde à classe de congruência de 1 módulo 2. Esse conjunto contém todos os números que apresentam resto 1 na divisão por 2.*

A proposição a seguir demonstra o fato de que dois números inteiros congruentes módulo um inteiro m geram a mesma classe de congruência.

Proposição 3.61. *Sejam a e b inteiros e $a \equiv b\,(mod\,m)$. Então, $\overline{a} = \overline{b}$.*

Demonstração: Dado um inteiro x tal que $x \in \overline{a}$, pela Definição 3.58, temos que $x \equiv a\,(mod\,m)$. Da Proposição 3.6, item (iii), temos que $x \equiv b\,(mod\,m)$. Portanto, $x \in \overline{b}$. De forma análoga, tomando um inteiro y, $y \in \overline{b}$, temos que $y \in \overline{a}$. Assim, podemos afirmar que $\overline{a} \subset \overline{b}$ e $\overline{b} \subset \overline{a}$, de onde $\overline{a} = \overline{b}$. ∎

O corolário a seguir mostra que as diferentes classes de congruência módulo um inteiro m são disjuntas.

Corolário 3.62. *Sejam a e b inteiros. Se $\overline{a} \neq \overline{b}$, então $\overline{a} \cap \overline{b} = \emptyset$.*

Demonstração: Suponha que existe um inteiro c tal que $c \in \overline{a}$ e $c \in \overline{b}$. Então, $c \equiv a\,(mod\,m)$ e $c \equiv b\,(mod\,m)$. Pela Proposição 3.6 (ii) e (iii), temos que $a \equiv b\,(mod\,m)$. O que, pela Proposição 3.61, contradiz a hipótese de que $\overline{a} \neq \overline{b}$. ∎

Observação 3.63. *Cada inteiro a pertencente a uma classe de congruência módulo m será chamado de representante da classe. Note que, dado um sistema completo de resíduos módulo m, temos que cada elemento desse conjunto é um representante de uma classe de congruência distinta módulo m.*

Exemplo 3.64. *O conjunto $\{0, 1, 2, 3, 4\}$ é um sistema completo de resíduos módulo 5. Então o conjunto $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ é o conjunto de todas as classes de congruência distintas módulo 5.*

Definição 3.65. *O conjunto de todas as classes de congruência módulo m pode ser representado por $\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ e denominado por $\mathbb{Z}_m$.*

3.8 GRUPOS E SUBGRUPOS

Nesta seção apresentaremos as definições de grupos e subgrupos que serão necessárias para compreender a ideia do algoritmo criptográfico ElGamal, apresentado no Capítulo 4.

Definição 3.66. *Um conjunto G com uma operação*

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

é um grupo se as condições seguintes são satisfeitas:

(i) A operação é associativa, isto é,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,\ \forall\ a, b, c \in G.$$

(ii) Existe um elemento neutro, isto é,

$$\exists\ e \in G \text{ tal que } e \cdot a = a \cdot e = a,\ \forall\ a \in G.$$

(iii) Todo elemento possui um elemento inverso, isto é,

$$\forall\ a \in G,\ \exists\ b \in G \text{ tal que } a \cdot b = b \cdot a = e.$$

Observação 3.67.

(i) Usamos a notação $(G, \cdot)$ para representar um grupo G com a operação $\cdot$.

(ii) Dado um grupo $(G, \cdot)$, o elemento neutro é único. De fato, se existirem e_1 e $e_2 \in G$ tais que e_1 e e_2 são elementos neutros de G, poderíamos escrever $e_1 = e_1 \cdot e_2 = e_2$, de onde, $e_1 = e_2$.

(iii) Dado um grupo $(G, \cdot)$, o elemento inverso é único. De fato, dado $a \in G$, suponha que existam b_1 e $b_2 \in G$, tais que $a \cdot b_1 = b_1 \cdot a = e$ e $a \cdot b_2 = b_2 \cdot a = e$. Então, podemos escrever $b_1 \cdot a \cdot b_1 = b_1 \cdot a \cdot b_2$, ou seja, $b_1 = b_2$.

(iv) Devido à unicidade do inverso, denotamos o inverso de a por a^{-1}.

Definição 3.68. *Um grupo G é dito abeliano ou comutativo se a sua operação é comutativa, isto é,*

$$a \cdot b = b \cdot a, \forall\ a, b \in G.$$

Exemplo 3.69. *O conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ com a operação*

$$\overline{x} + \overline{y} = \overline{x + y}$$

é um grupo abeliano. De fato, segue da Proposição 3.8 item (i) que a operação está bem definida. Além disso,

(i) para todo $\overline{x}$, $\overline{y}$, $\overline{z} \in \mathbb{Z}_n$, temos:

$$\begin{aligned} \overline{x} + (\overline{y} + \overline{z}) &= \overline{x} + \overline{(y + z)} = \overline{x + (y + z)} \\ &= \overline{(x + y) + z} = \overline{(x + y)} + \overline{z} \\ &= (\overline{x} + \overline{y}) + \overline{z}. \end{aligned}$$

(ii) Para todo $\overline{x}$, $\overline{y} \in \mathbb{Z}_n$,

$$\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}.$$

(iii) Para todo $\overline{x} \in \mathbb{Z}_n$ tal que:

$$\overline{x} + \overline{0} = \overline{x + 0} = \overline{x}.$$

(iv) Para todo $\overline{x} \in \mathbb{Z}_n$ *existe* $\overline{n-x} \in \mathbb{Z}_n$ *tal que:*

$$\overline{x} + \overline{n-x} = \overline{x + (n-x)} = \overline{n} = \overline{0}.$$

Portanto, $(\mathbb{Z}_n, +)$ *é um grupo abeliano.*

Exemplo 3.70. *O conjunto* $\mathbb{Z}_n^* = \{\overline{a}\,;\,(a,n) = 1\}$ *com a operação*

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b},\ \overline{a}, \overline{b} \in \mathbb{Z}_n^*$$

é um grupo abeliano. De fato, segue da Proposição 3.8 item (iii) *que a operação está bem definida. Então,*

(i) dados $\overline{a}, \overline{b}, \overline{c}, \overline{1} \in \mathbb{Z}_n^*$*, temos:* $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot (\overline{b \cdot c}) = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = (\overline{a \cdot b}) \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$*. Logo, a operação é associativa em* $\mathbb{Z}_n^*$*.*

(ii) $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{b} \cdot \overline{a}$*. Logo, a operação é comutativa em* $\mathbb{Z}_n^*$*.*

(iii) $\overline{1} \in \mathbb{Z}_n^*$ *e* $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}$*,* $\forall\, \overline{a} \in \mathbb{Z}_n^*$*. Logo,* $\overline{1}$ *é elemento neutro em* $\mathbb{Z}_n^*$*.*

(iv) Se $\overline{a} \in \mathbb{Z}_n^*$*, então* $(a,n) = 1$*. Pelo Teorema de Bézout, Teorema 2.24, existem* $r, s \in \mathbb{Z}$ *tais que* $ar + ns = 1$*. De onde,* $\overline{ar + ns} = \overline{1}$ *se, e somente se,*

$$\begin{aligned} \overline{ar} + \overline{ns} = \overline{1} &\Leftrightarrow \\ \overline{ar} = \overline{1} &\Leftrightarrow \\ \overline{a} \cdot \overline{r} = \overline{1}. & \end{aligned}$$

É claro que $\overline{r} \in \mathbb{Z}_n^*$*, pois de* $ar + ns = 1$*, segue que* $(r,n) = 1$*.*

Observação 3.71. *Para p primo, o conjunto* $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}$*, com a operação* $\overline{a} \cdot \overline{b} = \overline{a \cdot b},\ \overline{a}, \overline{b} \in \mathbb{Z}_p^*$ *é um grupo abeliano. Esse resultado se dá pelo fato de o conjunto* $\mathbb{Z}_p^* = \{\overline{a}\,;\,(a,p) = 1\}$ *da proposição anterior ser igual ao conjunto* $\{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}$ *quando p é primo.*

Exemplo 3.72. *Considere o conjunto* $\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \ldots, \overline{6}\}$ *e a operação*

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b},\ \overline{a}, \overline{b} \in \mathbb{Z}_7^*.$$

A Tabela 1 apresenta todos os resultados da operação $\cdot$ *entre os elementos de* $\mathbb{Z}_7^*$*:*

Note que, pelos resultados da tabela, dados $\overline{a}, \overline{b} \in \mathbb{Z}_7^*$*,* $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$*, pois a tabela é simétrica. Podemos, também, verificar que o elemento* $\overline{1}$ *de fato é o elemento neutro de* $\mathbb{Z}_7^*$*, pois* $\overline{1} \cdot \overline{a} = \overline{a}$ *para todo* $\overline{a} \in \mathbb{Z}_7^*$*. E, como cada linha apresenta o resultado* $\overline{1}$*, temos que para todo* $\overline{a} \in \mathbb{Z}_7^*$ *existe* $\overline{b} \in \mathbb{Z}_7^*$ *tal que* $\overline{a} \cdot \overline{b} = \overline{1}$*. Além disso, podemos constatar que* $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$*. Por exemplo,* $\overline{2} \cdot (\overline{5} \cdot \overline{4}) = \overline{2} \cdot (\overline{5 \cdot 4}) = \overline{2} \cdot \overline{6} = \overline{5}$ *e* $(\overline{2} \cdot \overline{5}) \cdot \overline{4} = (\overline{2 \cdot 5}) \cdot \overline{4} = \overline{3} \cdot \overline{4} = \overline{5}$*.*

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tabela 1: Operação $\cdot$ entre os elementos de $\mathbb{Z}_7^*$

Definição 3.73. *Seja $(G, \cdot)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de G $(H < G)$ quando, com a operação de G, o conjunto H é um grupo, isto é, quando as condições seguintes são satisfeitas:*

(i) H é fechado para a operação $\cdot$, ou seja, $h_1 \cdot h_2 \in H$, $\forall\, h_1, h_2 \in H$.

(ii) A operação $\cdot$ é associativa em H, ou seja,

$$h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3,\ \forall\, h_1, h_2, h_3 \in H.$$

(iii) H possui um elemento neutro, ou seja,

$$\exists\ e_H \in H \text{ tal que } e_H \cdot h = h \cdot e_H = h,\ \forall\, h \in H.$$

(iv) Todo elemento de H possui inverso, ou seja,

$$\forall h \in H,\ \exists k \in H \text{ tal que } h \cdot k = k \cdot h = e_H.$$

Observação 3.74.

1) A condição (i) é sempre satisfeita para todo subconjunto não vazio H de G, pois a propriedade associativa vale para todos os elementos de G.

Caso H seja subgrupo de G:

(i) O elemento neutro e_H é necessariamente igual ao elemento neutro e de G. De fato, se tomarmos $a \in H$, temos que $a \in G$. Como $e_H \cdot a = a$, multiplicando os dois lados pelo inverso de a em G, ou seja, a^{-1}, obtemos $e_H = e$.

(ii) Dado $h \in H$, o inverso de h em H é igual ao inverso de h em G. De fato, se k é o inverso de h em H, então $h \cdot k = k \cdot h = e_H$, logo $h \cdot k = k \cdot h = e$, pois $e_H = e$, e portanto k é o inverso de h em G.

A proposição a seguir mostra que precisamos testar apenas duas condições para mostrar que um subconjunto não-vazio H de G é um subgrupo de G.

Proposição 3.75. *Seja H um subconjunto não-vazio do grupo G. Então H é um subgrupo de G se, e somente se, as duas condições seguintes são satisfeitas:*

(i) $h_1 \cdot h_2 \in H, \forall\, h_1, h_2 \in H$.

(ii) $h^{-1} \in H, \forall\, h \in H$.

Demonstração: Suponhamos que H seja um subgrupo de G, então a condição (i) é satisfeita. E, considerando $h \in H$, temos que o inverso de h em H também pertence a H. Como o inverso de h em H é igual ao inverso de h em G, temos que $h^{-1} \in H$. Logo, a condição (ii) também é satisfeita.

Reciprocamente, suponhamos que (i) e (ii) sejam satisfeitas. Então, H é fechado para a operação $\cdot$. Como por (ii) $h, h^{-1} \in H$, temos por (i) que $h \cdot h^{-1} = e \in H$, portanto H possui elemento neutro. Além disso, por (ii) temos que os elementos de H possuem inverso. Como já observamos, os elementos de H são também elementos de G e, portanto, a operação entre eles é associativa. Assim, temos que H é subgrupo de G. ∎

Definição 3.76. *Sejam $(G, \cdot)$ um grupo e $a \in G$. Definimos as potências de a da seguinte forma:*

$$\begin{aligned} a^0 &= e; \\ a^1 &= a; \\ a^n &= a^{n-1} \cdot a, \text{ com } n \in \mathbb{N}; \\ a^{-n} &= (a^n)^{-1}, \text{ com } n \in \mathbb{N}. \end{aligned}$$

Denotamos por $\langle a \rangle$ o conjunto de todas as potências de a, ou seja:

$$\langle a \rangle = \{a^n \,;\, n \in \mathbb{Z}\}.$$

Proposição 3.77. *Dado $(G, \cdot)$ um grupo, $a \in G$ e $m, n \in \mathbb{Z}$, vale que:*

(i) $a^m a^n = a^{m+n}$ *e*

(ii) $(a^m)^n = a^{m \cdot n}$.

Demonstração:

(i) Demonstraremos, primeiro o seguinte caso particular: $n \geq 0$ e $m + n \geq 0$. O raciocínio será por indução sobre n.

Para $n = 0$, temos $a^m a^n = a^m a^0 = a^m e = a^m = a^{m+0} = a^{m+n}$. Portanto, a propriedade é válida quando $n = 0$.

Seja $n = r, r \geq 0$ e suponhamos que, para qualquer inteiro m tal que $m + r \geq 0$, se tenha $a^{m+r} = a^m a^r$. Então, como $r + 1 \geq 1$, pela Definição 3.76, temos

$$a^m a^{r+1} = a^m (a^r a^1) = (a^m a^r) a^1.$$

Pela hipótese de indução, temos $(a^m a^r) a^1 = a^{m+r} a^1$. E, como $m + r + 1 \geq 1$, podemos utilizar a Definição 3.76 novamente para escrever $a^{m+r} a^1 = a^{m+r+1}$.

Das igualdades anteriores, temos $a^m a^{r+1} = a^{m+r+1}$. O que mostra que quando a propriedade é válida para $n = r$, então ela também é válida para $n = r + 1$. Portanto, a propriedade é válida para todo $n \geq 0$.

Para o caso geral, sejam m e n inteiros qualquer. Tomemos um inteiro $p > 0$ tal que $p + n > 0$ e $p + m + n > 0$, o que obviamente sempre é possível. Note que, pela Definição 3.76, $a^p a^{-p} = a^p \left(a^p\right)^{-1} = e$. Então:

$$a^{m+n} = a^{m+n}\left(a^p a^{-p}\right) = \left(a^{m+n}a^p\right)a^{-p}.$$

Utilizando a conclusão do nosso caso particular na primeira, na terceira e na quarta igualdade a seguir, temos:

$$\begin{aligned}
\left(a^{m+n}a^p\right)a^{-p} &= a^{(m+n)+p}a^{-p} \\
&= a^{m+(n+p)}a^{-p} \\
&= \left(a^m a^{n+p}\right)a^{-p} \\
&= [a^m\left(a^n a^p\right)]a^{-p} \\
&= [\left(a^m a^n\right)a^p]a^{-p} \\
&= \left(a^m a^n\right)\left(a^p a^{-p}\right) \\
&= \left(a^m a^n\right)e \\
&= a^m a^n.
\end{aligned}$$

(ii) Provaremos o caso $n \geq 0$ por indução sobre n.

Para $n = 0$, temos que $\left(a^m\right)^n = \left(a^m\right)^0 = e = a^0 = a^{m\cdot 0} = a^{m\cdot n}$. Portanto, a propriedade é válida para $n = 0$.

Seja $n = r, r \geq 0$ e suponhamos que, para qualquer inteiro m tal que $m \cdot r \geq 0$, se tenha $a^{m\cdot r} = \left(a^m\right)^r$. Então, como $r + 1 \geq 1$, pela Definição 3.76, temos $\left(a^m\right)^{r+1} = \left(a^m\right)^r a^m$. Pela hipótese de indução, temos $\left(a^m\right)^r a^m = a^{mr}a^m$. E, por (i), temos $a^{mr}a^m = a^{mr+m} = a^{m(r+1)}$.

Das igualdades anteriores, temos $\left(a^m\right)^{r+1} = a^{m(r+1)}$. O que mostra que quando a propriedade é válida para $n = r$, então ela também é válida para $n = r + 1$. Portanto, a propriedade é válida para todo $n \geq 0$.

Agora, suponhamos $n < 0$. Então, pela Definição 3.76,

$$\left(a^m\right)^n = [\left(a^m\right)^{-n}]^{-1} = \left(a^{-mn}\right)^{-1} = a^{mn}.$$

■

Proposição 3.78. *$\langle a\rangle$ é subgrupo de G.*

Demonstração: Vamos verificar se as condições da Proposição 3.75 são satisfeitas:

(i) Dados a^m e $a^n \in \langle a \rangle$, temos, pela Proposição 3.77, que $a^m \cdot a^n = a^{m+n}$. Como $m+n \in \mathbb{Z}$, temos que $a^{m+n} \in \langle a \rangle$.

(ii) Pela própria definição de $\langle a \rangle$, temos que $a^{-1} \in \langle a \rangle$.

Portanto, $\langle a \rangle$ é subgrupo de G.

