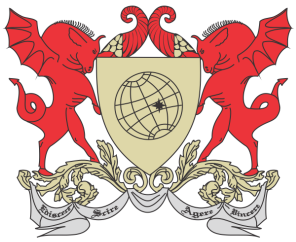
Universidade Federal de Viçosa

Dissertação de Mestrado



Júlio César Pereira

Números Primos e Criptografia RSA

Florestal
Minas Gerais – Brasil
2017

Júlio César Pereira

NÚMEROS PRIMOS E CRIPTOGRAFIA RSA

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título *Magister Scientiae*.

Florestal
Minas Gerais – Brasil
2017

Ficha catalográfica preparada pela Biblioteca da Universidade Federal de Viçosa - Câmpus Florestal

T
P436n
2017

Pereira, Júlio César, 1980-
Números primos e criptografia RSA / Júlio César Pereira. – Florestal, MG, 2017.
vi,63f. ; 29 cm.

Inclui apêndices.
Orientador: Danielle Franco Nicolau Lara.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.63.

1. Números Primos - Propriedades. 2. Teoria dos Números. 3. Criptografia. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-graduação Mestrado Profissional em Matemática em Rede Nacional. II. Título.

CDD 22 ed. 512.723

JÚLIO CÉSAR PEREIRA

NÚMEROS PRIMOS E CRIPTOGRAFIA RSA

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título *Magister Scientiae*.

APROVADA: 07 de agosto de 2017.

Jeanne do Carmo Amaral

Mehran Sabetti
(Coorientador)

Danielle Franco Nicolau Lara
(Orientadora)

Agradecimentos

A Deus, por sempre me dar força e fé pra continuar.

À minha esposa, Michele Pereira, pelo constante apoio e incentivo.

À minha orientadora, Profa. Dra. Danielle Franco Nicolau Lara, pelos ensinamentos transmitidos.

Ao Prof. Luis Alberto D'Afonseca pelo auxílio na elaboração da dissertação.

Aos meus professores do PROFMAT.

Aos meus colegas do PROFMAT, do meu polo e de outros polos, pela ajuda nos estudos.

Resumo

PEREIRA, Júlio César, M.Sc., Universidade Federal de Viçosa, agosto de 2017. **Números Primos e Criptografia RSA**. Orientadora: Danielle Franco Nicolau Lara. Coorientadores: Elisângela Aparecida de Oliveira e Mehran Sabeti.

Este trabalho apresenta uma revisão teórica de alguns conceitos da teoria dos números como o princípio da indução finita, o algoritmo da divisão Euclidiana, o teorema fundamental da aritmética, relações de equivalência, congruência módulo m, classes de equivalência e conjuntos quocientes. O objetivo principal é realizar um estudo das propriedades dos números primos, das propriedades da fatoração numérica, noções de máximo divisor comum e aritmética modular, apresentar aplicações práticas destes conceitos e uma aplicação da criptografia RSA. Para isso, é apresentado um estudo sistemas de equações lineares utilizando o teorema chinês do resto, que pode ser aplicado como um método de criptografia para partilhas de senhas. Por fim, é elaborada uma aplicação de criptografia para alunos de ensino médio.

Abstract

PEREIRA, Júlio César, M.Sc., Universidade Federal de Viçosa, August, 2017. **Prime Numbers and RSA Cryptography RSA**. Adviser: Danielle Franco Nicolau Lara. Co-advisers: Elisângela Aparecida de Oliveira and Mehran Sabeti.

The present study provides a theoretical review of some concepts of the theory of numbers such as the principle of finite induction, Euclidean division algorithm, fundamental theorem of arithmetic, equivalence relations, congruence modulo m, equivalence classes and quotient sets. The primary objective was to perform a study of the properties of prime numbers, properties of numerical factorization, notions of greatest common divisor and modular arithmetic and to present practical applications of these concepts and an application of RSA cryptography. To this end, we report a study of a system of linear equations using the Chinese remainder theorem, which can be applied as a cryptography method for password sharing. Lastly, a cryptography application was devised for high-school students.

Sumário

1

Introdução

O estudo da teoria dos números inteiros é feito desde as civilizações mais antigas, entretanto é na Grécia que a identificamos e a entendemos como é atualmente. Entre os problemas da teoria dos números que os gregos abordaram estão:

- O cálculo do máximo divisor comum entre dois números;
- A determinação dos números primos menores que um inteiro dado;
- A demonstração de que há um infinidade de números primos.

De acordo com COUTINHO (2005), estes e outros problemas são discutidos em detalhe num dos famosos livros de Matemática herdados da Grécia, os *Elementos* - livros VII, VIII e IX, escrito por Euclides por volta de 300 a. C. Dentre os vários matemáticos gregos que estudaram problemas da Teoria dos Números se destaca Diofanto, cuja obra trata principalmente da solução de equações indeterminadas com coeficientes inteiros.

Durante a Renascença, muitas obras de autores gregos foram redescobertas, editadas e publicadas na Europa. Foi nesta ocasião que o texto grego *Aritmética* de Diofanto foi publicado e caiu nas mãos do matemático francês Pierre de Fermat. Isso marcou o início do interesse desse matemático pela teoria dos números, que posteriormente se expressou em uma sequência de resultados importantes. Após sua morte em 1665, seu filho Samuel Fermat publicou a obra de seu pai e uma das publicações trouxe um famoso teorema conhecido como *Último Teorema de Fermat*:

"Se x, y, z e n são inteiros e $x^n + y^n = z^n$, onde $n \geq 3$, então $xyz = 0$"

O sucessor de Fermat, nesse campo, foi o matemático suíço Leonard Euler, nascido em 1707. Ao contrário de Fermat, que era magistrado por profissão, a Matemática era a principal ocupação de Euler. A obra de Fermat acabou chegando até Euler que começa a lê-la, aproximadamente em 1730. Nos anos seguintes, ele provaria e estenderia grande parte dos resultados enunciados por Fermat, resolvendo inclusive

uma questão proposta por ele:

Todos os números do tipo 2^{2^n} *são primos*

Através dos trabalhos de Euler, a teoria dos números se popularizou; mas o desenvolvimento sistemático da teoria só se iniciou com Gauss em sua obra *Disquisitiones Arithmeticae*, publicada em 1801. O enfoque atual da teoria teve início na obra de Gauss.

Fermat, Euler e Gauss são grandes expoentes da teoria dos números. Esta área tão fascinante da Matemática se caracteriza pela simplicidade de seus enunciados e da enorme dificuldade em demonstrá-los (COUTINHO, 2005).

Uma das grandes aplicações da Teoria dos Números é a implementação do sistema de criptografia. Segundo COUTINHO (2005), esse sistema estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la.

Sistemas de criptografia são usados desde os tempos antigos. Podemos citar, por exemplo, códigos como o de César, que usava mensagens criptografadas para se comunicar com seus soldados. No final da idade média, o movimento renascentista trouxe grandes novidades para a criptografia. Em 1452, Veneza criou uma organização especializada em lidar com segredos, cifras e decifrações; ela quebrava e criava cifras usadas pelo governo.

No século XIX, a tecnologia continuou a se desenvolver e as duas Grandes Guerras aumentaram ainda mais a importância da criptografia e da criptoanálise. Com o surgimento do computador, a criptografia se distancia dos conceitos tradicionais e entra numa nova era. A preocupação com a segurança de informações trocadas entre pessoas e instituições fica ainda maior com o advento da internet. Como é relativamente fácil interceptar mensagens enviadas por linha telefônica, torna-se necessário codificá-las, sempre que contenham informações sensíveis (COUTINHO, 2005). Assim, tornou-se necessário inventar códigos seguros que fossem difíceis de decifrar, mesmo com auxílio de computadores. Nesse contexto, foram criados códigos modernos de chave pública. Em um código de chave pública, saber codificar não implica saber decodificar. De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

A criptografia de chave simétrica, também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA. Já a criptografia de chaves assimétricas, também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA.

Por razões de segurança, o destinatário exige garantia de que a mensagem criptografada tenha sido originada no seu real remetente. Ou ainda, o remetente espera que sua mensagem criptografada chegue no verdadeiro destinatário sem que seja interceptada por um *hacker*, por exemplo. Assim, a mensagem deve ser *assinada*. A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz tê-la feito e que ela não foi alterada. Ela se baseia no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia tê-la feito. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

O mais conhecido dos métodos de chave pública é o RSA. Ele foi inventado em 1978 por Ronald L. Rivest, Adi Shamir e Leonard M. Adleman que, na época, trabalhavam no Massachussets Institute of Technology (M.I.T.). Este método é usado, por exemplo, no *Netscape*.

Por meio do uso da criptografia podemos proteger os dados sigilosos armazenados no computador, como arquivos de senhas e declaração de Imposto de Renda; criar uma área (partição) específica no computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas; proteger backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias; proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

Esta dissertação é uma continuação do meu trabalho de conclusão de curso (TCC) realizado na graduação sob orientação do professor José Carlos Souza Júnior e tem por finalidade aprofundar os conhecimentos matemáticos na Teoria dos Números e descrever algumas aplicações práticas. Apresenta um estudo das propriedades dos números primos e das propriedades da fatoração numérica, noções de máximo divisor comum e aritmética modular. O principal objetivo do trabalho é apresentar o método de criptografia RSA: sua implementação, viabilidade e segurança. A maior parte do conteúdo estudado se encontra nos trabalhos sobre a teoria dos números desenvolvidos pelos antigos gregos e por Fermat, Euler e Gauss.

Na revisão teórica, é abordado, primeiramente, o Princípio da Indução Finita e sua relação com o Princípio da Boa Ordem. Há também um estudo sobre o Algoritmo da Divisão Euclidiana. Em seguida, tratamos sobre máximo divisor comum e números primos, com suas propriedades fundamentais e o Teorema Fundamental da Aritmética. No capítulo seguinte, são abordadas as relações de equivalência, congruência módulo m, as classes de equivalência e os conjuntos quocientes. Apresentamos também a solução de sistemas de equações lineares, o chamado Algoritmo Chinês do Resto com uma aplicação a um método de criptografia para partilha de senhas. Por fim, apresentamos o sistema de criptografia RSA e uma aplicação desses conceitos para alunos do ensino médio.

2

Conceitos Preliminares

Este capítulo abordará alguns conceitos preliminares importantes para o entendimento do trabalho. Uma leitura mais ampla e profunda pode ser encontrada em Milies (2003) e Sampaio (2007).

2.1 Princípio da Indução Finita

Axioma 2.1 (Princípio da Boa Ordenação): *Todo subconjunto não vazio S de $\mathbb{Z}$ de elementos não negativos possui um elemento mínimo, ou seja, $\exists\ x_0 \in S$ tal que $x_0 \leq x\ \forall x \in S$.*

$\triangleright\triangleright\triangleright$ **Exemplo 2.1:** Usando o princípio da boa ordenação, mostre que $\sqrt{2}$ é irracional.

Solução: Suponha que $\sqrt{2} \in \mathbb{Q}$, neste caso, existem inteiros positivos a e b, tais que:

$$\sqrt{2} = \frac{a}{b} \ \Rightarrow\ a = b\sqrt{2}$$

Seja $A = \{m \in \mathbb{Z};\ m > 0 \text{ e } m\sqrt{2} \in \mathbb{Z}\}$.

Note que $A \neq \varnothing$, pois $b \in A$. Logo, pelo princípio da boa ordenação, A possui um menor elemento, digamos s.

Temos que s e $s\sqrt{2}$ são ambos inteiros positivos. Considere o inteiro $r = s\sqrt{2} - s$.

Note que r é um inteiro positivo, pois $\sqrt{2} - 1 > 0$. Além disso, $r\sqrt{2}$ também é um inteiro. De fato,

$$r\sqrt{2} = (s\sqrt{2} - s)\sqrt{2} = \underbrace{2s}_{\in\mathbb{Z}} - \underbrace{s\sqrt{2}}_{\in\mathbb{Z}} \in \mathbb{Z}$$

Mas $r = s\sqrt{2} - s = s(\sqrt{2} - 1) < s$, pois $\sqrt{2} - 1 < 1$.

Assim, $r \in A$ e é menor do que s. (Contradição)

Portanto, nossa suposição de que $\sqrt{2} \in \mathbb{Q}$ está errada. $\square$

Proposição 2.1 (Princípio da Indução Finita - Primeira Forma): Suponhamos que seja dada uma afirmação $P(n)$ dependendo de $n \in \mathbb{N}$ tal que:

(i) $P(0)$ é verdadeira (a sentença é válida para $n = 0$).

(ii) Para cada $k \in \mathbb{N}$, $P(k+1)$ é verdadeira sempre que $P(k)$ for verdadeira.

Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Demonstração: Seja S o conjunto dos inteiros $m \in \mathbb{N}$ tais que $P(m)$ seja falsa, e suponhamos que $S \neq \varnothing$. Pelo princípio da boa ordenação, existe um $x_0 \in S$ tal que $x_0 \leq m$, $\forall\ m \in S$. Como $P(0)$ é verdadeira por hipótese, temos que $0 \notin S$ e portanto $x_0 \geq 1$; mais ainda, como $x_0 - 1 \notin S$, temos que $P(x_0 - 1)$ é verdadeira. Agora, pela hipótese (ii), segue que $P(x_0) = P[(x_0 - 1) + 1]$ é verdadeira, o que é uma contradição. Logo $S = \varnothing$ e o resultado segue. ■

Proposição 2.2 (Princípio da Indução Finita - Segunda Forma): Suponhamos que seja dada uma afirmação $P(n)$ dependendo de $n \in \mathbb{N}$ tal que:

(i) $P(0)$ é verdadeira.

(ii) Para cada inteiro $m > 0$, $P(m)$ é verdadeira sempre que $P(k)$ for verdadeira para $0 \leq k < m$.

Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Demonstração: Seja S o conjunto dos inteiros $m \in \mathbb{N}$ tais que $P(m)$ seja falsa e suponhamos que S é não vazio. Então, pelo princípio da boa ordenação, existe um $x_0 \in S$ tal que $x_0 \leq x$, para todo $x \in S$, e pela hipótese (i) $x_0 > 0$. Como x_0 é o elemento mínimo de S, segue que $P(k)$ é verdadeira para todo k, $0 \leq k < x_0$, de forma que a hipótese (ii) nos leva a concluir que $P(x_0)$ é verdadeira, o que é uma contradição. Logo $S = \emptyset$ e o resultado segue. ■

⋆ Observação 2.1:Observe que as proposições 2.1 e 2.2 poderiam ser enunciadas a partir do inteiro 1 em vez de zero e nesse caso a hipótese (i) seria $P(1)$ é verdadeira. As mesmas demonstrações funcionam com as devidas modificações.

▷▷▷ **Exemplo 2.2:** Usando o princípio da indução finita, mostre que:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2},\ c\ n \geq 1.$$

Solução: Seja $P(n)$ a sentença: $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$. A sentença $P(1)$ estabelece que $1 = \frac{1\cdot(1+1)}{2}$, a qual é certamente válida.

Agora, assuma que $P(k)$ é verdadeira para algum $k \geq 1$, ou seja,

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}.$$

Vamos mostrar que $P(k+1)$ é verdadeira, isto é, que

$$1+2+3+\ldots+k+(k+1)=\frac{(k+1)(k+2)}{2}.$$

Temos que:

$$\begin{aligned}
1+2+\ldots+k+(k+1) &= (1+2+\ldots+k)+(k+1)\\
&\overset{HIP}{=} \frac{k(k+1)}{2}+(k+1)\\
&= (k+1)\left(\frac{k}{2}+1\right)\\
&= (k+1)\left(\frac{k+2}{2}\right)\\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Logo, $P(k+1)$ é verdadeira e pelo Princípio da Indução Finita, o resultado é válido para todo $n \geq 1$. □

▷▷▷ **Exemplo 2.3:** Usando o princípio da indução finita, mostre que $n^3 - n$ é múltiplo de 3, para todo $n \geq 0$.

Solução: Seja $P(n)$ a sentença: $n^3 - n$ é um múltiplo de 3. Temos que $P(0)$ é verdadeira pois $0^3 - 0 = 0 = 0 \cdot 3$.

Suponha que $P(k)$ é verdadeira para algum $k \geq 1$, ou seja, que $k^3 - k = 3 \cdot m$, para algum $m \in \mathbb{Z}$ e algum $k \geq 1$.

Então:

$$\begin{aligned}
(k+1)^3-(k+1) &= k^3+3k^2+3k+1-(k+1)\\
&= (k^3-k)+(3k^2+3k)\\
&\overset{HIP}{=} 3m+3(k^2+k)\\
&= 3\underbrace{(m+k^2+k)}_{\in\mathbb{Z}},
\end{aligned}$$

o qual é um múltiplo de 3 e assim, $P(k+1)$ é verdadeira. Logo, pelo Princípio da Indução Finita, concluímos que $P(n)$ é verdadeira para todo $n \geq 0$. □

▷▷▷ **Exemplo 2.4:** Mostre que o princípio da indução finita implica o princípio da boa ordenação.

Solução: Seja $U \subset \mathbb{N}$ tal que U não possui um menor elemento. Seja $P(n)$ a sentença: $n \notin U$. Vamos mostrar que $U = \varnothing$.

Note que $P(0)$ é verdadeira, uma vez que $0 \notin U$, caso contrário ele seria claramente o menor elemento de U.

Agora, suponha que $P(k)$ é verdadeira para algum $k \in \mathbb{N}$, ou seja, $k \notin U$.

Segue que para todo inteiro m tal que $0 \leq m \leq k$, temos que $m \notin U$. De fato,

se tivermos valores entre 0 e k pertencendo à U, então o menor dentre estes valores seria o menor elemento de U, contrariando a nossa hipótese. Conseqüentemente, $k+1$ também não poderá pertencer à U, pois caso contrário, este passaria a ser o menor elemento de U. Assim, $P(k+1)$ é verdadeira.

Logo, pelo Princípio da Indução Finita, temos que $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, ou seja, $U = \varnothing$.

Portanto, se $U \subset \mathbb{N}$ e $U \neq \varnothing$, então U possui um menor elemento. □

⋆ Observação 2.2:A proposição 2.1 e o exemplo 2.4 estabelecem que o princípio da indução finita e o princípio da boa ordenação são equivalentes.

2.2 Algoritmo da Divisão

Definição 2.1 (Divisibilidade): Dizemos que um inteiro a divide um inteiro b quando existe um inteiro m, tal que $b = a \cdot m$. Notação: $a|b$.

Neste caso, dizemos também que:

- a é um divisor de b;
- a é um fator de b;
- b é um múltiplo de a.

No caso em que $a \neq 0$, dizemos ainda que:

- b é divisível por a;
- $m = \frac{b}{a}$ é o quociente de b por a.

⋆ Observação 2.3:Quando a não divide b, escrevemos $a \nmid b$.

▷▷▷ **Exemplo 2.5:** Temos que 7 divide 161, uma vez que existe um inteiro, que no caso é o 23, tal que $161 = 7 \cdot 23$.

▷▷▷ **Exemplo 2.6:** Os divisores de 12 são: $1, 2, 3, 4, 6, 12, -1, -2, -3, -4, -6, -12$.

▷▷▷ **Exemplo 2.7:** Os divisores de 23 são: $1, 23, -1, -23$.

Proposição 2.3: Se a, b e c são inteiros, tais que $a|b$ e $b|c$, então $a|c$.

Demonstração: Como $a|b$ e $b|c$, então existem inteiros m e n tais que $b = a \cdot m$ e $c = b \cdot n$. Logo, $c = (a \cdot m) \cdot n = a \cdot \underbrace{(m \cdot n)}_{\in \mathbb{Z}}$ e, portanto, $a|c$ ■

PROPOSIÇÃO 2.4: Se a, b e c são inteiros, tais que $a|b$ e $a|c$, então para todo $m, n \in \mathbb{Z}$ temos que $a|(mb + nc)$.

Demonstração: Como $a|b$ e $a|c$, então existem inteiros e e f tais que $b = a \cdot e$ e $c = a \cdot f$. Logo, $m \cdot b + n \cdot c = m \cdot (a \cdot e) + n \cdot (a \cdot f) = a \cdot (me + nf)$. Portanto, $a|(mb + nc)$. ■

▷▷▷ **Exemplo 2.8:** $3|21$ e $3|33$, logo $3|(5 \cdot 21 - 3 \cdot 33)$, isto é, $3|6$.

TEOREMA 2.1 (ALGORITMO DA DIVISÃO EUCLIDIANA EM $\mathbb{N}$): Para cada número natural n e cada inteiro positivo d, $d \neq 0$, existem números naturais q (quociente) e r (resto), satisfazendo:

$$n = d \cdot q + r \text{ e } 0 \leq r < d.$$

Além disso, os naturais q e r, satisfazendo as condições apresentadas, são únicos.