Definição 3.79. *$\langle a \rangle$ é o subgrupo de G gerado por a. O elemento a é dito o gerador de $\langle a \rangle$*

Definição 3.80. *Um grupo G é dito cíclico quando ele pode ser gerado por um elemento, isto é, quando $G = \langle g \rangle$, para algum $g \in G$.*

Exemplo 3.81. *Dado o grupo $\mathbb{Z}_{19}^* = \{\overline{1}, \overline{2}, \ldots, \overline{18}\}$, temos que 13 é um gerador de $\mathbb{Z}_{19}^*$, pois todos os elementos desse grupo podem são gerados por potências de 13, como é possível ver na tabela 2.*

$13^1 \equiv 18\,(mod\,19)$	$13^{10} \equiv 7\,(mod\,19)$
$13^2 \equiv 11\,(mod\,19)$	$13^{11} \equiv 6\,(mod\,19)$
$13^3 \equiv 17\,(mod\,19)$	$13^{12} \equiv 3\,(mod\,19)$
$13^4 \equiv 4\,(mod\,19)$	$13^{13} \equiv 1\,(mod\,19)$
$13^5 \equiv 14\,(mod\,19)$	$13^{14} \equiv 5\,(mod\,19)$
$13^6 \equiv 10\,(mod\,19)$	$13^{15} \equiv 13\,(mod\,19)$
$13^7 \equiv 12\,(mod\,19)$	$13^{16} \equiv 8\,(mod\,19)$
$13^8 \equiv 15\,(mod\,19)$	$13^{17} \equiv 2\,(mod\,19)$
$13^9 \equiv 16\,(mod\,19)$	$13^{18} \equiv 9\,(mod\,19)$

Tabela 2: Potências de 13 módulo 19

Assim, podemos afirmar que $\mathbb{Z}_{19}^*$ é um grupo cíclico e que 13 é um gerador desse grupo, ou seja, $\mathbb{Z}_{19}^* = \langle 13 \rangle$.

Definição 3.82. *A ordem de um grupo G é o número de elementos de G. Ela será denotada por $|G|$.*

Exemplo 3.83. *A ordem de $(\mathbb{Z}_n^*, \cdot)$ é $\phi(n)$. Em particular, para p primo a ordem de $\left(\mathbb{Z}_p^*, \cdot\right)$ é $p-1$. De fato, o grupo abeliano $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ possui $p-1$ elementos.*

4

RAÍZES PRIMITIVAS

Neste capítulo, apresentaremos o conceito de *raiz primitiva* e algumas propriedades relativas a essas raízes. Para tanto, começaremos definindo o conceito de *ordem de um inteiro a módulo m.*

As principais referências utilizadas neste capítulo foram [8], [10] e [11].

4.1 ORDEM DE UM INTEIRO A MÓDULO M

Definição 4.1. *Seja $a \in \mathbb{Z}$, tal que $(a, m) = 1$. O menor inteiro positivo k para o qual $a^k \equiv 1 \,(mod\, m)$ é chamado ordem de a módulo m e é denotado por $ord_m a$.*

Exemplo 4.2. *Considerando as potências de 4 módulo 7, temos:*

$$4^1 = 4 \equiv 4 \,(mod\, 7),$$
$$4^2 = 16 \equiv 2 \,(mod\, 7) \ \ e$$
$$4^3 = 64 \equiv 1 \,(mod\, 7).$$

Note que 3 é o menor expoente inteiro positivo pelo qual elevamos 4 e obtemos um número congruente a 1 módulo 7. Então, 3 é a ordem de 4 módulo 7, isto é, $ord_7 4 = 3$.

Observação 4.3. *Na Definição 4.1 tomamos $(a, m) = 1$, pois, caso contrário, não existe k inteiro positivo tal que $a^k \equiv 1 \,(mod\, m)$. De fato, se $(a, m) = d > 1$, então $a = ds$, para algum $s \in \mathbb{Z}$ com $1 \leq s < a$. Agora, se existe k inteiro positivo, tal que $a^k \equiv 1 \,(mod\, m)$, temos que $aa^{k-1} = dsa^{k-1} \equiv 1 \,(mod\, m)$. Como $m = dt$, para algum $t \in \mathbb{Z}$, com $1 \leq t < m$, então, $tdsa^{k-1} \equiv t \,(mod\, m)$. De onde, $0 \equiv msa^{k-1} \equiv t \,(mod\, m)$, o que é absurdo, pois $1 \leq t < m$.*

Note que se $(a, m) = 1$, a existência de k tal que $a^k \equiv 1 \,(mod\, m)$ está garantida, pois, pelo Teorema de Euler, Teorema 3.50, $a^{\phi(m)} \equiv 1 \,(mod\, m)$.

No restante do capítulo, vamos considerar $a \in \mathbb{Z}$ e $(a, m) = 1$.

A proposição a seguir nos mostra que a ordem de um inteiro a módulo m divide qualquer outro inteiro h para o qual $a^h \equiv 1 \,(mod\, m)$.

Proposição 4.4. *Se $k = ord_m a$ e $a^h \equiv 1 \,(mod\, m)$, então $k \mid h$.*

Demonstração: Pelo Algoritmo Euclidiano da Divisão, Teorema 2.21, existem inteiros q e r, com $0 \leq r < k$, tais que $h = qk + r$. Desta forma, temos

$$a^h = a^{qk+r} = (a^{kq})a^r \equiv a^r \,(mod\, m), \text{ pois}$$

como $k = ord_m a$, temos que $a^k \equiv 1 \,(mod\, m)$. Então, pela relação que acabamos de mostrar, temos que $a^r \equiv 1 \,(mod\, m)$. Como $r < k$, r só pode ser igual a zero, pois k é o menor inteiro positivo para o qual $a^k \equiv 1 \,(mod\, m)$. Portanto, $r = 0$ e $h = qk$, ou seja, $k \mid h$. ■

Corolário 4.5. *Temos que* $ord_m a \mid \phi(m)$.

Demonstração: Pelo Teorema de Euler, Teorema 3.50, temos que $a^{\phi(m)} \equiv 1 \,(mod\, m)$ para $(a, m) = 1$. Logo, a Proposição 4.4 nos garante que $ord_m a \mid \phi(m)$. ■

A proposição a seguir apresenta uma importante propriedade da ordem de um inteiro a módulo m.

Proposição 4.6. *Seja* $k = ord_m a$, *então* $a^t \equiv a^h \,(mod\, m)$ *se, e somente se,* $t \equiv h \,(mod\, k)$.

Demonstração: Supondo, sem perda de generalidade, $t \geq h$. Como $a^t = a^h a^{t-h}$ e, supondo, $a^t \equiv a^h \,(mod\, m)$, temos que $a^h a^{t-h} \equiv a^h \,(mod\, m)$. Como $(a, m) = 1$, então $(a^h, m) = 1$. Portanto, podemos cancelar a^h, nesta última congruência, obtendo

$$a^{t-h} \equiv 1 \,(mod\, m).$$

Pela Proposição 4.4, $k \mid (t - h)$ o que equivale a dizer que $t \equiv h \,(mod\, k)$.

Reciprocamente, se $t \equiv h \,(mod\, k)$, existe um inteiro n tal que $t = h + nk$. Logo,

$$a^t = a^{h+nk} = a^h(a^{nk}) \equiv a^h \,(mod\, m)$$

pois k é a ordem de a módulo m. ■

O corolário a seguir mostra que o conjunto formado por todas as potências de a com expoentes inteiros não negativos e menores do que a ordem de a módulo m contém apenas elementos incongruentes entre si módulo m.

Corolário 4.7. *Se* $k = ord_m a$, *então os números* $1, a, a^2, \ldots, a^{k-1}$ *são incongruentes módulo* m.

Demonstração: Suponhamos que $a^t \equiv a^h \,(mod\, m)$, $0 \leq t, h \leq k - 1$. Pela Proposição 4.6, $t \equiv h \,(mod\, k)$, ou seja, $k \mid t - h$. Como t e h são maiores ou iguais a zero e menores do que k, podemos concluir que $t = h$. Portanto, os números $1, a, a^2, \ldots, a^{k-1}$ são todos incongruentes módulo m. ■

A proposição e o corolário a seguir apresentam algumas propriedades da ordem de um inteiro a módulo m.

Proposição 4.8. *Para* $k = ord_m a$ *e* t *um inteiro positivo temos,*

$$ord_m a = (k, t) \cdot ord_m(a^t).$$

Demonstração: Considerando que $ord_m(a^t) = h$, temos $(a^t)^h = a^{th} \equiv 1\,(mod\, m)$. Como $k = ord_m a$, temos que $k \mid th$. Portanto, $th \equiv 0\,(mod\, k)$, o que é equivalente a $h \equiv 0\,(mod\, \frac{k}{d})$, com $d = (k,t)$. A menor solução positiva da congruência $h \equiv 0\,(mod\, \frac{k}{d})$ é $\frac{k}{d}$, o que nos leva a concluir que $ord_m(a^t) = \frac{k}{d}$. Assim, $d \cdot ord_m(a^t) = ord_m a$ e $(k,t) \cdot ord_m(a^t) = ord_m a$. ∎

Corolário 4.9. *$ord_m(a^t) = ord_m a$ se, e somente se, $(k,t) = 1$, onde $k = ord_m a$.*

Demonstração: Pela Proposição 4.8, $(k,t) \cdot ord_m(a^t) = ord_m a$. Logo $(k,t) = 1$ se, e somente se, $ord_m(a^t) = ord_m a$. ∎

4.2 RAÍZES PRIMITIVAS MÓDULO M

De posse da definição de ordem de um inteiro a módulo m e das propriedades apresentadas, podemos definir o que é uma *raiz primitiva módulo m*.

Definição 4.10. *Se $ord_m a = \phi(m)$ dizemos que a é uma raiz primitiva módulo m.*

Exemplo 4.11. *O número 2 é uma raiz primitiva módulo 5. De fato, temos que:*

$$2^1 = 2 \equiv 2\,(mod\, 5),$$
$$2^2 = 4 \equiv 4\,(mod\, 5),$$
$$2^3 = 8 \equiv 3\,(mod\, 5)\ \ e$$
$$2^4 = 16 \equiv 1\,(mod\, 5).$$

Portanto, a ordem de 2 módulo 5 é 4, que corresponde a $\phi(5) = 5 - 1 = 4$.

Proposição 4.12. *Seja a uma raiz primitiva módulo m. Então, a^t é uma raiz primitiva módulo m se, e somente se, $(t, \phi(m)) = 1$.*

Demonstração: Se a é uma raiz primitiva módulo m, então $ord_m a = \phi(m)$.

Se a^t é raiz primitiva módulo m, então $ord_m(a^t) = ord_m a$ e, do Corolário 4.9, temos que $(t, \phi(m)) = 1$. Por outro lado, se $(t, \phi(m)) = 1$, então $ord_m(a^t) = ord_m a$ e, portanto, a^t é raiz primitiva módulo m. ∎

Proposição 4.13. *Um inteiro positivo m que possui uma raiz primitiva, possui exatamente $\phi(\phi(m))$ raízes primitivas incongruentes.*

Demonstração: Seja a uma raiz primitiva módulo m. Note que $a, a^2, a \ldots, a^{\phi(m)}$ forma um sistema reduzido de resíduos módulo m. Pela Proposição 4.12, a^t é raiz primitiva se, e somente se, $(t, \phi(m)) = 1$. A quantidade de $t's$ tal que $(t, \phi(m)) = 1$, $1 \leq t \leq \phi(m)$, é $\phi(\phi(m))$. ∎

Exemplo 4.14. *Temos que 5 possui uma raiz primitiva: 2. Logo, 5 possui $\phi(\phi(5)) = \phi(4) = 2$ raízes primitivas, a saber 2 e 3.*

4.3 RAÍZES PRIMITIVAS MÓDULO p, p PRIMO

Proposição 4.15. *Sejam p um primo ímpar e d um divisor positivo de $p-1$. Então o número de inteiros incongruentes módulo p tendo ordem igual a d é $\phi(d)$.*

Demonstração: Da Proposição 3.44, temos:

$$\sum_{d|n} \phi(d) = n.$$

Tomando $n = p-1$, temos:

$$\sum_{d|(p-1)} \phi(d) = p-1.$$

Agora, vamos tomar o conjunto $B = \{1, 2, \ldots, p-1\}$ e dividi-lo em subconjuntos B_d para cada divisor d de $p-1$, de modo que $B_d = \{a \ ; \ ord_p a = d\}$. Note que esses subconjuntos são disjuntos e a sua união resulta em B, pois pelo Corolário 4.5, a ordem de qualquer inteiro positivo a tal que $(a, p) = 1$ divide $\phi(p) = p-1$.

Considere $g(d)$ o número de elementos de B_d. Então,

$$\sum_{d|(p-1)} g(d) = p-1.$$

De onde, podemos concluir:

$$\sum_{d|(p-1)} (\phi(d) - g(d)) = 0$$

Precisamos mostrar que $\phi(d) = g(d)$ para todo d tal que $d \mid (p-1)$.

Suponha $g(d) \neq 0$, isto é, $B_d \neq \phi$. Considere $a \in B_d$, então $ord_p a = d$, ou seja, $a^d \equiv 1 \, (mod\, p)$.

Como $a, a^2, \ldots, a^d$ são todos incongruentes módulo p, Corolário 4.7, todas essas potências são soluções de $x^d \equiv 1 \, (mod\, p)$.

Pelo Teorema 3.55 de Lagrange, sendo p primo $x^d - 1 \equiv 0 \, (mod\, p)$ tem no máximo d soluções incongruentes módulo p. Portanto, estes d números $a, a^2, \ldots, a^d$ são todas as soluções incongruentes módulo p de $x^d - 1 \equiv 0 \, (mod\, p)$. Logo, todo elemento de B_d é da forma a^t para algum $t \in \{1, 2, \ldots, d\}$. Mas, pelo Corolário 4.7, $ord_p(a^t) = ord_p a = d$ se, e somente se, $(t, d) = 1$. Portanto, dentre os números $a, a^2, \ldots, a^d$ existem exatamente $\phi(d)$ com ordem igual a d. Isto nos garante que $g(d) = \phi(d)$. Agora, se $g(d) = 0$, então $\phi(d)$ deveria ser zero, o que não ocorre. Portanto, $g(d) = \phi(d)$, para todo d que divide n.

■

Exemplo 4.16. *Consideremos $p = 7$ e $\{1, 2, 3, 6\}$ o conjunto dos divisores de $p - 1 = 6$. Vamos separar o conjunto $B = \{1, 2, 3, 4, 5, 6\}$ em subconjuntos para cada divisor de 6:*

$$B_1 = \{1\},$$
$$B_2 = \{6\},$$
$$B_3 = \{2, 4\} \text{ e}$$
$$B_6 = \{3, 5\}.$$

Note que $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$ e $\phi(6) = 2$, que correspondem a exatamente a quantidade de elementos dos conjuntos B_1, B_2, B_3 e B_6, respectivamente.

Proposição 4.17. *Todo número primo ímpar possui uma raiz primitiva*

Demonstração: Essa propriedade é consequência imediata da Proposição 4.15. Como $\phi(p) = p - 1$ é um divisor de $p - 1$, existem $\phi(\phi(p)) = \phi(p - 1)$ raízes primitivas módulo p. ∎

Exemplo 4.18. *Considerando o número primo ímpar 7, temos:*

$$3^1 = 3\,(mod\,7)$$
$$3^2 = 9 = 2\,(mod\,7)$$
$$3^3 = 27 = 6\,(mod\,7)$$
$$3^4 = 81 = 4\,(mod\,7)$$
$$3^5 = 243 = 5\,(mod\,7)$$
$$3^6 = 729 = 1\,(mod\,7)$$

Portanto, 3 é raiz primitiva módulo 7.

4.4 RAÍZES PRIMITIVAS MÓDULO p^t, p PRIMO ÍMPAR, $t > 1$ INTEIRO

Proposição 4.19. *Se a é uma raiz primitiva módulo p, então $a + p$ também é.*

Demonstração: Note que queremos mostrar que $ord_p(a + p) = \phi(p)$. Suponha $(a + p)^n \equiv 1\,(mod\,p)$, para $n < \phi(p)$. Como $(a + p)^n \equiv a^n\,(mod\,p)$, temos um absurdo, pois a é raiz primitiva. Logo, $a + p$ tem ordem $\phi(p)$ e também é raiz primitiva módulo p. ∎

Proposição 4.20. *Existe r, raiz primitiva módulo p, p primo ímpar, para a qual a seguinte relação se verifica:*

$$r^{p-1} \not\equiv 1(mod\,p^2)$$

Demonstração: Pelo Teorema 4.17 existe r uma raiz primitiva módulo p. Se r verifica a propriedade $r^{p-1} \not\equiv 1\,(mod\,p^2)$, não há o que demonstrar. Caso contrário, se

$r^{p-1} \equiv 1\,(mod\, p^2)$, vamos mostrar que $b = r + p$ é uma raiz primitiva módulo p que satisfaz a propriedade desejada.