Demonstração: (EXISTÊNCIA) Mostraremos a existência dos naturais q e r, por indução sobre n. Provaremos que, fixado um inteiro positivo d, para cada número natural n, existem q e r nas condições enunciadas.

Se $n = 0$, basta tomar $q = r = 0$.

Seja k um número natural e suponhamos que existam q e r satisfazendo:

$$k = d \cdot q + r \text{ e } 0 \leq r < d.$$

Então, $k + 1 = d \cdot q + (r + 1)$. Como $0 \leq r < d$, temos que $r + 1 < d + 1$, ou seja, $r + 1 \leq d$.

Se $r + 1 < d$, tomamos $q' = q$ e $r' = r + 1$ e teremos:

$$k + 1 = d \cdot q' + r', \text{ com } 0 \leq r' < d.$$

Se $r + 1 = d$, então:

$$\begin{aligned} k + 1 &= d \cdot q + d \\ &= d \cdot \underbrace{(q + 1)}_{q''} + \underbrace{0}_{r''}, \end{aligned}$$

tomando $q'' = q + 1$ e $r'' = 0$, teremos $k + 1 = d \cdot q'' + r''$.

Portanto, pelo princípio da indução finita, para cada $n \in \mathbb{N}$, existem q e r satisfazendo:

$$n = d \cdot q + r, \text{ com } 0 \leq r < d.$$

(UNICIDADE) Suponhamos que existam naturais q_1, q_2, r_1 e r_2 tais que:

- $n = q_1 \cdot d + r_1 = q_2 \cdot d + r_2$;
- $0 \leq r_1 < d$, $0 \leq r_2 < d$.

Então, $(q_1 - q_2)d = r_2 - r_1$. Daí, $|q_1 - q_2| \cdot |d| = |r_2 - r_1|$. $(*)$
Como $0 \leq r_1 < d$ e $0 \leq r_2 < d$, segue que:

$$\begin{aligned} 0 &\leq r_1 < d \\ -r_2 &\leq r_1 - r_2 < d - r_2 \\ -d < -r_2 &\leq r_1 - r_2 < d - r_2 \\ -d &< r_1 - r_2 < d - r_2 < d \\ 0 &\leq |r_1 - r_2| < d. \qquad (**) \end{aligned}$$

De $(*)$ e $(**)$ resulta que $|q_1 - q_2| \cdot |d| < |d|$ e, então, $|q_1 - q_2| < 1$.
Sendo $0 \leq |q_1 - q_2| < 1$, como não existem inteiros x com $0 < x < 1$, temos necessariamente que $|q_1 - q_2| = 0$, ou seja, $q_1 = q_2$ e, por $(*)$', $r_1 = r_2$.
Logo o quociente e o resto em uma divisão euclidiana são determinados de maneira única. ■

⋆ Observação 2.4:No próximo teorema, estenderemos o resultado acima para os números inteiros.

Teorema 2.2 (Algoritmo da Divisão em $\mathbb{Z}$): Se a e b são números inteiros e $b \neq 0$, então existem inteiros q e r tais que:

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

Os inteiros q e r, nas condições acima, são únicos.

Demonstração: (EXISTÊNCIA)

1. Caso $b > 0$:

   Se $a \geq 0$, pelo teorema 2.1, existem números naturais q e r satisfazendo:

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

   Se $a < 0$, então $|a| > 0$. Novamente pelo Teorema 2.1, existem naturais q e r satisfazendo:

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

   Como $|a| = -a$, temos então:

   $$\begin{aligned} -a &= b \cdot q + r,\ 0 < r < b \\ a &= b \cdot (-q) + (-r),\ -b < -r < 0 \end{aligned}$$

Se $r = 0$, temos $a = b \cdot (-q) + 0$, sendo $-q$ e 0 o quociente e o resto da divisão de a por b, respectivamente.

Se $r > 0$, temos:

$$\begin{aligned} a &= b \cdot (-q) + (-r) \\ a &= b \cdot (-q) - b + b - r \\ a &= b \cdot (-q - 1) + (b - r). \end{aligned}$$

Como $0 < r < b$, temos que $-b < -r < 0$ e, então somando b aos três membros desta última igualdade, obtemos $0 < b - r < b$.

Fazendo $q' = -q - 1$ e $r' = b - r$, temos:

$$a = b \cdot q' + r', \text{ com } 0 < r' < b.$$

2. Caso $b < 0$:

   Se $b < 0$, então $|b| > 0$. Pelo caso anterior, temos que existem números inteiro q e r tais que:

   $$a = |b| \cdot q + r, \ 0 \leq r < |b|.$$

   Como $|b| = -b$, temos então:

   $$\begin{aligned} a &= -b \cdot q + r, \ 0 \leq r < |b| \\ &= b \cdot (-q) + r, \ 0 \leq r < |b| \end{aligned}$$

   tal que $-q$ e r são quociente e resto da divisão de a por b.

(UNICIDADE) Para demonstrar a unicidade do quociente q e do resto r, vamos supor que seja possível escrever

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2,$$

com q_1, q_2, r_1 e r_2 inteiros, além de $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$.

Mostraremos que necessariamente $q_1 = q_2$ e $r_1 = r_2$.

A partir da igualdade $b \cdot q_1 + r_1 = b \cdot q_2 + r_2$, obtemos:

$$0 = b \cdot (q_1 - q_2) + (r_1 - r_2), \text{ ou, equivalentemente, } (r_2 - r_1) = b \cdot (q_1 - q_2).$$

Logo, b divide $r_2 - r_1$ e, consequentemente, b divide $|r_2 - r_1|$. $\quad (*)$

Por outro lado, como $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$, segue que $-|b| < r_2 - r_1 < |b|$ e portanto, $|r_2 - r_1| < |b|$. $\quad (**)$

De $(*)$ segue que $|r_2 - r_1| = b \cdot m$, para algum $m \in \mathbb{Z}$. Logo, $m = \frac{|r_2 - r_1|}{b}$. A partir de $(**)$ concluímos que m resulta em uma fração própria (numerador menor que o denominado), assim $m \in \mathbb{Z} \Leftrightarrow |r_2 - r_1| = 0$, ou seja, $r_2 - r_1 = 0 \Rightarrow r_2 = r_1$ e, consequentemente, $q_1 - q_2 = 0$. Segue portanto, a unicidade $q_1 = q_2$ e $r_1 = r_2$. ■

▷▷▷ **Exemplo 2.9:** Na divisão de 47 por -5, temos:

$$\begin{aligned} 47 &= 9 \cdot 5 + 2 \\ \therefore\ 47 &= (-9) \cdot (-5) + \underbrace{2}_{resto} \end{aligned}$$

Observe que $0 \leq resto < |-5|$.