Temos que

$$\begin{aligned} b^{p-1} &= (r+p)^{p-1} \\ &= \sum_{i=0}^{p-1} \binom{p-1}{i} r^{p-1-i} p^i \\ &= r^{p-1} + (p-1)r^{p-2}p + \sum_{i=2}^{p-1} \binom{p-1}{i} r^{p-1-i} p^i. \end{aligned}$$

Note que todo termo da última soma acima possui o fator p^2. Logo, módulo p^2, temos:

$$b^{p-1} \equiv 1 + r^{p-2}(p^2 - p) \equiv 1 - pr^{p-2}\,(mod\, p^2).$$

Como estamos supondo que $r^{p-1} \equiv 1\,(mod\, p^2)$, temos que $b^{p-1} \not\equiv 1\,(mod\, p^2)$, pois a congruência $pr^{p-2} \equiv 0\,(mod\, p^2)$ não pode ser verdadeira, uma vez que ela implicaria $r^{p-2} \equiv 0\,(mod\, p)$, o que não pode ocorrer sendo r uma raiz primitiva e $(r, p) = 1$. Isto mostra que b satisfaz a propriedade desejada. ■

Proposição 4.21. *Se a for uma raiz primitiva módulo p, p primo ímpar, com $a^{p-1} \not\equiv 1\,(mod\, p^2)$, então*

$$a^{\phi(p^{t-1})} \not\equiv 1\,(mod\, p^t)$$

para todo $t \geq 2$.

Demonstração: Vamos demonstrar essa propriedade por indução em t.

Para $t = 2$, temos:

$$a^{\phi(p^{2-1})} = a^{\phi(p)} = a^{p-1} \not\equiv 1\,(mod\, p^2).$$

Portanto, a propriedade é válida para $t = 2$.

Suponha que a propriedade seja válida para t, vamos verificar se, nessas condições, ela permanece válida para $t + 1$.

Como $(a, p) = 1$, pois a é uma raiz primitiva, temos que $(a, p^{t-1}) = 1$ e, portanto, pelo Teorema de Euler, Teorema 3.50,

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

Então, existe um inteiro n tal que

$$a^{\phi(p^{t-1})} = 1 + np^{t-1}.$$

Este inteiro n não é divisível por p, pois se tivéssemos $n = kp$, teríamos:

$$a^{\phi(p^{t-1})} = 1 + kp^t, \tag{1}$$

o que contradiz a hipótese de indução. Sabendo que $p \nmid n$, elevamos ambos os membros de (1) à potência p.

$$\begin{aligned}
[a^{\phi(p^{t-1})}]^p &= a^{p\phi(p^{t-1})} \\
&= (1+np^{t-1})^p \\
&= \sum_{i=0}^{p} \binom{p}{i} (np^{t-1})^i \\
&= \binom{p}{0} + \binom{p}{1} np^{t-1} + \binom{p}{2} n^2 p^{2(t-1)} + \sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i \\
&= 1 + np^t + \frac{p(p-1)}{2} n^2 p^{2t-2} + \sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i \\
&= 1 + np^t + \frac{p-1}{2} n^2 p^{2t-1} + \sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i.
\end{aligned}$$

Mas, sendo $3t-3 = t + (2t-3) \geq t+1$ para $t \geq 2$, todo termo da soma

$$\sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i$$

possui uma potência de p que é maior do que ou igual a p^{t+1}.

Como $2t - 1 \geq t + 1$, para $t \geq 2$, as igualdades acima nos garantem que

$$a^{p\phi(p^{t-1})} \equiv 1 + np^t \,(mod\, p^{t+1}).$$

De onde,

$$a^{\phi(p^t)} \not\equiv 1 \,(mod\, p^{t+1}),$$

uma vez que $p \nmid n$. Mas isto é a propriedade desejada com $t+1$ no lugar de t. ∎

Proposição 4.22. *Se p é um primo ímpar, então uma raiz primitiva módulo p é também uma raiz primitiva módulo p^t, para $t > 1$ se, e somente se, $a^{p-1} \not\equiv 1 \,(mod\, p^2)$.*

Demonstração: Seja a uma raiz primitiva módulo p e suponhamos que a também seja uma raiz primitiva módulo p^t, para $t > 1$. Ou seja, $a^{\phi(p^t)} \equiv 1 \,(mod\, p^t)$, o que, pela Proposição 3.42, equivale a

$$\begin{aligned}
a^{p^t - p^{t-1}} &= 1 + kp^t \Leftrightarrow \\
a^{p^{t-2}(p^2-p)} &= 1 + kp^t \Leftrightarrow \\
a^{p^{t-2}(p^2-p)} &\equiv 1 \,(mod\, p^2) \Leftrightarrow \\
a^{p^2-p} &\equiv 1 \,(mod\, p^2).
\end{aligned}$$

Neste caso, a é raiz primitiva módulo p^2 o que implica em

$$a^{p-1} \not\equiv 1 \,(mod\, p^2),$$

caso contrário, teríamos uma contradição, pois $p-1 < p(p-1) = \phi(p^2)$.

Para provar a recíproca, suponha que a seja uma raiz primitiva módulo p e $a^{p-1} \not\equiv 1\,(mod\, p^2)$. Vamos mostrar que a também é uma raiz primitiva módulo p^t, para todo $t \geq 2$.

Precisamos mostrar que

$$k = ord_{p^t} a = \phi(p^t).$$

Como $a^k \equiv 1\,(mod\, p^t)$ temos que $a^k \equiv 1\,(mod\, p)$. Pela Proposição 4.8, $\phi(p) \mid k$. Logo, $k = n\phi(p)$. Mas sendo $k = ord_{p^t} a$, temos que $k \mid \phi(p^t)$ e, portanto, $n\phi(p) \mid \phi(p^t)$. Como $\phi(p^t) = p^{t-1}(p-1)$ temos que,

$$n(p-1) \mid p^{t-1}(p-1) \text{ implica } n \mid p^{t-1}.$$

Como p é primo, $n = p^h$, $h \leq t-1$. Portanto, $k = p^h\phi(p) = p^h(p-1)$.

Precisamos mostrar que $h = t-1$. Vamos supor que $h < t-1$, isto é, $h \leq t-2$. Neste caso, teríamos

$$k = p^h(p-1) \mid p^{t-2}(p-1) = \phi(p^{t-1})$$

Isto nos diz que $\phi(p^{t-1})$ é um múltiplo de k e, portanto,

$$a^{\phi(p^{t-1})} \equiv 1(mod\, p^t)$$

o que contradiz a Proposição 4.21. Logo, $h = t-1$ implica $n = p^{t-1}$, que implica em $k = p^{t-1}\phi(p) = p^{t-1}(p-1) = \phi(p^t)$. ■

Exemplo 4.23. *Considerando $p = 5$, temos que 2 é raiz primitiva módulo 5. Note que $2^{5-1} = 2^4 = 16 \not\equiv 1\,(mod\, 5^2)$. Então, pela Proposição 4.22, 2 é raiz primitiva módulo 5^t para todo $t > 1$.*

Teorema 4.24. *Se p é primo ímpar, então p^t possui raiz primitiva para $t > 1$.*

Demonstração: Pela Proposição 4.20, existe a, raiz primitiva módulo p, tal que $a^{p-1} \not\equiv 1\,(mod\, p^2)$. Pela Proposição 4.22, a é raiz primitiva módulo p^t para $t > 1$. ■

Exemplo 4.25. *Seja $p = 29$. Temos que 14 é raiz primitiva módulo 29. Porém, $14^{p-1} = 14^{28} \equiv 1\,(mod\, 29^2)$. Então, 14 não é raiz primitiva módulo 29^2. Por outro lado, 2 é raiz primitiva módulo 29 e $2^{28} \equiv 30\,(mod\, 29^2)$. Então, 2 é raiz primitiva módulo 29^2.*

Com os resultados anteriores, provamos a existência de raízes primitivas módulo p^t para p um primo ímpar. Com o argumento que utilizamos na demonstração da Proposição 4.19, concluímos que se a é uma raiz primitiva módulo p^t, então $a + p^t$ também será. Como ou a ou $a + p^t$ é um número ímpar, temos que p^t possui sempre uma raiz primitiva ímpar.

4.5 RAÍZES PRIMITIVAS MÓDULO $2p^t$, p PRIMO ÍMPAR

Teorema 4.26. *Para p um primo ímpar, $2p^t$ possui raiz primitiva.*

Demonstração: Como vimos, p^t possui raiz primitiva ímpar. Considere a uma raiz primitiva ímpar módulo p^t. Vamos provar que a é, também, raiz primitiva módulo $2p^t$. Temos que, $(a, 2p^t) = 1$, pois a é ímpar e $1 < a < p$. Seja $k = ord_{2p^t}a$. Precisamos mostrar que $k = \phi(2p^t)$. Sabemos que $k \mid \phi(2p^t)$. Sendo $\phi(2p^t) = \phi(p^t)$, $k \mid \phi(p^t)$. Mas como $a^k \equiv 1\,(mod\,2p^t)$ temos $a^k \equiv 1\,(mod\,p^t)$. Logo, sendo a uma raiz primitiva módulo p^t, podemos concluir que $\phi(p^t) \mid k$. Portanto, $k = \phi(2p^t)$, isto é, a é uma raiz primitiva módulo $2p^t$. ■

4.6 NÚMEROS QUE POSSUEM RAÍZES PRIMITIVAS

Nesta seção iremos mostrar quais números possuem raízes primitivas. Antes, porém, iremos apresentar dois resultados que nos mostram quais potências de 2 não possuem raiz primitiva.

Proposição 4.27. *Para k inteiro, $k \geq 3$ e a um inteiro ímpar, temos*

$$a^{\frac{\phi(2^k)}{2}} \equiv 1\,(mod\,2^k).$$

Demonstração: A demonstração será feita por indução em k.

Para $k = 3$, temos $\phi(2^3) = \phi(8) = 4, logo, a^{\frac{\phi(2^3)}{2}} = a^{\frac{4}{2}} = a^2$.

Como a é ímpar, podemos representar $a = 2n + 1$, para algum n inteiro. Logo:

$$a^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1.$$

Como $n(n+1)$ é par, temos que $4n(n+1)$ é múltiplo de 8. Então, $a^2 \equiv 1\,(mod\,8)$ e, portanto, $a^2 \equiv 1\,(mod\,2^3)$.

Agora, suponha que essa propriedade seja válida para algum k inteiro, $k \geq 3$, ou seja, $a^{\frac{\phi(2^k)}{2}} \equiv 1\,(mod\,2^k)$. Vamos verificar se essa propriedade vale para $k+1$.

Podemos escrever, pela Proposição 3.42:

$$a^{\frac{\phi(2^k)}{2}} = a^{\frac{2^k - 2^{k-1}}{2}} = a^{\frac{2^{k-1}(2-1)}{2}} = a^{\frac{2^{k-1}}{2}} = a^{2^{k-2}}.$$

Então,

$$a^{\frac{\phi(2^k)}{2}} = 2^{k-2} \equiv 1\,(mod\,2^k)$$

Assim, $a^{2^{k-2}} = 1 + m \cdot 2^k$, para algum $m \in \mathbb{Z}$. De onde,

$$\begin{aligned}
\left(a^{2^{k-2}}\right)^2 &= \left(1 + m \cdot 2^k\right)^2 \Leftrightarrow \\
a^{2^{k-1}} &= 1 + 2^{k+1} \cdot m + m^2 \cdot 2^{2k} \Leftrightarrow \\
a^{2^{k-1}} &= 1 + 2^{k+1}\left(m + m^2 \cdot 2^{k-1}\right) \Leftrightarrow \\
a^{2^{k-1}} &\equiv 1\,\left(mod\,2^{k+1}\right).
\end{aligned}$$

Perceba que essa última relação de congruência corresponde à relação $a^{\frac{\phi\left(2^{k+1}\right)}{2}} = a^{\frac{2^{k+1}-2^k}{2}} = a^{2^{k-1}} \equiv 1\,(mod\,2^{k+1})$. Portanto, a propriedade é válida para $k+1$.

Como essa propriedade é válida para $k = 3$ e, supondo ela válida para algum k inteiro, mostramos que ela também é válida para $k+1$, podemos concluir que essa propriedade é válida para todo $k \geq 3$. ■

Teorema 4.28. *2^k não possui raiz primitiva se, e somente se, $k \geq 3$.*

Demonstração: Se $k \geq 3$, vimos na Proposição 4.27 que se a é ímpar, $a^{\frac{\phi(2^k)}{2}} \equiv 1\,(mod\,2^k)$. Portanto, $ord_{2^k}a < \phi(2^k)$. Logo, a não é raiz primitiva módulo 2^k. Para $k = 1$, temos que $ord_2 1 = 1 = \phi(2)$. Para $k = 2$, temos $ord_4 3 = 2 = \phi(4)$. ■

Agora vamos analisar outros valores de m.

Exemplo 4.29. *Seja $m = 15$. Temos que m não possui raiz primitiva. De fato, tomando o conjunto $\{a\,;\,(a,15) = 1\} = \{1,2,4,7,8,11,13,14\}$, podemos perceber que ele possui 8 elementos. Logo, $\phi(15) = 8$. Então uma raiz primitiva módulo 15 deve ser um número inteiro k, com $(k,15) = 1$, tal que $k^8 \equiv 1\,(mod\,15)$ e $k^j \not\equiv 1\,(mod\,15)$ para todo $0 < j < 8$. Temos que:*

- *2 não é raiz primitiva módulo 15, pois $2^4 = 16 \equiv 1\,(mod\,15)$;*
- *4 não é raiz primitiva módulo 15, pois $4^2 = 16 \equiv 1\,(mod\,15)$;*
- *7 não é raiz primitiva módulo 15, pois $7^4 = 2401 \equiv 1\,(mod\,15)$;*
- *8 não é raiz primitiva módulo 15, pois $8^4 = 4096 \equiv 1\,(mod\,15)$;*
- *11 não é raiz primitiva módulo 15, pois $11^2 = 121 \equiv 1\,(mod\,15)$;*
- *13 não é raiz primitiva módulo 15, pois $13^4 = 28561 \equiv 1\,(mod\,15)$ e*
- *14 não é raiz primitiva módulo 15, pois $14^2 = 196 \equiv 1\,(mod\,15)$.*

Portanto, 15 não possui raiz primitiva.

Com o teorema a seguir mostraremos que nenhum número m, que não seja de uma das seguintes formas: $1, 2, 4, p^t$ e $2p^t$, com p primo ímpar, possui raiz primitiva.

Teorema 4.30. *Se $m \geq 1$ não é da forma $1, 2, 4, p^t$ e $2p^t$ (p primo ímpar), então m não possui raiz primitiva.*

Demonstração: Seja

$$m = p_1^{t_1} p_2^{t_2} \dots p_s^{t_s}.$$

Vamos supor que m possua uma raiz primitiva. Seja a uma raiz primitiva módulo m. Logo, $(a,m) = 1$ e $ord_m a = \phi(m)$. Como $(a,m) = 1$, então, $(a, p_i^{t_i}) = 1, \forall i = 1, 2, \dots, s$ e $t_i \geq 1$. Assim, pelo Teorema de Euler, Teorema 3.50, temos

$$a^{\phi(p_i^{t_i})} \equiv 1 (mod\, p_i^{t_i}).$$

Como

$$\phi(m) = \phi(p_1^{t_1})\phi(p_2^{t_2}) \dots \phi(p_s^{t_s}),$$

podemos considerar

$$B = [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_s^{t_s})].$$

Então

$$a^B \equiv 1 \,(mod\, p_i^{t_i}), \forall i = 1, 2, \dots, s$$

e, portanto, $\phi(m) \leq B$. Logo,

$$\phi(p_1^{t_1})\phi(p_2^{t_2}) \dots \phi(p_s^{t_s}) \leq [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_s^{t_s})].$$

Mas, para que um produto de números seja menor do que ou igual ao mínimo múltiplo comum destes números, estes números, necessariamente, deverão ser relativamente primos dois a dois.

Como $\phi(p^t) = p^{t-1}(p-1)$ sabemos que este número é par para p ímpar ou se $p = 2, t \geq 2$. Disto concluímos que os números

$$\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_s^{t_s})$$

serão primos, dois a dois, somente se $s = 1$ ou $s = 2$ e $m = 2p^t$. Isso mostra que m, caso tenha raiz primitiva, deverá ser de forma p^t ou $2p^t$ (p primo ímpar). Como já provamos que números desta forma possuem raízes primitivas então, ser da forma $1, 2, 4, p^t, 2p^t$ é uma condição necessária e suficiente para que possua raiz primitiva. ■

Saber quais números possuem raiz primitiva é uma informação interessante para encontrar alguns grupos cíclicos, como mostra a definição a seguir.

Definição 4.31. *Se a é uma raiz primitiva módulo n, então a é um gerador de $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$. Portanto, $(\mathbb{Z}_n^*, \cdot)$ é um grupo cíclico.*

Exemplo 4.32. *Seja $(\mathbb{Z}_5^*, \cdot)$. Temos que 3 é raiz primitiva módulo 5, pois*

$$3^1 \equiv 3 \,(mod\, 5)$$
$$3^2 \equiv 4 \,(mod\, 5)$$
$$3^3 \equiv 2 \,(mod\, 5)$$
$$3^4 \equiv 1 \,(mod\, 5)$$

Note que dado $b \in \mathbb{Z}_5^*$, temos que existe $j \in \mathbb{Z}, 0 < j < 5$ tal que $3^j \equiv b \,(mod\, 5)$. Portanto, 3 é um gerador de $\mathbb{Z}_5^*$ e $(\mathbb{Z}_5^*, \cdot)$ é um grupo cíclico.

Proposição 4.33. *$(\mathbb{Z}_n^*, \cdot)$ é um grupo cíclico se, e somente se, $n = 2, 4, p^t, 2p^t$; p primo ímpar, $t \geq 1$.*

Demonstração: Temos que, pela Definição 4.31, $(\mathbb{Z}_n^*, \cdot)$ é um grupo cíclico se, e somente se, n possui uma raiz primitiva. Pelo Teorema 4.30, apenas números da forma $1, 2, 4, p^t, 2p^t$ possuem raiz primitiva. ■

5

APLICAÇÕES NA CRIPTOGRAFIA

Neste capítulo apresentaremos os *logaritmos discretos*, que apresentam forte ligação com as raízes primitivas. Além da aplicação desse tipo de logaritmo em um algoritmo criptográfico de chave pública, conhecido como ElGamal.

As principais referências utilizadas neste capítulo foram [2], [3], [5], [12] [13].

5.1 LOGARITMOS DISCRETOS

Sejam p um inteiro primo e a uma raiz primitiva módulo p. Para todo inteiro b, tal que $p \nmid b$, existe um único inteiro $j, 0 \leq j < p-1$, tal que:

$$b \equiv a^j \,(mod\, p).$$

Definição 5.1. *Denotamos j por $dlog_{a,p}(b)$ e o chamamos índice do inteiro b na base a módulo p. Portanto, $dlog_{a,p}(b)$ é o menor inteiro maior ou igual a zero, tal que:*

$$a^{dlog_{a,p}(b)} \equiv b \,(mod\, p)$$

Exemplo 5.2. *As potências de 2 módulo 5 são:*

$$\begin{aligned} 2^0 &\equiv 1 \,(mod\, 5),\\ 2^1 &\equiv 2 \,(mod\, 5),\\ 2^2 &\equiv 4 \,(mod\, 5),\\ 2^3 &\equiv 3 \,(mod\, 5),\\ 2^4 &\equiv 1 \,(mod\, 5), \end{aligned}$$

o que mostra que 2 é raiz primitiva módulo 5, pois $4 = \phi(5)$ é o menor inteiro positivo m, tal que $2^m \equiv 1 \,(mod\, 5)$.

Com isso, podemos determinar o índice de um inteiro x na base 2 módulo 5, ou seja, $dlog_{2,5}(x)$.

Note que $dlog_{2,5}(1) = 0$, pois $x = 0$ é o menor expoente maior ou igual a zero tal que $2^x \equiv 1 \,(mod\, 5)$. Do mesmo modo, podemos obter a Tabela 3:

x	1	2	4	3
$dlog_{2,5}(x)$	0	1	2	3

Tabela 3: Índice de x na base 2 módulo 5

Como vimos na Definição 4.31, se a é uma raiz primitiva módulo p, então a é um gerador de $\mathbb{Z}_p^*$. Portanto, se tomarmos o conjunto $S = \{a^j \,;\, 0 \leq j < p-1\}$, teremos $S = \mathbb{Z}_p^*$. Com isso, podemos interpretar $dlog_{a,p}(x)$ como uma função com domínio no conjunto $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}$ e imagem no conjunto $\{0, 1, 2, \ldots, p-2\}$. Essa função possui propriedades semelhantes às do logaritmo de números reais, verificadas a seguir.

Proposição 5.3. *Dados a uma raiz primitiva módulo p e $x, y \in \mathbb{Z}$, tais que $p \nmid x$ e $p \nmid y$, valem as seguintes propriedades:*

(i) $dlog_{a,p}(1) = 0$

(ii) $dlog_{a,p}(a) = 1$

(iii) $dlog_{a,p}(xy) \equiv dlog_{a,p}(x) + dlog_{a,p}(y) \,(mod\,(p-1))$

(iv) $dlog_{a,p}(x^r) \equiv r \cdot dlog_{a,p}(x) \,(mod\,(p-1))$.

Demonstração:

(i) Como $a^0 = 1 \equiv 1 \,(mod\, p)$, temos que $dlog_{a,p}(1) = 0$ para todo a inteiro e p inteiro primo.

(ii) Como $a^1 = a \equiv a \,(mod\, p)$, temos que $dlog_{a,p}(a) = 1$ para todo a inteiro e p inteiro primo.

(iii) Note que $a^{dlog_{a,p}(x)} \equiv x \,(mod\, p)$ e $a^{dlog_{a,p}(y)} \equiv y \,(mod\, p)$. Multiplicando essas congruências, temos:

$$a^{dlog_{a,p}(x)} \cdot a^{dlog_{a,p}(y)} = a^{dlog_{a,p}(x)+dlog_{a,p}(y)} \equiv xy \equiv a^{dlog_{a,p}(xy)} \,(mod\, p).$$

De onde,

$$a^{dlog_{a,p}(x)+dlog_{a,p}(y)-dlog_{a,p}(xy)} \equiv 1 \,(mod\, p).$$

Como a é raiz primitiva módulo p, $ord_p a = p-1$. Então,

$$(p-1) \mid dlog_{a,p}(x) + dlog_{a,p}(y) - dlog_{a,p}(xy)$$

e,

$$dlog_{a,p}(xy) \equiv dlog_{a,p}(x) + dlog_{a,p}(y) \,(mod\,(p-1)).$$

(iv) Como vale a propriedade (iii), podemos tomar $y = x$ de modo a obter:

$$dlog_{a,p}(x^2) \equiv dlog_{a,p}(x) + dlog_{a,p}(x) = 2 \cdot dlog_{a,p}(x) \,(mod\,(p-1)).$$

Note que podemos aplicar essa propriedade $r-1$ vezes para obter

$$dlog_{a,p}(x^r) = r \cdot dlog_{a,p}(x) \,(mod\,(p-1)).$$

■

Exemplo 5.4. *No Exemplo 5.2, vimos que, para $x = 4$, $dlog_{2,5}(4) = 2$, e para $x = 3$, $dlog_{2,5}(3) = 3$. Então:*

$$dlog_{2,5}(12) = dlog_{2,5}(4 \cdot 3) = dlog_{2,5}(4) + dlog_{2,5}(3) = 2 + 3 \equiv 1 \,(mod\,5),$$

de acordo com a terceira propriedade. Do mesmo modo,

$$dlog_{2,5}(27) = dlog_{2,5}(3^3) = 3 \cdot dlog_{2,5}(3) = 3 \cdot 3 = 9 \equiv 1 \,(mod\,4),$$

de acordo com a quarta propriedade.

Considere a função

$$\begin{aligned} dlog_{a,p}(x) : \mathbb{Z}_p^* &\longrightarrow \{0, 1, \ldots, p-2\} \\ \bar{b} &\longmapsto dlog_{a,p} b \end{aligned}$$

Como esta função apresenta as mesmas propriedades do logaritmo usual, temos a seguinte definição:

Definição 5.5. *A função $dlog_{a,p}(x) : \mathbb{Z}_p^* \longrightarrow \{0, 1, \ldots, p-2\}$ é chamada logaritmo discreto de base a módulo p.*

Observação 5.6. *De forma similiar, podemos generalizar o conceito de logaritmo discreto para qualquer grupo cíclico finito $(G, \cdot)$. No entanto, para este trabalho consideramos apenas $G = \mathbb{Z}_p^*$.*

A ideia de logaritmos discretos apresenta importantes aplicações no campo da criptografia, algumas das quais apresentaremos mais adiante.

Vamos, agora, discutir o porquê dos logaritmos discretos serem interessantes para criar algoritmos criptográficos.

5.1.1 *O Problema do Logaritmo Discreto*

Fixada a uma raiz primitiva módulo p e dado $\bar{b} \in \mathbb{Z}_p^*$, o problema do logaritmo discreto consiste em encontrar $x, 0 \leq x \leq (p-2)$, tal que $b \equiv a^x \,(mod\,p)$. Em geral, dados b, a e p, é muito difícil calcular o logaritmo discreto quando p é um número primo formado por muitos algarismos.

Exemplo 5.7. *Determine $dlog_{13,19}(12)$.*

Como vimos no Exemplo 3.81, o número 13 é um gerador de $\mathbb{Z}_{19}^*$. Na tabela 2, podemos observar que $13^7 \equiv 12 \,(mod\,19)$. Portanto, $dlog_{13,19}(12) = 7$.

Neste exemplo, utilizamos valores baixos, o que torna o problema de fácil resolução com o uso de um computador. No entanto, quando escolhemos o primo p e o gerador a de $\mathbb{Z}_p^*$ convenientemente grandes, a resolução torna-se difícil até mesmo para um computador. Segundo [13], para impedir ataques, p deveria ter, pelo menos, 300 dígitos e $p-1$ deveria ter, pelo menos, um fator primo grande.

Essa dificuldade inspirou os matemáticos Bailey Whitfield Diffie e Martin Edward Hellman a criarem um algoritmo de chave pública, conhecido como método de troca de chaves de Diffie-Hellman, que permite aos usuários uma troca de chaves em um meio inseguro. E, inspirado nesse método de troca de chaves, o matemático Taher Elgamal criou o algoritmo criptográfico de chave pública ElGamal, o qual apresentaremos a seguir.

5.2 O ALGORITMO CRIPTOGRÁFICO ELGAMAL

O algoritmo ElGamal se inicia com a escolha de um grupo cíclico G, de ordem n e de um gerador g de G. Neste trabalho, vamos optar por $G = \mathbb{Z}_p^*$, o grupo das classes inversíveis módulo p, sendo p um número primo. O gerador de G será qualquer raiz primitiva módulo p e a ordem de G será $p-1$.

O algoritmo de criptografia ElGamal foi inspirado no método de troca de chaves de Diffie-Hellman, o qual apresentamos a seguir.

5.2.1 *O método de troca de chaves de Diffie-Hellman*

A ideia dessa troca de chaves é baseada no princípio da troca de uma caixa com cadeados:

Imagine que Maria deseja enviar uma caixa para João por um meio inseguro e deseja garantir que somente João será capaz de abrir essa caixa. O processo para realizar essa troca pode ser feito da seguinte forma:

(i) Maria envia a caixa com um cadeado que só ela consegue abrir para o João.

(ii) João recebe a caixa, coloca um cadeado que só ele consegue abrir nela e envia de volta para Maria.

(iii) Maria recebe a caixa de volta, retira o seu cadeado e envia novamente para João, com o cadeado dele.

(iv) Ao receber a caixa, João retira o seu cadeado e consegue abri-la.

Perceba que para fazer esse processo, nem Maria e nem João precisam ter as chaves um do outro. Além disso, uma pessoa que intercepte essa troca de caixas não será capaz de abrir a caixa, pois não terá a chave de nenhum dos dois.

O método de troca de chaves de Diffie-Hellman segue esse princípio e funciona da seguinte forma:

(i) Maria e João combinam de utilizar um número inteiro primo p e uma raiz primitiva α módulo p.

(ii) Maria escolhe um inteiro aleatório x_m e envia para João y_m, onde $y_m \equiv \alpha^{x_m} \, (mod\, p)$.

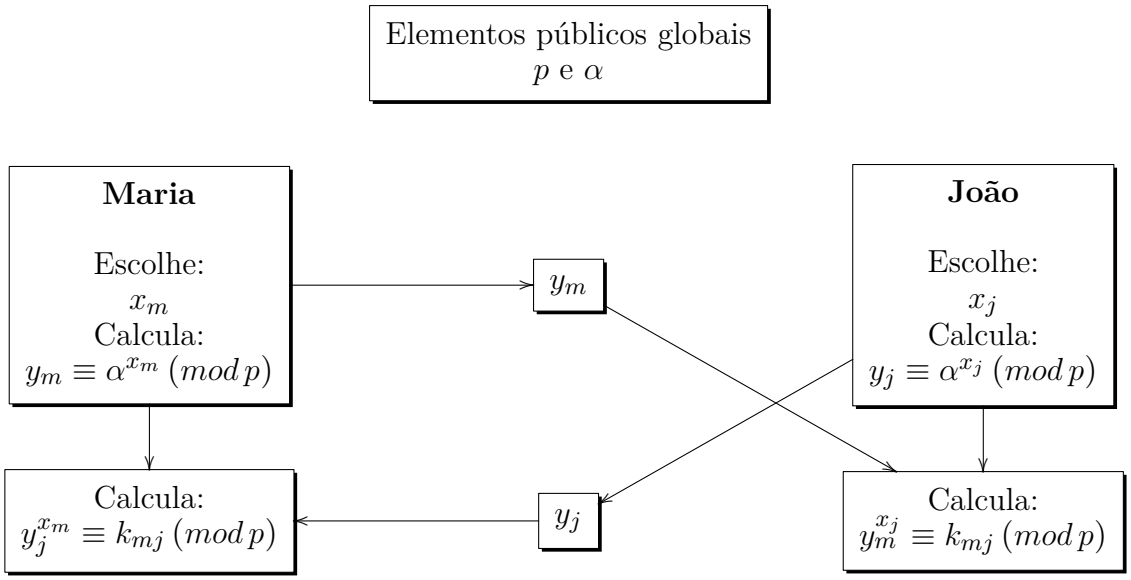
(iii) João escolhe um inteiro aleatório x_j e envia para Maria y_j, onde $y_j \equiv \alpha^{x_j} \, (mod\, p)$.

(iv) Ao receber y_j, Maria calcula k_{mj}, onde $k_{mj} \equiv y_j^{x_m} \, (mod\, p)$.

(v) João calcula k_{mj}, onde $k_{mj} \equiv y_m^{x_j} \, (mod\, p)$.

Dessa forma, Maria e João conhecerão o valor de k_{mj}, pois

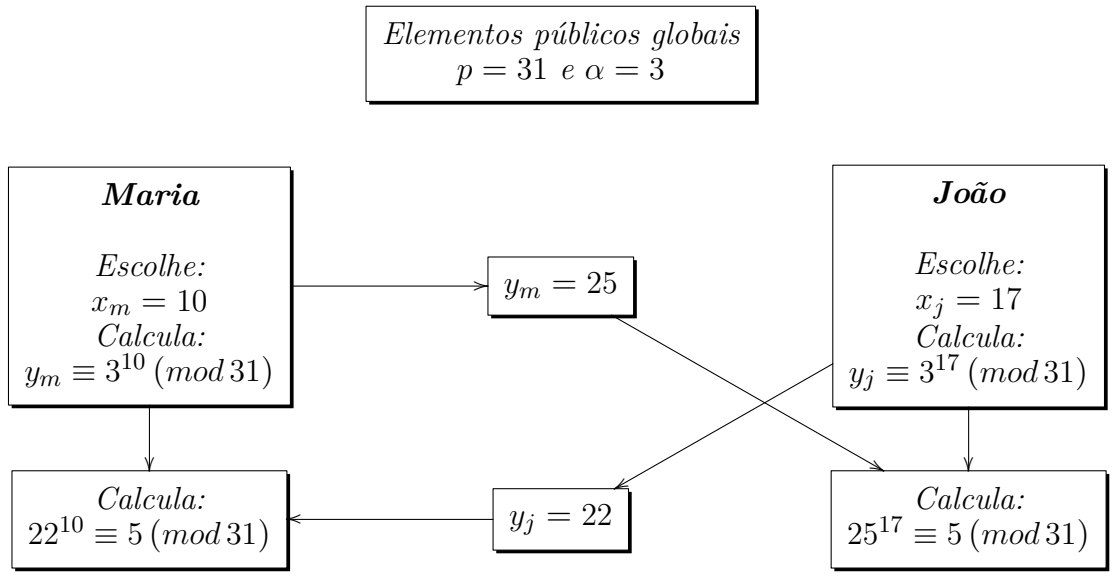
$$y_j^{x_m} \equiv (\alpha^{x_j})^{x_m} \equiv (\alpha^{x_m})^{x_j} \equiv y_m^{x_j} \, (mod\, p).$$



Note que qualquer pessoa que tentar interceptar essa comunicação entre os dois terá acesso somente a α, p, y_m e y_j e, para calcular k_{mj}, seria necessário conhecer o valor de x_m ou de x_j. Para determinar esses valores, seria necessário calcular o logaritmo discreto de y_m módulo p ou de y_j módulo p. Note que para valores de p, x_m e x_j grandes o suficiente, temos um problema computacionalmente complexo.

Observação 5.8. *O algoritmo pode ser implementado da mesma forma para qualquer grupo cíclico G de ordem n com gerador g.*

Exemplo 5.9. *Imagine que Maria e João desejam trocar mensagens e vão utilizar o esquema de troca de chaves de Diffie-Hellman. Então, eles escolhem o primo $p = 31$ e o inteiro $\alpha = 3$ raiz primitiva módulo 31. Maria escolhe o inteiro $m = 10$ e João escolhe o inteiro $j = 17$. A troca de chaves entre Maria e João está descrita no diagrama a seguir:*



Perceba que ao final desse processo, tanto Maria, quanto João conseguem obter o número 5 sem que esse valor seja trocado entre eles.

Note que esse sistema não é totalmente seguro, pois é possível que um atacante, alguém desejando interceptar as mensagens, se passe por Maria e João e combine chaves secretas distintas com os dois. Nesse caso, esse atacante poderia interceptar toda as comunicações entre Maria e João. Portanto, para utilizar o esquema de troca de chaves de Diffie-Hellman, é necessário fazer uso de um esquema para garantir a autenticação. Neste trabalho não trataremos de autenticação, porém é possível encontrar esse conteúdo nas referências [3], [12] e [13].

Apresentaremos, agora, o método para o envio de mensagens utilizando o algoritmo criptográfico ElGamal. Nesse método, o envio de mensagens será feito simultaneamente com a troca de chaves e a cada nova mensagem as chaves serão trocadas.

5.2.2 *Envio de mensagens*

Suponha que Maria deseja enviar uma mensagem para João. Para iniciar o processo, João deve criar uma chave pública, seguindo os passos a seguir.

(i) João escolhe um grupo cíclico $\mathbb{Z}_p^*$ e um gerador α de $\mathbb{Z}_p^*$.