▷▷▷ **Exemplo 2.10:** Na divisão de -17 por 7, temos:

$$\begin{aligned} 17 &= 2 \cdot 7 + 3 \\ 17 &= 3 \cdot 7 - 4 \\ \therefore\ -17 &= (-3) \cdot (7) + \underbrace{4}_{resto} \end{aligned}$$

Note que $0 \leq resto < |7|$.

2.3 Máximo Divisor Comum

O maior inteiro positivo que divide, simultaneamente, dois ou mais números inteiros é chamado máximo divisor comum. Nessa seção, será formalizado esse conceito bem como algumas proposições e propriedades que o cercam.

Proposição 2.5: Se a e b são números inteiros, em que $b \neq 0$ e $a|b$, então $|a| \leq |b|$.

Demonstração: Como $a|b$ e $b \neq 0$, então existe um inteiro $c \neq 0$ tal que $b = a \cdot c$. Logo, $|c| \geq 1$ e, portanto,

$$|a| \leq |a| \cdot |c| = |a \cdot c| = |b|.$$

■

Definição 2.2 (Máximo Divisor Comum): O Máximo Divisor Comum de dois inteiros a e b (a ou b diferente de zero), denotado por (a,b) ou $mdc(a,b)$, é um inteiro d satisfazendo as seguintes condições:

(i) $d > 0$;

(ii) $d|a$ e $d|b$ (consequentemente d divide $|a|$ e d divide $|b|$);

(iii) Se $k \in \mathbb{Z}$ é tal que $k|a$ e $k|b$, então $k \leq d$.

Em outras palavras, temos que se $d = (a,b)$, então d é o maior inteiro que divide a e b.

⋆ Observação 2.5:$(a,b) = (|a|,|b|)$

TEOREMA 2.3: Sejam $a,b \in \mathbb{Z}$, com $a \neq 0$. Se $a|b$, então $(a,b) = |a|$.

Demonstração: Observe que $|a|$ satisfaz as seguintes condições:

(i) $|a| > 0$, pois $a \neq 0$.

(ii) Claramente $|a|$ divide a. Como por hipótese $a|b$, é imediato que $|a|$ divide b.

(iii) Suponhamos que existe um inteiro k tal que $k|a$ e $k|b$. Como $k|a$ segue da Proposição 2.5 que $|k| \leq |a|$, consequentemente, $k \leq |a|$.

Logo, $(a,b) = |a|$. ■

TEOREMA 2.4: Sejam $a,b \in \mathbb{Z}$, em que $b > 0$. Se $a = b \cdot q + r$, tal que $q, r \in \mathbb{Z}$ e $0 \leq r < b$, então $(a,b) = (b,r)$.

Demonstração: Seja $d = (a,b)$. Mostraremos que $d = (b,r)$. Temos que:

(i) $d > 0$, pois $d = (a,b)$.

(ii) Sabemos que $d|b$ e $d|a$. Então, segue da Proposição 2.4, que $d|(a - b \cdot q)$, ou seja, $d|r$. Logo, $d|b$ e $d|r$.

(iii) Seja $k \in \mathbb{Z}$ tal que $k|r$ e $k|b$. Segue da Proposição 2.4, que $k|(b \cdot q + r) \Rightarrow k|a$.

Assim, $k|a$ e $k|b$. Como $d = (a,b)$, $k \leq d$.

Portanto, $d = (b,r)$. ■

▷▷▷ **Exemplo 2.11:** (Método Prático para Encontrar o M.D.C.) Encontre o máximo divisor comum entre:

(a) 28 e -6.

Solução: Segue da observação 2.5 que $(28,-6) = (28,6)$. Como $28 = 6 \cdot 4 + \underbrace{4}_{resto}$, segue do Teorema 2.4 que $(28,6) = (6,4)$.

Novamente pelo algoritmo da divisão, temos $6 = 4 \cdot 1 + \underbrace{2}_{resto}$. Assim, do Teorema 2.4 concluímos que $(6,4) = (4,2)$.

Como $2|4$, segue do Teorema 2.3 que $(4,2) = 2$.

Portanto, $(28,-6) = 2$.

Podemos esquematizar este raciocínio através do seguinte método prático:

Fazendo a divisão de 28 por 6, obtemos quociente igual a 4 e resto igual a 4:

	4			quocientes
28	6			
	4			restos

Na sequência, fazemos a divisão de 6 pelo resto obtido:

	4			quocientes
28	6	4		
	4 ↗			restos

Na divisão de 6 por quatro, obtemos quociente igual a 1 e resto igual a 2:

	4	1		quocientes
28	6	4		
	4	2		restos

Na sequência, fazemos a divisão de 4 por 2 (atual resto):

	4	1		quocientes
28	6	4	2	
	4	2 ↗		restos

Finalmente, fazendo a divisão de 4 por 2, obtemos quociente igual a 2 e resto igual a zero.

	4	1	2	quocientes
28	6	4	2	
	4	2	0	restos

Assim, conforme o raciocínio descrito anteriormente, concluímos que $(28, 6) = 2$.

	4	1	2	quocientes
28	6	4	$2_{//}$ (Resposta!)	
	4	2	0	restos

□

(b) 45 e 12.

Solução: Fazendo pelo método prático, obtemos a seguinte tabela:

	3	1	3	quocientes
45	12	9	$3_{//}$ (Resposta!)	
	9	3	0	restos

Portanto (45,12) = 3. □

(c) 45 e 15.

Solução: Como 15|45, segue do Teorema 2.3 que (45,15) = 15. □

(d) 41 e 12.

Solução: Fazendo pelo método prático, obtemos a seguinte tabela:

	3	2	2	2	quocientes
41	12	5	2	$1_{//}$ (Resposta!)	
	5	2	1	0	restos

Portanto (41,12) = 1. □

Definição 2.3 (Primos entre si): Dois inteiros a e b são ditos primos entre si, se $(a,b) = 1$.

⋆ Observação 2.6:No Exemplo 2.11 (d), observamos que os números 41 e 12 são primos entre si.

Teorema 2.5 (Teorema de Bezout): Para quaisquer inteiros a e b ($a \neq 0$ ou $b \neq 0$), existem inteiros x_0 e y_0 tais que $d = a \cdot x_0 + b \cdot y_0$ é o máximo divisor comum de a e b.

Demonstração:

1. Caso $a = 0$ e $b \neq 0$.

   Como $|b|$ é o maior inteiro que divide simultaneamente 0 e b, segue que $(0,b) = |b|$. Nesse caso, basta tomar $x_0 = 0$ e $y_0 = \pm 1$ (dependendo do sinal de b), que a expressão $|b| = a \cdot x_0 + b \cdot y_0$ é satisfeita.

2. Caso $a \neq 0$ e $b = 0$. É análogo ao anterior.

3. Caso $a \neq 0$ e $b \neq 0$. Levando em conta a última observação acima, podemos nos ater ao caso em que $a > 0$ e $b > 0$.

   Considere o conjunto

   $$L = \{w \in \mathbb{Z};\ w > 0 \text{ e } w = ax + by,\ \text{com } x,y \in \mathbb{Z}\}$$

   Note que $L \neq \varnothing$, pois $a + b \in L$ $(x = y = 1)$.