(ii) João escolhe uma chave particular x_j, $1 < x_j < p-1$ e calcula y_j, onde $y_j = \alpha^{x_j} \, (mod\, p)$.

(iii) A chave pública de João será (p, α, y_j).

Para cifrar a mensagem M, Maria utiliza a chave pública de João (p, α, y_j) e realiza os passos a seguir.

(iv) Maria escolhe um número inteiro $x_m, 0 < x_m < p-1$ e calcula:

$$c_1 \equiv \alpha^{x_m} \, (mod\, p)$$

e

$$c_2 \equiv M y_j^{x_m} \, (mod\, p).$$

(v) Maria envia para João a mensagem encriptada (c_1, c_2). Note que o tamanho da mensagem criptografada é maior do que o da mensagem que se deseja enviar.

Para decifrar a mensagem, João utiliza (c_1, c_2) e aplica os passos a seguir:

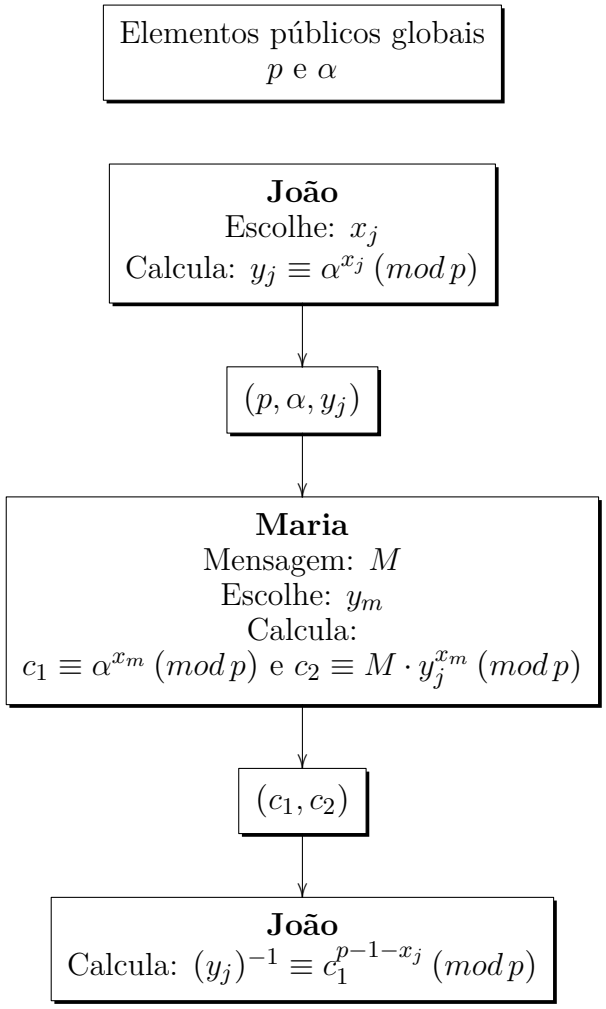
(vi) João calcula $(y_j^{x_m})^{-1}$, da seguinte forma:

$$(y_j^{x_m})^{-1} \equiv c_1^{p-1-x_j} \, (mod\, p).$$

De fato, $c_1^{p-1-x_j} \equiv c_1^{p-1} c_1^{-x_j} \equiv 1 \cdot (\alpha^{x_m})^{-x_j} \equiv (\alpha^{x_j})^{-x_m} \equiv (y_j^{x_m})^{-1} \, (mod\, p)$.

(vii) João obtém M, da relação $M \equiv c_2 (y_j^{x_m})^{-1} \, (mod\, p)$.

O diagrama a seguir ilustra o funcionamento do algoritmo Elgamal para o envio de uma mensagem M.



Observação 5.10. *Não é recomendado utilizar o mesmo valor de y_j para encriptar mais de uma mensagem. Caso isso ocorra, um atacante que conhecer a mensagem e o par $(c_{1,1}, c_{2,1})$ de uma primeira troca de mensagens e $(c_{1,2}, c_{2,2})$ de uma segunda troca de mensagens, ele poderá encontrar m_2 fazendo o seguinte cálculo: Sejam,*

$$c_{2,1} \equiv m_1(y_j^{x_m})^{-1} \,(mod\, p),$$
$$c_{2,2} \equiv m_2(y_j^{x_m})^{-1} \,(mod\, p),$$

então, $\frac{m_1}{m_2} \equiv \frac{c_{2,1}}{c_{2,2}} \,(mod\, p)$. Então, caso o atacante conheça m_1, ele poderá facilmente calcular m_2.

Perceba que quebrar esse sistema é equivalente a quebrar o esquema de troca de chaves de Diffie-Hellman. Sempre que M é conhecido, calcular x_j ou x_m a partir de p, α, c_1, c_2 e y_j é equivalente a calcular logaritmos discretos, pois tanto x_j, quanto x_m aparecem como expoentes.

Para enviar uma mensagem, utilizando o algoritmo ElGamal, precisamos converter o texto em um valor numérico. Para tanto, geralmente se utiliza uma tabela ASCII (Figura 1), que estabelece valores numéricos para cada um dos caracteres que possam ser utilizados. Simplificamos essa ideia codificando algumas palavras por números de dois algarismos, apresentados na Tabela 4.

ARITMÉTICA	11
CRIPTOGRAFIA	13
ELGAMAL	17
LOGARITMOS	19
MATEMÁTICA	24
PRIMOS	26
PROFMAT	28
RAÍZES	30

Tabela 4: Tabela de códigos e palavras

Utilizando os códigos da Tabela 4, podemos aplicar o algoritmo criptográfico ElGamal, como mostram os exemplos a seguir.

Exemplo 5.11. *Vamos enviar como mensagem a palavra PROFMAT, utilizando $p = 31$ e $\alpha = 3$, para facilitar os cálculos.*

Para criar uma chave pública, nosso destinatário deve escolher um número inteiro $x_j, 0 \leq x_j \leq 30$, por exemplo, $x_j = 20$ e calcular:

$$y_j \equiv 3^{20} \,(mod\, 31).$$

Temos, $y_j = 5$. Então, a chave pública do nosso destinatário será $(31, 3, 5)$.

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
0	0	NUL	16	10	DLE	32	20	(space)	48	30	0
1	1	SOH	17	11	DC1	33	21	!	49	31	1
2	2	STX	18	12	DC2	34	22	"	50	32	2
3	3	ETX	19	13	DC3	35	23	#	51	33	3
4	4	EOT	20	14	DC4	36	24	$	52	34	4
5	5	ENQ	21	15	NAK	37	25	%	53	35	5
6	6	ACK	22	16	SYN	38	26	&	54	36	6
7	7	BEL	23	17	ETB	39	27	'	55	37	7
8	8	BS	24	18	CAN	40	28	(	56	38	8
9	9	TAB	25	19	EM	41	29	)	57	39	9
10	A	LF	26	1A	SUB	42	2A	*	58	3A	:
11	B	VT	27	1B	ESC	43	2B	+	59	3B	;
12	C	FF	28	1C	FS	44	2C	,	60	3C	<
13	D	CR	29	1D	GS	45	2D	-	61	3D	=
14	E	SO	30	1E	RS	46	2E	.	62	3E	>
15	F	SI	31	1F	US	47	2F	/	63	3F	?

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
64	40	@	80	50	P	96	60	`	112	70	p
65	41	A	81	51	Q	97	61	a	113	71	q
66	42	B	82	52	R	98	62	b	114	72	r
67	43	C	83	53	S	99	63	c	115	73	s
68	44	D	84	54	T	100	64	d	116	74	t
69	45	E	85	55	U	101	65	e	117	75	u
70	46	F	86	56	V	102	66	f	118	76	v
71	47	G	87	57	W	103	67	g	119	77	w
72	48	H	88	58	X	104	68	h	120	78	x
73	49	I	89	59	Y	105	69	i	121	79	y
74	4A	J	90	5A	Z	106	6A	j	122	7A	z
75	4B	K	91	5B	[	107	6B	k	123	7B	{
76	4C	L	92	5C	\	108	6C	l	124	7C	|
77	4D	M	93	5D	]	109	6D	m	125	7D	}
78	4E	N	94	5E	^	110	6E	n	126	7E	~
79	4F	O	95	5F	_	111	6F	o	127	7F	

Figura 1: Tabela ASCII. Disponível em:<https://ascii.cl/>. Acesso em 13 set. 2018

Para enviar a mensagem PROFMAT, utilizamos o código $M = 28$ *e escolhemos uma chave* $x_m, 0 \leq x_m \leq 30$, *por exemplo,* $x_m = 17$ *e calculamos*

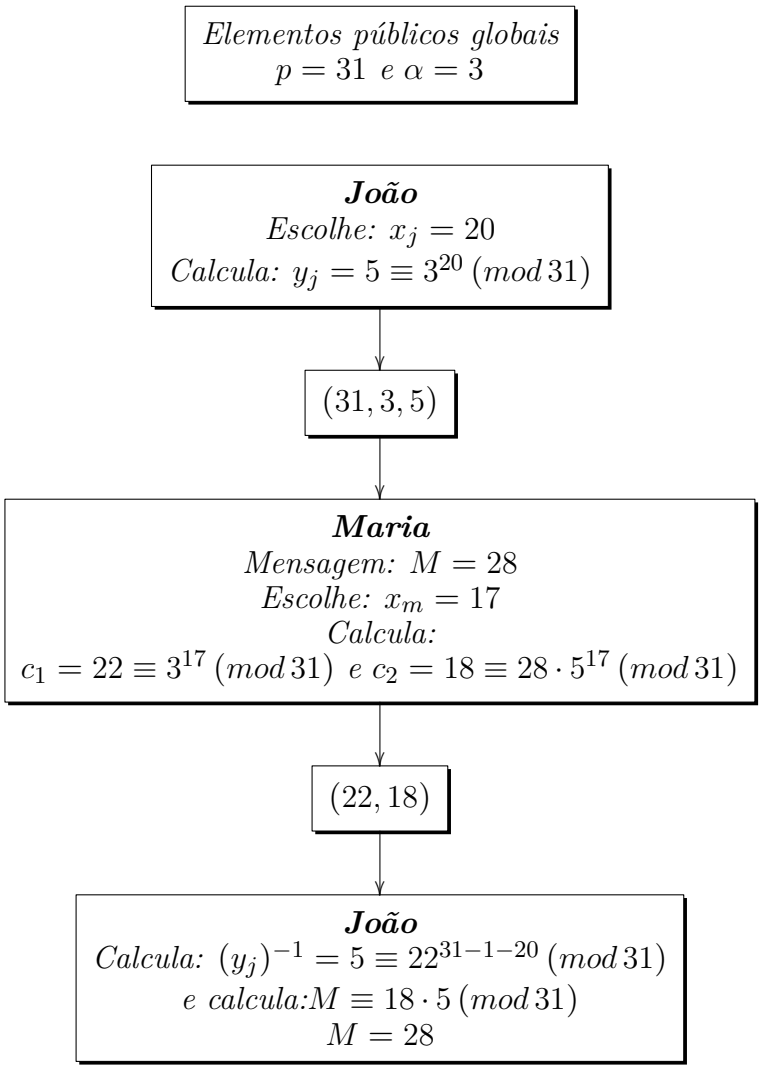
$$c_1 \equiv 3^{17} \, (mod \, 31).$$

Portanto, $c_1 = 22$. *Calculando*

$$c_2 \equiv 28 \cdot 5^{17} \, (mod \, 31),$$

obtemos, portanto, $c_2 = 18$, *e a nossa mensagem m cifrada será o par* $(22, 18)$.

Para decifrar a mensagem, nosso destinatário calcula $(y_j^{x_m})^{-1} \equiv 22^{31-1-20} \equiv 5 \, (mod \, 31)$ *e, depois, calcula* $M \equiv c_2 (y_j^{x_m})^{-1} \equiv 18 \cdot 5 \equiv 28 \, (mod \, 31)$, *obtendo* 28 *que é o código da nossa mensagem.*



Exemplo 5.12. *Suponha que criamos uma chave pública* $(19, 13, 8)$ *e a chave secreta* $x_j = 5$.

Recebemos, então, a mensagem $(17, 5)$ *e desejamos desencriptá-la. Para tanto, calculamos:*

$$(y_j^{x_m})^{-1} \equiv 17^{19-1-5} \equiv 11 \, (mod \, 19)$$

E, em seguida, calculamos:

$$M \equiv c_2 (y_j^{x_m})^{-1} \equiv 5 \cdot 11 \equiv 17 \, (mod \, 19)$$

Portanto, recebemos a mensagem ELGAMAL, de acordo com a Tabela 4.

De posse do algoritmo de criptografia ElGamal, elaboramos uma proposta didática que consiste em uma sequência didática para ser trabalhada com alunos do Ensino Médio, a qual apresentamos no próximo capítulo.

6 PROPOSTA DIDÁTICA

Neste capítulo, apresentaremos uma sequência didática para aplicar os assuntos tratados ao longo dos demais capítulos. Esse tipo de sequência consiste em uma série de atividades devidamente organizadas para alcançar alguns objetivos de aprendizagem pré-definidos.

6.1 SEQUÊNCIA DIDÁTICA

A presente sequência didática tem por objetivo propor uma sequência de atividades nas quais os alunos terão contato com conceitos básicos de Teoria dos Números e com uma aplicação prática desses conceitos em um algoritmo criptográfico. Com essas atividades, pretendemos que os alunos reconheçam a importância dos números inteiros e suas propriedades.

6.2 PÚBLICO ALVO

Alunos de qualquer série do Ensino Médio, desde que já tenham sido apresentados ao conceito de logaritmo e suas propriedades.

6.3 NÚMERO DE AULAS PREVISTAS

4 aulas

6.4 OBJETIVOS DE APRENDIZAGEM

1. Reconhecer a importância dos números inteiros e suas propriedades para o desenvolvimento de sistemas de criptografia.
2. Compreender os conceitos de congruência modular e raízes primitivas.
3. Relacionar o conceito de logaritmo discreto com o conceito de logaritmo de números reais e reconhecer as semelhanças de suas propriedades.
4. Compreender o funcionamento do algoritmo criptográfico ElGamal e criptografar e descriptografar mensagens, utilizando esse algoritmo.

6.5 COMPETÊNCIA E HABILIDADE PREVISTAS PELA BNCC

A competência e a habilidade indicadas abaixo foram retiradas da Base Nacional Comum Curricular BNCC Ensino Médio [1].

6.5.1 *Competência específica 3*

> Utilizar estratégias, conceitos e procedimentos matemáticos, em seus campos - Aritmética, Álgebra, Grandezas e Medidas, Geometria, Probabilidade e Estatística -, para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.

6.5.2 *Habilidade*

> **(EM13MAT305)** Resolver e elaborar problemas com funções logarítmicas nos quais é necessário compreender e interpretar a variação das grandezas envolvidas, em contextos como os de abalos sísmicos, pH, radioatividade, Matemática Financeira, entre outros.

6.6 DESENVOLVIMENTO

Nesta seção apresentaremos propostas para o desenvolvimento de cada uma das aulas. Pela necessidade de oferecer recursos para que os alunos compreendam o processo do algoritmo criptográfico ElGamal, algumas aulas apresentam uma característica mais expositiva.

6.6.1 *Aula 1: Aritmética modular e criação da calculadora de módulo*

Duração: 45 minutos.
Local de desenvolvimento da atividade: sala de informática.
Recursos necessários: lousa, giz, computadores com um software de planilhas eletrônicas instalado e projetor.

Professor, inicie a aula explicando aos alunos que nas primeiras aulas eles irão trabalhar alguns conceitos que servirão de base para as atividades das aulas 3 e 4. Apresente a eles a definição de congruência, Definição 3.1. Para garantir a compreensão dessa relação de congruência, faça alguns exemplos com eles, como os apresentados a seguir.

Exemplo 6.1. *Verifique se* 19 *e* 36 *são congruentes módulo* 17*.*

Solução: Como $19 = 1 \cdot 17 + 2$ *e* $36 = 2 \cdot 17 + 2$*, temos que ambos os números apresentam resto* 2 *na divisão por* 17*. Assim, podemos afirmar que* $36 \equiv 19 \equiv 2 \,(mod\, 17)$*.*

Exemplo 6.2. *Verifique se* 23 *e* 46 *são congruentes módulo* 11.

Solução: Como $23 = 2 \cdot 11 + 1$ *e* $45 = 4 \cdot 11 + 2$*, temos que esses números não apresentam o mesmo resto na divisão por* 11*. Assim, podemos afirmar que* $46 \not\equiv 23 \,(mod\, 17)$.

Aproveite esses exemplos para deixar os alunos mais familiarizados com as notações utilizadas.

Explique aos alunos que, a partir desse momento, eles irão criar uma calculadora de módulo, utilizando um *software* de planilhas eletrônicas.

A escolha por utilizar planilhas eletrônicas se deu porque esses softwares são de fácil acesso e muitos estudantes são minimamente familiarizados com as suas ferramentas. Para as imagens, utilizamos o *software* Excel, mas é possível utilizar qualquer outro *software* de planilha eletrônica, existem, inclusive, opções gratuitas.

Ao abrir o *software* de planilhas eletrônicas, vocês encontrarão um ambiente com várias células para inserir informações, como mostra a Figura 2.

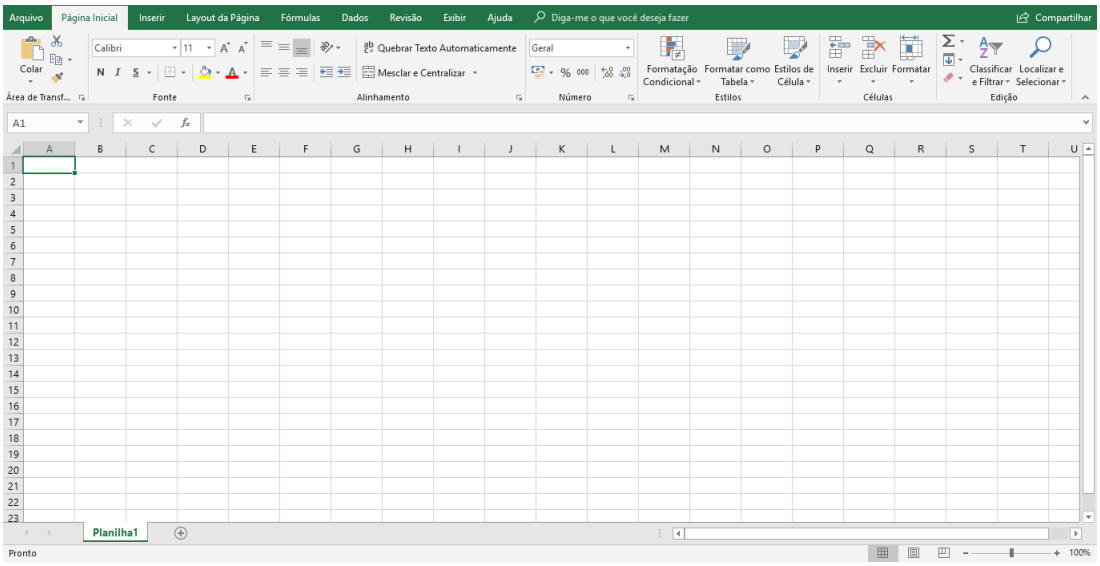


Figura 2: Ambiente de um *software* de planilhas eletrônicas

A calculadora que iremos criar funcionará da seguinte forma: ao escolhermos inteiros a e b, ela retornará o resultado de a módulo b, ou seja, o resto da divisão de a por b. Para tanto, precisamos selecionar as células que receberão essas informações e a célula que irá retornar o resultado. Podemos destacar as células utilizando as ferramentas de borda e cor. Na Figura 3, apresentamos uma sugestão, na qual optamos por inserir o valor de a na célula $B1$ e o valor de b na célula $B2$. Optamos, também, por retornar o resultado de $a \,mod\, b$ na célula $E1$.

Precisamos, agora, definir a a fórmula que retornará o resto da divisão de a por b. Vamos observar o seguinte: se dividirmos um número a por b na calculadora, encontraremos um número inteiro ou um número decimal. Esse resultado será um número inteiro quando essa divisão apresentar resto zero. E, esse resultado será um número decimal quando essa divisão apresentar resto diferente de zero. Podemos obter o resto dessa divisão a partir da parte decimal do resultado, como mostramos no exemplo a seguir.

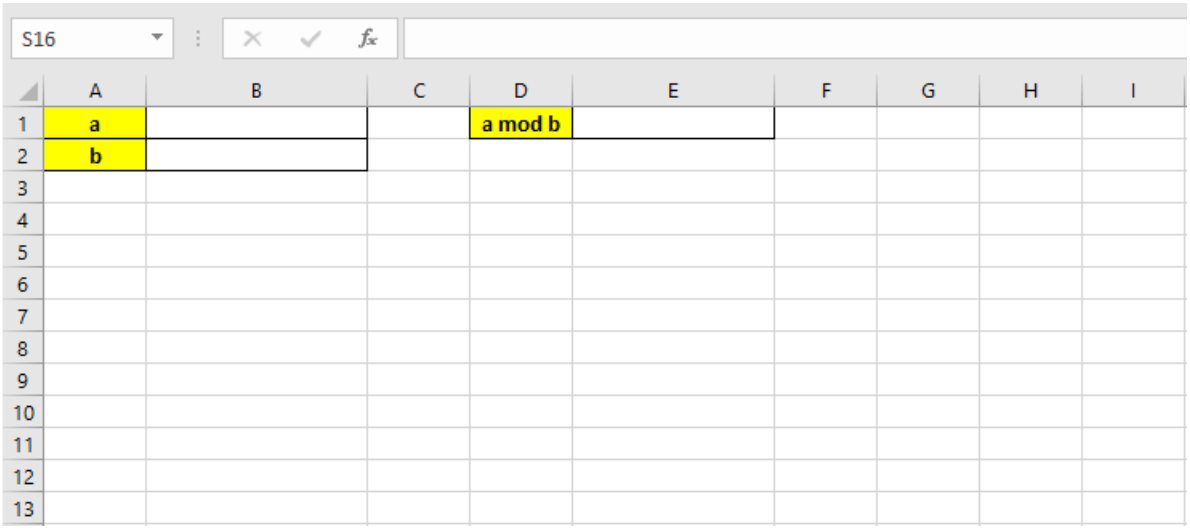


Figura 3: Células que receberão os valores de a e b e célula que retornará a módulo b

Exemplo 6.3. *Ao dividir* 19 *por* 4*, obtemos* $4,75$*. A parte inteira desse número, representa o quociente dessa divisão. O resto dessa divisão pode ser obtido a partir da multiplicação da parte decimal por* 4*. Ou seja,* $0,75 \cdot 4 = 3$ *é o resto dessa divisão. De fato,* $19 = 4 \cdot 4 + 3$.

Assim, nós precisaremos tomar o resultado da divisão de a por b, obtido por $B1/B2$, e retirar dele a parte inteira desse número. Para isso, temos uma fórmula INT que retorna esse resultado. Então, se usarmos $INT(B1/B2)$ obteremos a parte inteira da divisão de a por b. Para obter apenas a parte decimal, fazemos: $(B1/B2) - INT(B1/B2)$. Como vimos no exemplo, devemos multiplicar a parte decimal por b, então fazemos $((B1/B2) - INT(B1/B2)) * B2$. Para que o Excel entenda que é uma fórmula, inserimos o sinal "=" antes da fórmula, ou seja,

$$= ((B1/B2) - INT(B1/B2)) * B2$$

Essa será a fórmula que deverá ser inserida na célula $E1$, como mostra a Figura 4.

Com essa fórmula o valor na célula retornará o resto da divisão de a por b. Então, podemos inserir alguns valores nas células B1 e B2, correspondentes a a e b, para testar a nossa calculadora. Escolhemos $a = 29$ e $b = 3$. Note que $29 = 3 \cdot 9 + 2$, então o resultado que a calculadora deverá retornar será 2, como mostra a Figura 5.

Por fim, basta salvar o arquivo para utilizar a calculadora de módulo nas atividades propostas, sempre que for necessário.

Para finalizar a aula, apresente algumas propriedades da relação de congruência, presentes nas Proposições 3.6, 3.7, 3.8 e 3.9. Para esse trabalho, não é necessário demonstrar essas propriedades para os alunos, apenas peça a eles que, em duplas, escolham exemplos e verifiquem a validade das propriedades apresentadas, utilizando a calculadora construída.

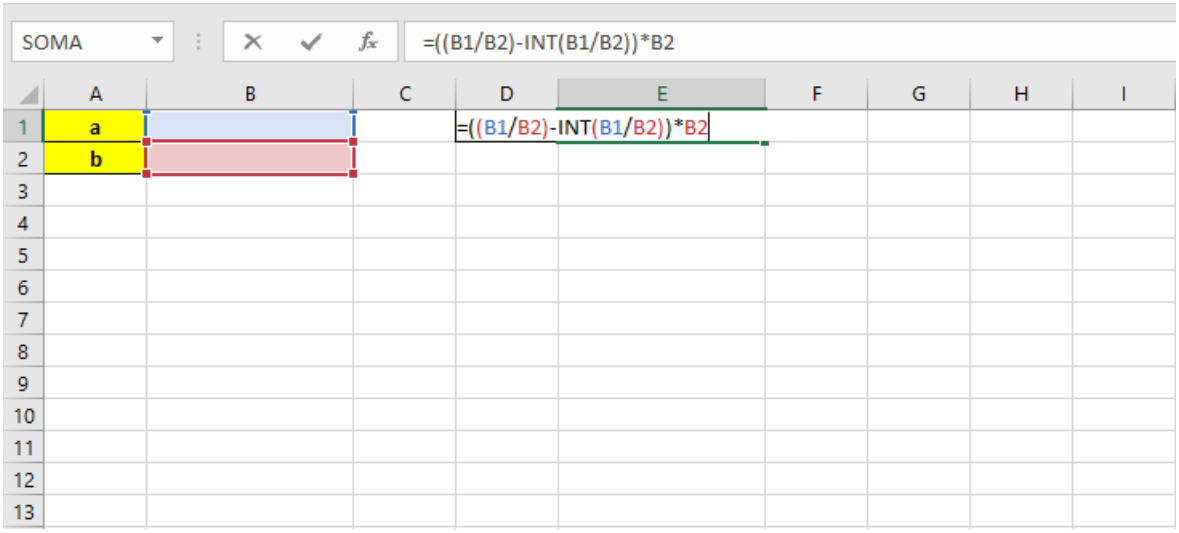


Figura 4: Fórmula completa da calculadora de módulo.

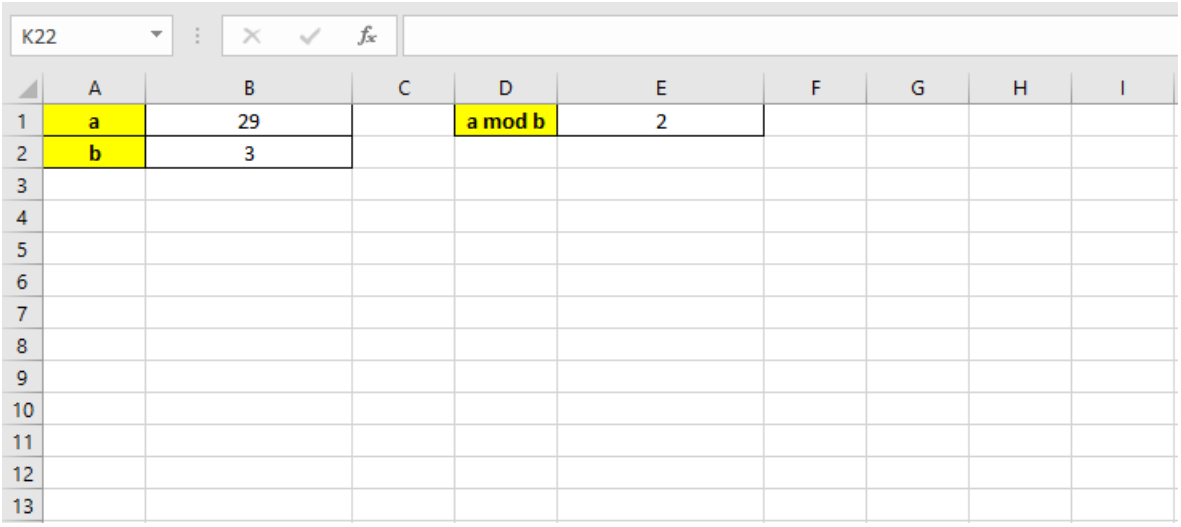


Figura 5: Teste da calculadora de módulo.

6.6.2 *Aula 2: Função ϕ de Euler, raízes primitivas e logaritmos discretos*

Duração: 45 minutos.
Local de desenvolvimento da atividade: sala de aula.
Recursos necessários: lousa e giz.

Inicie a aula apresentando a definição da função ϕ de Euler, Definição 3.40 e trabalhe os seguintes exemplos.

Exemplo 6.4. *Encontre $\phi(4)$.*

Solução: O conjunto $\{0, 1, 2, 3, 4\}$ é um sistema completo de resíduos módulo 4. Dentro desse conjunto, os elementos que são relativamente primos com 4 são apenas dois, $\{1, 3\}$. Então, $\phi(4) = 2$.

Exemplo 6.5. *Encontre $\phi(7)$.*

Solução: O conjunto $\{0, 1, 2, 3, 4, 5, 6\}$ *é um sistema completo de resíduos módulo* 7. *Dentro desse conjunto, os elementos que são relativamente primos com* 7 *são apenas seis,* $\{1, 2, 3, 4, 5, 6\}$. *Então,* $\phi(7) = 6$.

Exemplo 6.6. *Encontre* $\phi(3)$.

Solução: O conjunto $\{0, 1, 2\}$ *é um sistema completo de resíduos módulo* 3. *Dentro desse conjunto, os elementos que são relativamente primos com* 3 *são apenas dois,* $\{1, 2\}$. *Então,* $\phi(3) = 2$.

Exemplo 6.7. *Encontre* $\phi(11)$.

Solução: O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ *é um sistema completo de resíduos módulo* 11. *Dentro desse conjunto, os elementos que são relativamente primos com* 11 *são apenas dez,* $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. *Então,* $\phi(11) = 10$.

Peça aos alunos que comparem os resultados dos exemplos. Destaque que nos três últimos exemplos estamos calculando a função ϕ de números primos e peça a eles que verifiquem se há alguma regularidade nos resultados. É esperado que os alunos consigam verificar que para p primo, $\phi(p) = p - 1$.

Em seguida, apresente a eles a definição de ordem de um inteiro a módulo m, Definição 4.1 e o exemplo a seguir.

Exemplo 6.8. *Encontre a ordem de 3 módulo 5.*

Solução: Considerando as potências de 3 módulo 5, temos:

$$3^1 = 3 \equiv 3 \,(mod\, 5)$$
$$3^2 = 9 \equiv 4 \,(mod\, 5)$$
$$3^3 = 27 \equiv 2 \,(mod\, 5)$$
$$3^4 = 81 \equiv 1 \,(mod\, 5).$$

Note que 4 *é o menor expoente inteiro positivo pelo qual elevamos* 3 *e obtemos um número congruente a* 1 *módulo* 5. *Então, 4 é a ordem de* 3 *módulo* 5.

A partir da definição de ordem, apresente a definição de raiz primitiva módulo m, Definição 4.10 e o exemplo a seguir.

Exemplo 6.9. *Verifique se 2 é raiz primitiva módulo 3.*

Solução: Considerando as potências de 2 módulo 3, temos:

$$2^1 = 2 \equiv 2 \,(mod\, 3)$$
$$2^2 = 4 \equiv 1 \,(mod\, 3).$$

Note que 2 *é o menor expoente inteiro positivo pelo qual elevamos* 2 *e obtemos um número congruente a* 1 *módulo* 3. *Além disso,* $\phi(3) = 3 - 1 = 2$. *Então,* $ord_3 2 = \phi(3) = 2$. *Portanto,* 2 *é raiz primitiva módulo* 3.

Peça aos alunos que, em duplas, encontrem as raízes primitivas de 7, 10 e 13, utilizando a calculadora de restos para fazer os cálculos.

Explique aos alunos que a definição e raízes primitivas será essencial para que eles compreendam o conceito de logaritmo discreto, que será trabalhado a partir desse momento.

Relembre com os alunos as propriedades dos logaritmos de números reais.

1. $log_b 1 = 0$
2. $log_b b = 1$
3. $log_b (a \cdot c) = log_b a + log_b c$
4. $log_b a^n = n \cdot log_b a$

Apresente a definição de logaritmo discreto, Definição 5.1 e Definição 5.5. Para que eles compreendam a definição, apresente o exemplo a seguir.

Exemplo 6.10. *Sabendo que* 3 *é raiz primitiva módulo* 7*, determine:*

(a) $dlog_{3,7}(3)$

(b) $dlog_{3,7}(4)$

(c) $dlog_{3,7}(6)$

Solução:

(a) O $dlog_{3,7}(3)$ *é o expoente ao qual elevamos 3 para obter um número equivalente a 3 módulo 7. Como* $3^1 = 3 \equiv 3 \, (mod\, 7)$*, temos que* $dlog_{3,7}(3) = 1$*.*

(b) O $dlog_{3,7}(4)$ *é o expoente ao qual elevamos 3 para obter um número equivalente a 4 módulo 7. Como* $3^4 = 81 \equiv 4 \, (mod\, 7)$*, temos que* $dlog_{3,7}(4) = 4$*.*

(c) O $dlog_{3,7}(6)$ *é o expoente ao qual elevamos 3 para obter um número equivalente a 6 módulo 7. Como* $3^3 = 27 \equiv 6 \, (mod\, 7)$*, temos que* $dlog_{3,7}(6) = 3$

Explique aos alunos que se estivéssemos trabalhando com um número primo muito grande, encontrar o logaritmo discreto de um número também muito grande seria muito trabalhoso. Essa dificuldade também se estende para computadores e, por esse motivo, esse problema é conhecido como o *Problema do Logaritmo Discreto* e é base para o algoritmo criptográfico ElGamal, que será trabalhado na aula seguinte.

6.6.3 *Aula 3: O algoritmo criptográfico ElGamal*

Duração: 45 minutos.
Local de desenvolvimento da atividade: sala de informática.
Recursos necessários: lousa, giz, computadores com um *software* de planilhas eletrônicas instalado e projetor.

Inicie a aula apresentando aos alunos o funcionamento da troca de mensagens do algoritmo criptográfico ElGamal, Subseção 5.2.2. Faça o passo a passo dos Exemplos 5.11 e 5.12 com os alunos, utilizando a calculadora de módulo para realizar os cálculos.

Explique aos alunos que na aula seguinte eles irão trocar mensagens utilizando esse algoritmo. Para tanto, vamos fazer algumas adaptações na calculadora de módulo produzida na aula 1 para calcular os elementos do algoritmo ElGamal.