   Pelo Princípio da Boa Ordenação, L possui um menor elemento, digamos d.

   Assim, $d = a \cdot x_0 + b \cdot y_0$, para convenientes $x_0, y_0 \in \mathbb{Z}$. Mostraremos que $d = (a,b)$. De fato,

   (i) $d > 0$ por pertencer a L.

(ii) $d|a$ pois, pelo algoritmo da divisão, temos que

$$a = q \cdot d + r, \text{ com } q, r \in \mathbb{Z} \text{ e } 0 \leq r < d.$$

Se $r \neq 0$ (resta-nos apenas a opção $r > 0$), então:

$$\begin{aligned} r &= a - q \cdot d \\ &= a - q \cdot (a \cdot x_0 + b \cdot y_0) \\ &= (1 - q \cdot x_0) \cdot a - (y_0 \cdot q) \cdot b \end{aligned}$$

Assim, $0 < r < d$ e $r \in L$, o que contraria o fato de $d \in L$ ser mínimo. Logo, $r = 0$ e $d|a$.

De maneira analoga, temos que $d|b$.

(iii) Se $k|a$ e $k|b$, para algum $k \in \mathbb{Z}$, então pela Proposição 2.4, k divide qualquer combinação linear de a e b, em particular, $k|(a \cdot x_0 + b \cdot y_0)$, ou seja, $k|d$. Portanto, pela Proposição 2.5, temos que $|k| \leq |d| = d$, pois $d > 0$, consequentemente, $k \leq d$.

Portanto, $d = (a,b)$. ■

Proposição 2.6 (Caracterização Alternativa do M.D.C.): Sejam a e b dois inteiros ($a \neq 0$ ou $b \neq 0$), então:

$$d = (a,b) \Leftrightarrow \begin{cases} (i)\ d > 0 \\ (ii)\ d|a \text{ e } d|b \\ (iii) \text{ para todo } k \in \mathbb{Z}, \text{ se } k|a \text{ e } k|b, \text{ então } k|d \end{cases}$$

Demonstração:

($\Rightarrow$) Observe que (i) e (ii) já são propriedades estabelecidas do mdc. Assim, só nos resta mostrar que $d = (a,b)$ satisfaz a condição (iii).

Pelo Teorema 2.5, $d = x_0 \cdot a + y_0 \cdot b$ para certos inteiros x_0 e y_0. Logo, se $k \in \mathbb{Z}$ é tal que $k|a$ e $k|b$, então pela Proposição 2.4, temos que $k|(a \cdot x_0 + b \cdot y_0)$, ou seja, $k|d$.

($\Leftarrow$) Seja d um inteiro satisfazendo $(i), (ii)$ e (iii). As condições (i) e (ii) são comuns à Definição 2.2 de máximo divisor comum. Pela condição (iii), se k é um inteiro tal que $k|a$ e $k|b$, então $k|d$. Como $d > 0$, segue da Proposição 2.5 que $k \leq d$. Portanto, conforme a Definição 2.2, $d = (a,b)$. ■

Teorema 2.6: Se a e b são inteiros primos entre si e $a|(b \cdot c)$, então $a|c$.

Demonstração: Como a e b são primos entre si, $d = (a,b) = 1$. Pelo Teorema 2.5, temos que existem $x_0, y_0 \in \mathbb{Z}$, tais que $a \cdot x_0 + b \cdot y_0 = 1$. Ou seja, $a \cdot c \cdot x_0 + b \cdot c \cdot y_0 = c$.

Como $a|(a \cdot c)$ e por hipótese, $a|(b \cdot c)$, segue da Proposição 2.4 que $a|(acx_0 + bcy_0)$, ou seja, $a|c$. ■

2.4 Números Primos

Definição 2.4 (Números Primos): Um número inteiro p é chamado número primo se as seguintes condições se verificam:

(i) $p \neq 0$;

(ii) $p \neq \pm 1$;

(iii) Os únicos divisores de p são ± 1 e $\pm p$.

Proposição 2.7: Sejam p e q primos distintos e seja $a \in \mathbb{Z}$.

(i) Se $q \mid ap$ então $q \mid a$;

(ii) Se $p \mid a$ e $q \mid a$ então $pq \mid a$.

Demonstração:

(i) Por hipótese, sabemos que $mcd(p,q) = 1$. Assim, pelo Teorema 2.5 existem inteiros x_0 e y_0 tais que

$$x_0 \cdot p + y_0 \cdot q = 1$$

Multiplicando ambos os lados dessa igualdade por a, temos:

$$x_0 \cdot pa + y_0 \cdot qa = a$$

Note que $y_0 \cdot qa$ é divisível por q. Mas $x_0 \cdot pa$ também é divisível por q pois, por hipótese, q divide ap. Assim, $x_0 \cdot pa + y_0 \cdot qa$ é divisível por q. Portanto, $q \mid a$.

(ii) Como $p \mid a$, temos que $a = pt$ para algum inteiro t. Como $q \mid a = pt$ e $mcd(p,q) = 1$, segue de (i) que $q \mid t$. Assim $t = qk$, para algum inteiro k. Logo, $a = pt = p(qk) = (pq)k$ e portanto $pq \mid a$.

■

Lema 2.1 (Lema de Euclides): Sejam $a, b, p \in \mathbb{Z}$, tal que p é primo e $p|(a \cdot b)$, então $p|a$ ou $p|b$.

Demonstração: Temos que p pode dividir a e b ou pode não dividir a ou b. No primeiro caso, o Lema está provado. Suponhamos que $p \nmid a$. Mostraremos que $p|b$. Se p não divide a, então $-p$ também não é divisor de a. Como os divisores de p são apenas ± 1 e $\pm p$, então os divisores comuns de p e a são apenas ± 1. Logo, $(a,p) = 1$ e, pelo Teorema 2.5, existem $x_0, y_0 \in \mathbb{Z}$, tais que

$$\begin{aligned} p \cdot x_0 + a \cdot y_0 &= 1. \\ p \cdot b \cdot x_0 + a \cdot b \cdot y_0 &= b. \end{aligned}$$

Como $p|(p \cdot b)$ e por hipótese $p|(a \cdot b)$, segue da Proposição 2.4 que $p|(p \cdot b \cdot x_0 + a \cdot b \cdot y_0)$, ou seja, $p|b$. ■

⋆ Observação 2.7:A recíproca do Lema 2.1 também é verdadeira. Sejam $a, b, p \in \mathbb{Z}$ tal que p é primo, se $p|a$ ou $p|b$, então $p|(a \cdot b)$.

Um generalização do Lema de Euclides é o seguinte Lema:

Lema 2.2: Sejam $p, a_1, a_2, \ldots a_n \in \mathbb{Z}$, com $n \geq 2$ e p primo. Se $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_n)$, então $p|a_i$ para algum índice i, $i \in \{1, 2, \ldots, n\}$.