Para adaptar a calculadora para calcular y_j, seguimos os seguintes passos:

- Em outra planilha escolhemos as células para inserir as informações de p, α e x_j, além da célula que retornará o valor de y_j, como mostra a Figura 6.

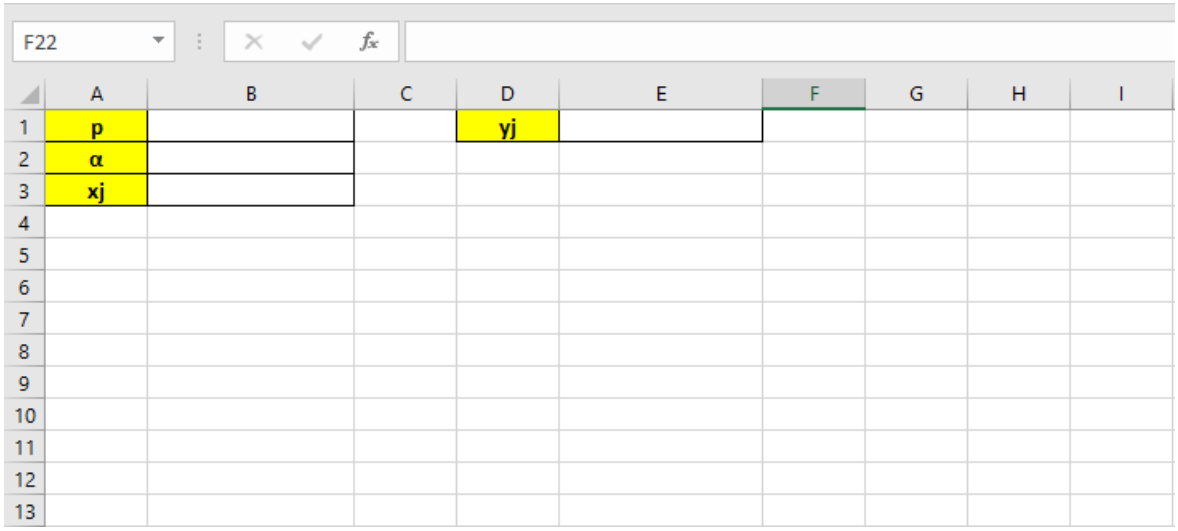


Figura 6: Adaptação da calculadora de módulo para calcular a chave pública y_j

- Na célula que retornará o valor de y_j, inserimos uma fórmula semelhante à utilizada na primeira planilha. Porém, o que estamos considerando como a aqui será α^{x_j}. Se inserirmos o valor de p na célula $B1$, o valor de α na célula $B2$ e o valor de x_j na célula $B3$, a fórmula que deverá ser inserida na célula que retornará o valor de y_j será:

$$= (((B2\hat{}B3)/B1) - INT((B2\hat{}B3)/B1)) * B1,$$

como mostra a Figura 7.

Feito isso, podemos testar a calculadora. Para tanto, vamos utilizar os valores presentes no Exemplo 5.11, como mostra a Figura 8.

Podemos fazer o mesmo para adaptar a calculadora para calcular c_1 e c_2, seguindo os seguintes passos:

- Em outra planilha escolhemos as células para inserir as informações de p, α, y_j, x_m e M, além das células que retornarão os valores de c_1 e c_2, como mostra a Figura 9.

- Na célula que retornará o valor de c_1, inserimos uma fórmula semelhante à utilizada nas outras planilhas. Porém, o que queremos calcular aqui é o resto da divisão de

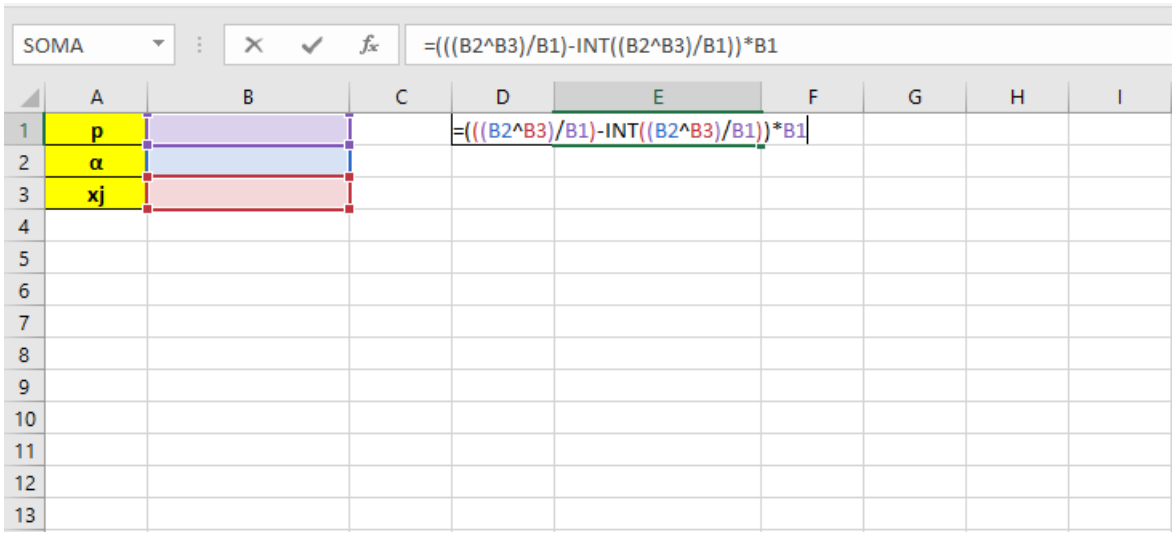


Figura 7: Fórmula da calculadora da chave pública y_j

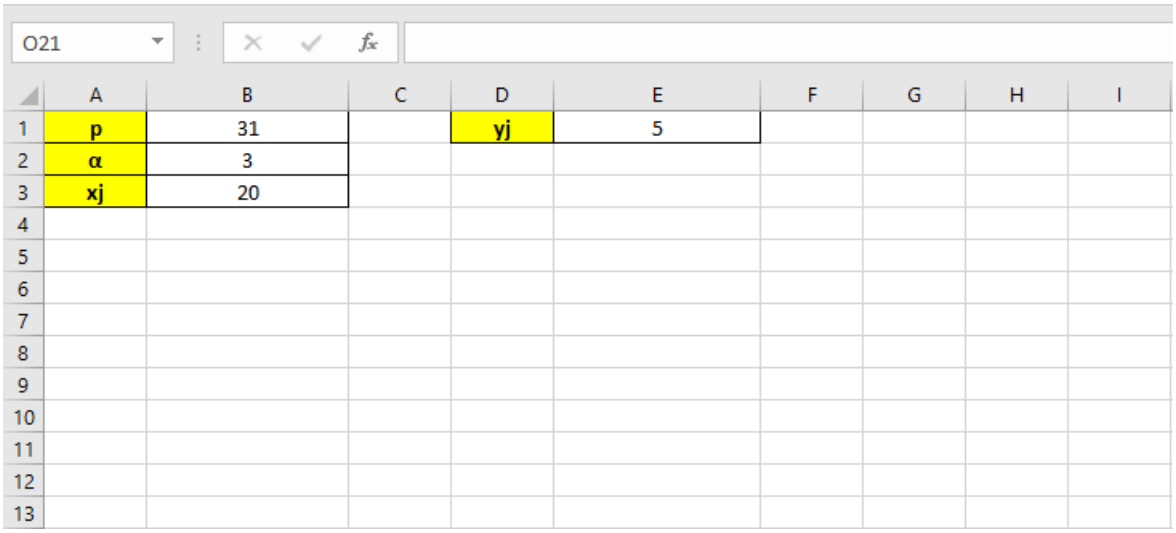


Figura 8: Teste da calculadora da chave pública y_j

α^{x_m} por p. Se inserirmos o valor de α na célula $B2$, o valor de x_m na célula $B4$ e o valor de p na célula $B1$, a fórmula que deverá ser inserida na célula que retornará o valor de c_1 será: $= (((B2\hat{}B4)/B1) - INT((B2\hat{}B4)/B1)) * B1)$, como mostra a Figura 10.

- Na célula que retornará o valor de c_2, inserimos uma fórmula semelhante à utilizada nas outras planilhas. Porém, o que queremos calcular aqui é o resto da divisão de $M \cdot y_j^{x_m}$ por p. Se inserirmos o valor de M na célula $B5$, o valor de y_j na célula $B3$, o valor de x_m na célula $B4$ e o valor de p na célula $B1$, a fórmula que deverá ser inserida na célula que retornará o valor de c_2 será:

$$= (((B5 * (B3\hat{}B4))/B1) - INT((B5 * (B3\hat{}B4))/B1)) * B1,$$

como mostra a Figura 11.

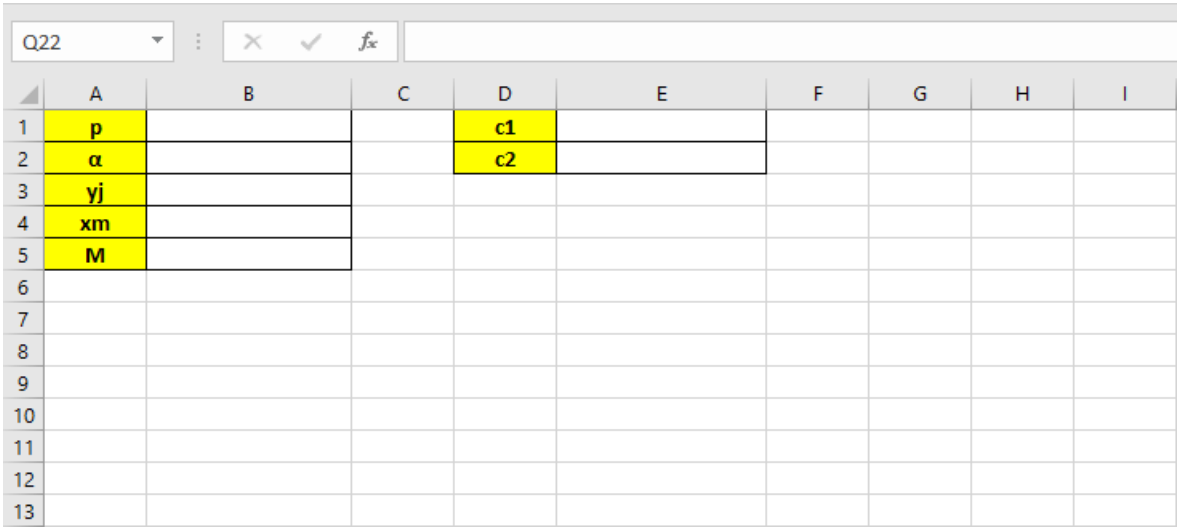


Figura 9: Adaptação da calculadora de módulo para calcular a mensagem criptografada (c_1, c_2)

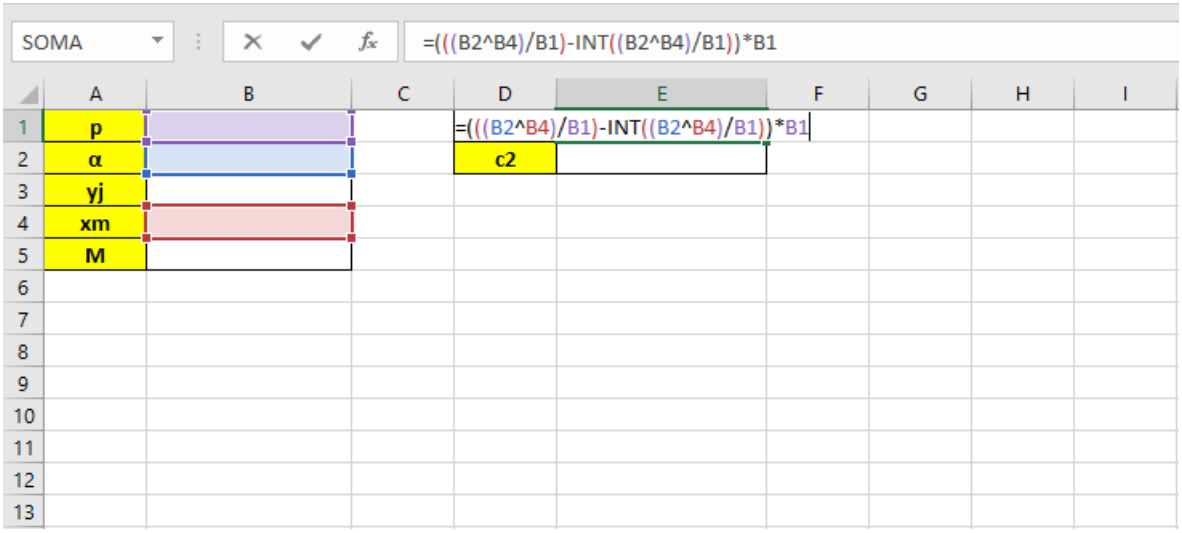


Figura 10: Fórmula da calculadora de c_1

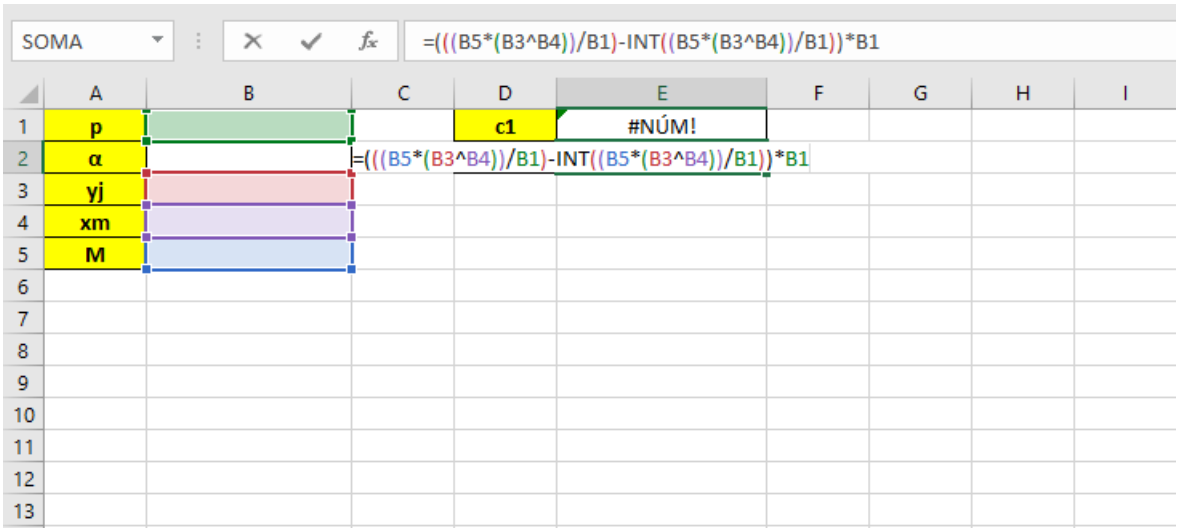


Figura 11: Fórmula da calculadora de c_2

Feito isso, podemos testar a calculadora. Para tanto, vamos, novamente, utilizar os valores presentes no Exemplo 5.11, como mostra a Figura 12.

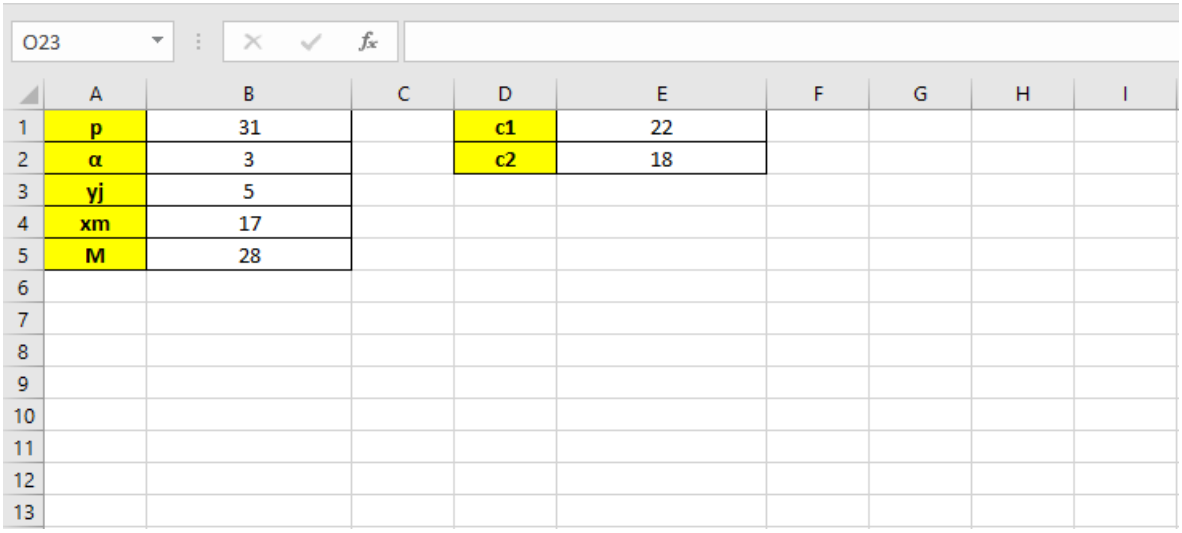


Figura 12: Teste da calculadora da mensagem criptografada (c_1, c_2)

Para adaptar a calculadora para descriptografar a mensagem M, seguimos os seguintes passos:

- Em outra planilha escolhemos as células para inserir as informações de p, x_j, c_1 e c_2. Além das células que retornarão os valores de $c_1^{p-1-x_j}$, $(y_j^{x_m})^{-1}$ e M, pois criaremos fórmulas para calcular os resultados auxiliares $c_1^{p-1-x_j}$ e $(y_j^{x_m})^{-1}$ para facilitar a escrita da fórmula para calcular M. A planilha ficará como mostra a Figura 13.

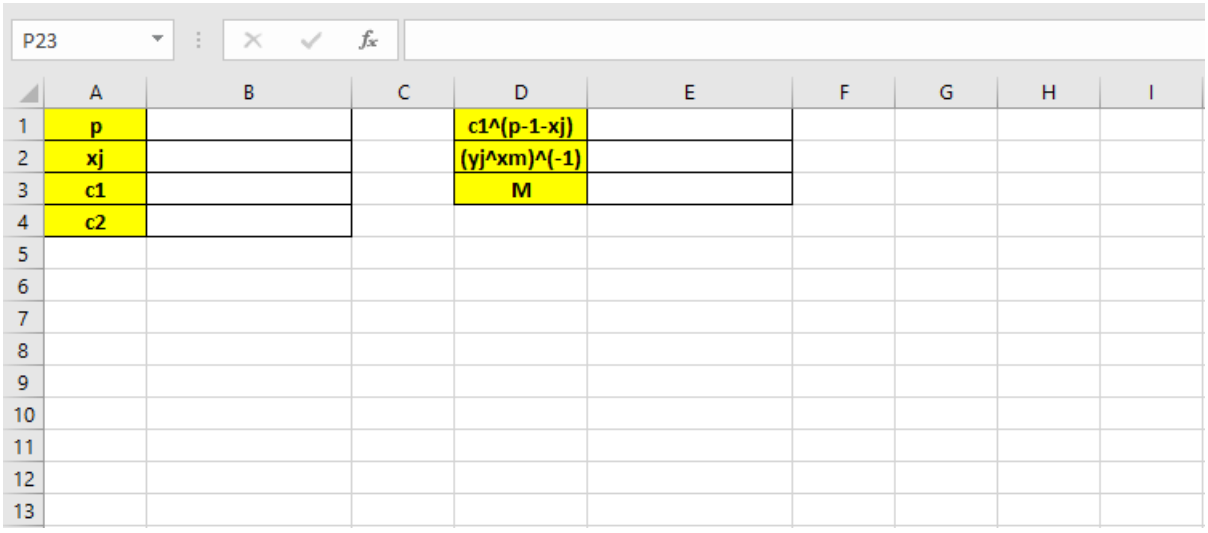


Figura 13: Adaptação da calculadora de módulo para descriptografar a mensagem M

- Se inserirmos o valor de c_1 na célula $B3$, o valor de x_j na célula $B2$ e o valor de p na célula $B1$, a fórmula que retornará o valor de $c_1^{(p-1-x_j)}$ será:

$$= B3\hat{}(B1 - 1 - B2),$$

como mostra a Figura 14.

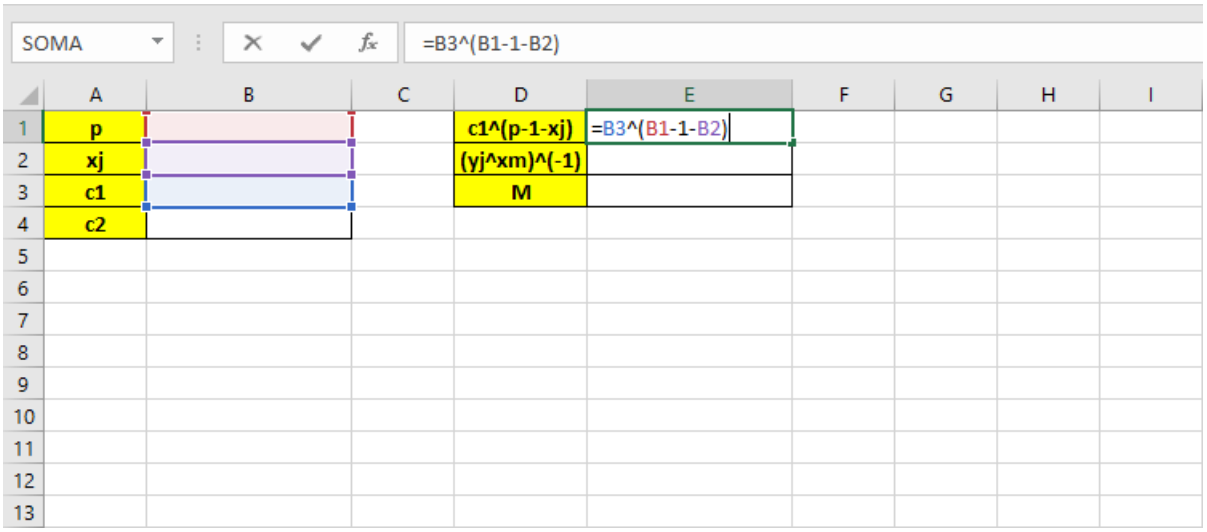


Figura 14: Calculadora de $c_1^{(p-1-x_j)}$

- Na célula que retornará o valor de $(y_j^{x_m})^{-1}$, inserimos uma fórmula que irá calcular o resto da divisão de $c_1^{(p-1-x_j)}$ por p. Se o valor de $c_1^{(p-1-x_j)}$ for retornado na célula $E1$ e o valor de p for inserido na célula $B1$, a fórmula que retornará o valor de $(y_j^{x_m})^{-1}$ será:

$$= ((E1/B1) - INT(E1/B1)) * B1,$$

como mostra a Figura 15.

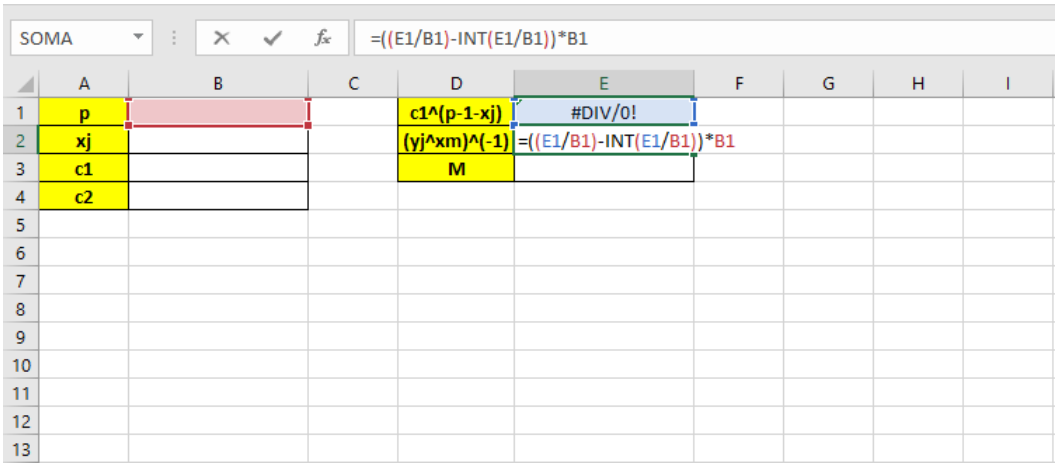


Figura 15: Calculadora de $(y_j^{x_m})^{-1}$

- Na célula que retornará o valor de M, inserimos a fórmula que irá calcular o resto da divisão de $c_2 \cdot (y_j^{x_m})^{-1}$ por p. Se o valor de c_2 for retornado na célula $B4$, o valor de $(y_j^{x_m})^{-1}$ for retornado na célula $E2$ e o valor de p for inserido na célula $B1$, a fórmula que retornará o valor de M será:

$$= (((B4 * E2)/B1) - INT((B4 * E2)/B1)) * B1,$$

como mostra a Figura 16.

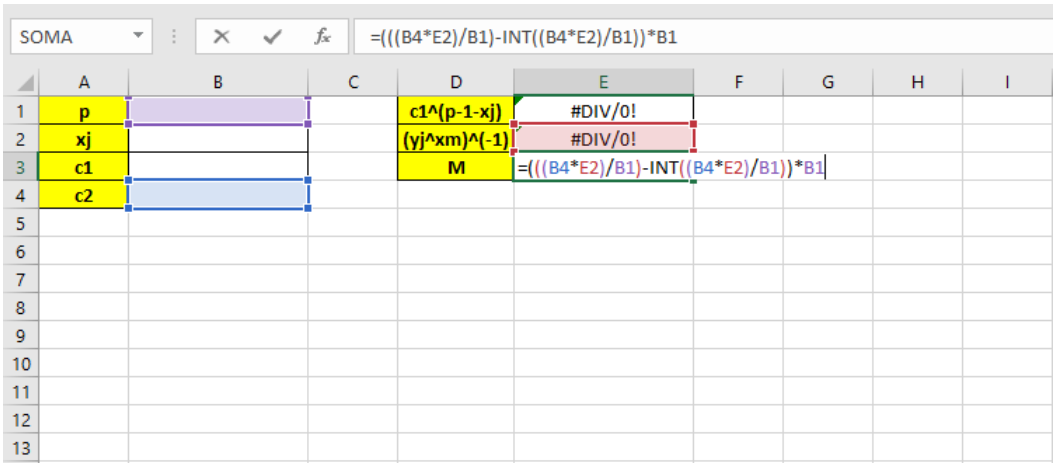


Figura 16: Calculadora de M

Feito isso, podemos testar a calculadora. Para tanto, vamos, novamente, utilizar os valores presentes no Exemplo 5.11, como mostra a Figura 17.

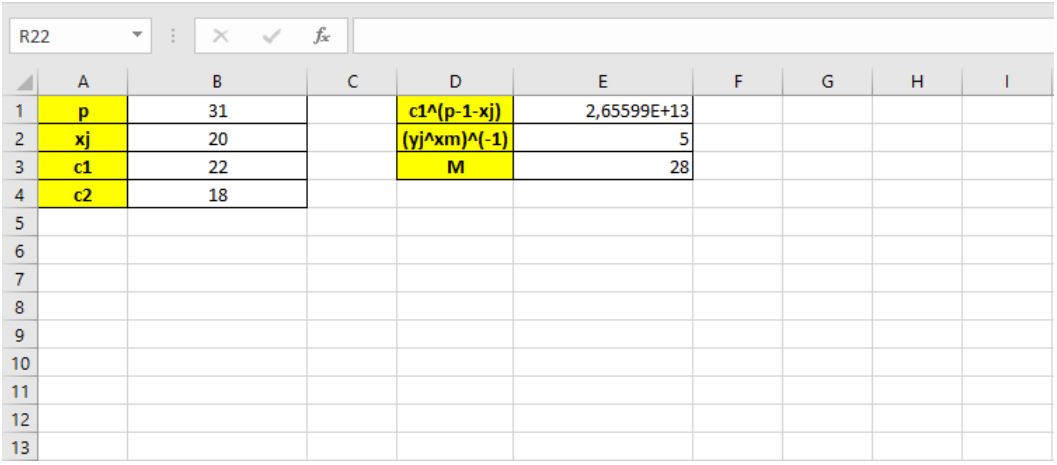


Figura 17: Teste da calculadora da mensagem M

Para finalizar, peça aos alunos que salvem os arquivos, pois na aula seguinte eles farão uso dos mesmos para criptografar e descriptografar mensagens.

6.6.4 *Aula 4: Troca de mensagens criptografadas*

Duração: 45 minutos.
Local de desenvolvimento da atividade: sala de informática.
Recursos necessários: lousa, giz, computadores com *software* de planilhas eletrônicas instalado e projetor.

Inicie a aula organizando os alunos em quatro grupos. Numere os grupos como $1, 2, 3$ e 4.

Explique aos grupos que eles irão trocar mensagens entre eles, utilizando o algoritmo criptográfico ElGamal. Para tanto, eles irão criar uma tabela que relaciona algumas frases escolhidas com os números indicados na tabela da Figura 18.

	7
	8
	9
	11
	14
	16
	21
	22

Figura 18: Tabela para codificar mensagens.

Feito isso, explique aos alunos que eles trabalharão com o número primo 23 e com 7, que é uma raiz primitiva módulo 23. Peça a cada grupo i que crie a sua chave pública $(23, 7, y_i)$, escolhendo uma chave secreta $x_i, 0 < x_i < 23$ e calculando $y_i \equiv \alpha^{x_i} \, (mod\, 23)$, utilizando a calculadora feita na aula anterior.

Exponha as chaves públicas de todos os grupos, anotando-as na lousa.

Peça aos grupos que escolham um grupo destinatário e envie a mensagem escolhida dentre as frases que eles criaram na tabela da Figura 18. A partir do código dessa frase e da chave pública do grupo destinatário, eles devem calcular a mensagem criptografada (c_1, c_2), utilizando a calculadora que eles produziram na aula anterior. Feito isso, eles devem enviar a mensagem criptografada para o grupo destinatário. Cuide para organizar o envio das mensagens de modo que todos os grupos enviem e recebam mensagens.

Exemplo 6.11. *Vamos supor que um grupo tenha codificado uma frase utilizando a* 4^a *linha da tabela. Então, a frase ficou codificada pelo número* 11*. Suponha, ainda, que este grupo tenha recebido a chave pública* $(23, 7, 5)$ *do seu destinatário e escolhido a chave*

secreta 12. *Com essas informações, o grupo poderá utilizar as calculadoras construídas e obter a mensagem criptografada* $(16, 14)$ *e envia essa mensagem para o grupo destinatário.*

Recebidas as mensagens, os grupos deverão descriptografá-las, utilizando a calculadora produzida na aula anterior.

Exemplo 6.12. *Ao receber a mensagem* $(16, 14)$*, o grupo destinatário coloca essas informações na calculadora de módulo e obtém o número* 11 *e descobre a frase que corresponde à mensagem.*

Durante os processos de criptografar e descriptografar as mensagens, caminhe pelos grupos, sanando dúvidas, e fazendo anotações a respeito da compreensão que os alunos apresentam sobre as etapas do algoritmo.

6.7 AVALIAÇÃO

Durante todas as etapas, procure observar a participação dos alunos e avaliar os conhecimentos adquiridos. Avalie a capacidade que os alunos apresentam de interpretar os conceitos novos e relacioná-los com conhecimentos prévios. Procure registrar os diálogos estabelecidos e recolher os registros de estratégias produzidos por eles.

7

CONCLUSÕES

Este trabalho teve por objetivo apresentar o conceito de raízes primitivas e sua importância para a definição de logaritmos discretos, que por sua vez apresenta grande relevância no desenvolvimento de algoritmos criptográficos, como o ElGamal. Com isso, procuramos ressaltar a importância do conjunto dos números inteiros e suas propriedades para o desenvolvimento da Criptografia, que é uma ciência cuja importância se faz cada vez maior diante do desenvolvimento da tecnologia relacionada à troca de mensagens.

Propomos uma sequência didática, cujo público alvo são alunos do Ensino Médio, a qual tem por objetivo apresentar aos alunos conceitos básicos de Teoria dos Números, o conceito de raízes primitivas, a definição de logaritmos discretos e a aplicação destes na Criptografia. A sequência proposta é uma sugestão para que o professor possa relacionar os logaritmos de números reais com os logaritmos discretos, levando o aluno a expandir a ideia de logaritmo e a compreender melhor suas propriedades. Além disso, essa sequência tem por objetivo estimular o raciocínio lógico; trabalhar com planilhas eletrônicas de uma forma diferente da forma como os alunos costumam trabalhar (apenas produzindo tabelas e gerando gráficos); levar os alunos a perceberem como a Matemática está presente nas tecnologias e sobretudo mostrar aos alunos a importância dos números inteiros e suas propriedades.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BRASIL. Ministério da Educação. *Base Nacional Comum Curricular Ensino Médio – BNCC*. Brasília, 2018.

http://basenacionalcomum.mec.gov.br/wp-content/uploads/2018/06/BNCC_EnsinoMedio_embaixa_site_110518.pdf

[2] COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. 2ª Edição. Coleção Matemática e Aplicações. Rio de Janeiro: IMPA, 2014.

[3] ELGAMAL, T. , *A public key cryptosystem and a signature scheme based on discrete logarithms*. IEEE Transactions on information theory, 1984, 473-481.

[4] EVES, H. *Introdução à história da matemática*. Campinas: Editora da Unicamp, 2004.

[5] FIGUEIREDO, L. M. *Introdução à Criptografia v.2*. Fundação CECIERJ. Rio de Janeiro: UFF/CEP-EB, 2010.

[6] GARCIA, A. LEQUAIN, Y. *Elementos de álgebra*. 6ª Edição. Projeto euclides. Rio de Janeiro: IMPA, 2013.

[7] HEFEZ, A. *Aritmética*. Coleção PROFMAT. Rio de Janeiro: SBM, 2014.

[8] MARTINEZ, F. B., MOREIRA, C. G., SALDANHA, N., TENGAN, E. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. 4ª Edição. Projeto Euclides. Rio de Janeiro: IMPA, 2015.

[9] MILIES, C. P., COELHO, S. P. *Números: uma introdução à matemática*. 3ª Edição. São Paulo: Edusp, 2003.

[10] RIBENBOIM, P. *Números Primos: Velhos Mistérios e Novos Records*. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 2014.

[11] SANTOS, J. P. O. *Introdução à Teoria dos Números*. 3ª Edição. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 2015.

[12] STALLINGS, W. *Criptografia e segurança de redes*. 4ª Edição. São Paulo: Pearson Prentice Hall, 2008.

[13] STINSON, D. R. *Cryptography theory and practice*. 3ª Edtion. Canada: Chapman & Hall/CRC - Taylor & Francis Group, 2006.