Demonstração: Mostraremos por indução sobre n. Se $n = 2$, então o resultado segue do Lema 2.1. Seja k um inteiro, com $k \geq 2$, e suponhamos que o resultado seja verdadeiro para $n = k$, ou seja, suponhamos que se p é primo e p divide um produto de k números inteiros, então p divide ao menos um dos fatores.

Consideremos agora, um produto de $k+1$ inteiros $a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot a_{k+1}$ e suponhamos que $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot a_{k+1})$. Então, $p|[(a_1 \cdot a_2 \cdot \ldots \cdot a_k) \cdot a_{k+1}]$.

Pelo Lema 2.1, $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_k)$ ou $p|a_{k+1}$. Assim, pela hipótese de indução, $p|a_j$ para algum $j \in \{1, 2, \ldots, k\}$ ou $p|a_{k+1}$ e desta forma, a propriedade enunciada também se aplica ao produto de $k + 1$ inteiros. ■

Teorema 2.7 (Teorema Fundamental da Aritmética): Todo número inteiro maior do que 1 pode ser escrito na forma:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k, \text{ em que } p_1 \leq p_2 \leq \ldots \leq p_k$$

são números primos positivos, não necessariamente distintos. Além disso, essa expressão é única.

Demonstração: Primeiramente provaremos que qualquer inteiro n pode ser escrito como acima e a demonstração será dada por indução. Se $n = 2$, então n é primo e

já se encontra na forma desejada. Suponhamos que todo número inteiro m tal que $2 \leq m < n$, pode ser escrito como produto de primos. Mostraremos que n também pode ser escrito como produto de primos.

Se n for primo, então não há nada a ser demonstrado. Se n não for um número primo, então existem divisores d e d' de n tais que $n = d \cdot d'$, com $1 < d, d' < n$. Pela hipótese de indução, segue que $d = q_1 \cdot q_2 \cdot \ldots \cdot q_r$, com $q_1 \leq q_2 \leq \ldots \leq q_r$ primos positivos e $d' = q'_1 \cdot q'_2 \cdot \ldots \cdot q'_s$, com $q'_1 \leq q'_2 \leq \ldots \leq q'_s$ primos positivos.

Segue que

$$n = d \cdot d' = (q_1 \cdot q_2 \cdot \ldots \cdot q_r) \cdot (q'_1 \cdot q'_2 \cdot \ldots \cdot q'_s)$$

e rearranjando os números primos $q_1, q_2, \ldots, q_r, q'_1, q'_2, \ldots, q'_s$ podemos escrever:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k,$$

em que $k = r + s$ e $p_1 \leq p_2 \leq \ldots \leq p_k$, como queríamos demonstrar.

Demonstraremos a unicidade da expressão $n = p_1 \cdot \ldots \cdot p_k$, em que $p_1 \leq p_2 \leq \ldots \leq p_k$ são números primos positivos. Suponhamos que exista um inteiro positivo $n, n \geq 2$, que possa ser escrito como produto de fatores primos positivos de duas maneiras diferentes, isto é, suponhamos

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s,$$

sendo $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ primos positivos com $p_1 \leq p_2 \leq \ldots \leq p_r$ e $q_1 \leq q_2 \leq \ldots \leq q_s$.

Cancelando os fatores primos que aparecem em ambos os lados da igualdade

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s,$$

como as duas fatorações de n são supostamente distintas, chegaremos a uma igualdade:

$$p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_u} = q_{j_1} \cdot q_{j_2} \cdot \ldots \cdot q_{j_v}$$

em que $u \geq 1$ e $v \geq 1$ e cada um dos primos do lado esquerdo é diferente de cada um dos primos do lado direito, ou seja, os membros à esquerda e à direita não têm mais fatores primos comuns. Da última igualdade acima, temos que p_{i_1} divide o produto $q_{j_1} \cdot q_{j_2} \cdot \ldots \cdot q_{j_v}$. Pelo Lema 2.2, temos que p_{i_1} divide um dos fatores $q_{j_1}, q_{j_2}, \ldots, q_{j_v}$, o que é impossível, uma vez que cada um destes fatores é primo e diferente de p_{i_1}.

Portanto, chegamos em um absurdo e concluímos que a fatoração de n em primos positivos é única. ■

Corolário 2.1: Para cada inteiro n, com $n \geq 2$, existem primos positivos $p_1, \ldots, p_s$, com $s \geq 1$ e $p_1 < \ldots < p_s$ se $s \geq 2$, e inteiros positivos $\alpha_1, \ldots, \alpha_s$, tais que

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}.$$

Tal representação é única.

Demonstração: Pelo Teorema 2.7, n é um produto de fatores primos $q_1 \cdot \ldots \cdot q_r$, com $q_1 \leq \ldots \leq q_r$ $(r \geq 1)$. Agrupando-se os fatores primos repetidos na forma de potências de primos, temos a representação enunciada neste corolário. Além disso, pelo Teorema Fundamental da Aritmética, tal representação é única. ■

▷▷▷ **Exemplo 2.12:** Exemplificando o 2.7, temos as seguintes fatorações de inteiros, com fatores primos escritos em ordem não decrescente:

(a) $40 = 2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5$.

(b) $342 = 2 \cdot 3 \cdot 3 \cdot 19 = 2 \cdot 3^2 \cdot 19$.

PROPOSIÇÃO 2.8: Seja m um inteiro tal que $m = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$, com $n \geq 1$ e $p_1, \ldots, p_n$ primos positivos com $p_1 < \ldots < p_n$ se $n \geq 2$ e $\alpha_1, \ldots, \alpha_n$ inteiros positivos.
Então, cada inteiro a divisor de m é da forma:

$$a = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n},$$

com $\beta_1, \ldots, \beta_n$ inteiros satisfazendo $0 \leq \beta_i \leq \alpha_i, \forall i \in \{1, 2, \ldots n\}$.

Demonstração: Se $a|m$, então $m = a \cdot c$, para algum inteiro positivo c. Assim, os eventuais fatores primos de a (eventuais, pois podemos ter $a = 1$) são fatores primos de m, ou seja, o conjunto de fatores primos de a é um subconjunto dos fatores primos de m.
Assim sendo, $a = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$ para certos números inteiros não negativos $\beta_1, \ldots, \beta_n$ (em que teremos $\beta_j = 0$ se p_j não for fator de a). Claramente, para cada índice j teremos $\beta_j \leq \alpha_j$, pois, como $p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n} \cdot c$, se $\alpha_j < \beta_j$ para algum índice j, teremos uma contradição em relação ao Teorema 2.7. ■

⋆ OBSERVAÇÃO 2.8:A Proposição 2.8 nos fornece um meio de encontrar todos os divisores de um inteiro m, $m \geq 2$, a partir da fatoração de m em primos positivos.

▷▷▷ **Exemplo 2.13:** Os divisores positivos de $120 = 2^3 \cdot 3 \cdot 5$ são os inteiros positivos cujas fatorações possuem somente potências dos primos $2, 3$ e 5, com expoentes menores que ou iguais a $3, 1$ e 1 respectivamente. Os divisores de 120 são, portanto,

1	3	5	$3 \cdot 5 = 15$
2	$2 \cdot 3 = 6$	$2 \cdot 5 = 10$	$2 \cdot 3 \cdot 5 = 30$
$2^2 = 4$	$2^2 \cdot 3 = 12$	$2^2 \cdot 5 = 20$	$2^2 \cdot 3 \cdot 5 = 60$
$2^3 = 8$	$2^3 \cdot 3 = 24$	$2^3 \cdot 5 = 40$	$2^3 \cdot 3 \cdot 5 = 120$

PROPOSIÇÃO 2.9: Sejam a e b dois inteiros positivos. Então existem primos positivos $p_1, \ldots, p_n$, com $n \geq 1$, sendo $p_1 < \ldots < p_n$ se $n \geq 2$ e inteiros não negativos $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$, tais que:

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \text{ e } b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}.$$

A partir destas representações de a e b, teremos:

$$(a,b) = p_1^{\gamma_1} \cdot \ldots \cdot p_n^{\gamma_n},$$

sendo para cada índice i, $\gamma_i = min\{\alpha_i, \beta_i\}$.

Demonstração: Para que um produto de fatores primos comuns seja um divisor comum de a e b, temos pela Proposição 2.8 que nenhum expoente γ_i de p_i poderá superar nem α_i e nem β_i. Como estamos interessados no maior dos divisores positivos, basta tomarmos $\gamma_i = min\{\alpha_i, \beta_i\}$. ■

▷▷▷ **Exemplo 2.14:** Calcular $mdc(700, 720)$, com base nas decomposições de 700 e 720 em fatores primos.

Solução: Fatorando-se 720 e 700 em potências de primos, obtemos:

$$720 = 2^4 \cdot 3^2 \cdot 5$$
$$700 = 2^2 \cdot 5^2 \cdot 7$$

Podemos então, escrever:

$$720 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^0$$
$$700 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1$$

Pela Proposição 2.9, $mdc(a,b) = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 2^2 \cdot 5 = 20$. □

DEFINIÇÃO 2.5 (MÍNIMO MÚLTIPLO COMUM): O Mínimo Múltiplo Comum de dois inteiros a e b é o menor inteiro positivo que é divisível por a e b. Vamos denotá-lo por $mmc(a,b)$ ou por $[a,b]$.

PROPOSIÇÃO 2.10: Sejam a e b dois inteiros positivos. Então existem primos positivos $p_1, \ldots, p_n$, com $n \geq 1$, sendo $p_1 < \ldots < p_n$ se $n \geq 2$ e inteiros não negativos $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$, tais que:

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \text{ e } b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}.$$

A partir destas representações de a e b, teremos:

$$[a,b] = p_1^{\delta_1} \cdot \ldots \cdot p_n^{\delta_n},$$

sendo para cada índice i, $\delta_i = max\{\alpha_i, \beta_i\}$.

Demonstração: Da definição de mínimo múltiplo comum nenhum fator primo p_i deste mínimo poderá ter um expoente que seja inferior nem a α_i e nem a β_i. Se tomarmos o maior destes dois para expoente de p_i teremos, não apenas um múltiplo comum, mas o menor possível dentre todos eles. O que conclui a demonstração. ■

▷▷▷ **Exemplo 2.15:** Calcular $mmc(700, 720)$, com base nas decomposições de 700 e 720 em fatores primos.

Solução: Conforme vimos,

$$720 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^0$$
$$700 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1$$

Pela Proposição 2.10, $mmc(720,700) = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 25200$ □

Teorema 2.8: Se a e b são dois inteiros positivos, então

$$mmc(a,b) \cdot mdc(a,b) = a \cdot b.$$

Demonstração: Sejam a e b inteiros positivos, e os consideremos representados como na Proposição 2.9, isto é,

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \text{ e } b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n},$$

sendo $p_1, \ldots, p_n$ primos positivos e $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ inteiros não negativos.

Pelas Proposições 2.9 e 2.10, temos:

$$mdc(a,b) = p_1^{\gamma_1} \cdot \ldots \cdot p_n^{\gamma_n}$$
$$mmc(a,b) = p_1^{\delta_1} \cdot \ldots \cdot p_n^{\delta_n}$$

sendo para cada índice i, $\gamma_i = min\{\alpha_i, \beta_i\}$ e $\delta_i = max\{\alpha_i, \beta_i\}$.

Como para cada índice i, $\gamma_i + \delta_i = min\{\alpha_i, \beta_i\} + max\{\alpha_i, \beta_i\} = \alpha_i + \beta_i$, então:

$$\begin{aligned} mdc(a,b) \cdot mmc(a,b) &= (p_1^{\gamma_1} \cdot \ldots \cdot p_n^{\gamma_n})(p_1^{\delta_1} \cdot \ldots \cdot p_n^{\delta_n}) \\ &= p_1^{\gamma_1+\delta_1} \cdot \ldots \cdot p_n^{\gamma_n+\delta_n} \\ &= p_1^{\alpha_1+\beta_1} \cdot \ldots \cdot p_n^{\alpha_n+\beta_n} \\ &= (p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n})(p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}) \\ &= a \cdot b \end{aligned}$$

■

TEOREMA 2.9 (EUCLIDES): Existem infinitos números primos.

Demonstração: Suponhamos que exista uma quantidade finita de números primos. Seja $p_1, p_2, \ldots, p_n$ a relação de todos os primos. Consideremos o número $R = p_1 \cdot \ldots \cdot p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa relação, pois caso contrário, $1 = R - p_1 \cdot \ldots \cdot p_n$ seria divisível por p_i, o que é um absurdo. Além disso, temos que R é maior que qualquer p_i. Mas 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 relação original. Portanto a quantidade de números primos não pode ser finita. ■

3

Relação de Equivalência

O conteúdo presente neste capítulo é baseado em *Teoria Elementar dos números* de Landau, 2002, *Números primos: mistérios e recordes* de Ribemboim, 2001 e também em *Uma introdução à teoria dos números* de Santos, 2007. Algumas proposições e definições podem ser encontradas em *Aritmética*, Hefez, 2014.

3.1 Relação

Definição 3.1 (Produto Cartesiano): Dados dois conjuntos não vazios A e B, chamamos de produto cartesiano de A por B o conjunto de todos os pares ordenados (a,b), tais que $a \in A$ e $b \in B$.

Notação: $A \times B = \{(a,b);\ a \in A \text{ e } b \in B\}$.

⋆ Observação 3.1:Em geral, $A \times B \neq B \times A$.

▷▷▷ **Exemplo 3.1:** Considere os conjuntos $A = \{1,2\}$ e $B = \{1,2,3\}$. Temos que:

$$\begin{aligned} A \times B &= \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3)\} \\ B \times A &= \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2)\} \end{aligned}$$

Observe que $A \times B \neq B \times A$.

⋆ Observação 3.2:Se A ou B for o conjunto vazio, então definimos $A \times B = \varnothing$.

Definição 3.2 (Relação): Dados dois conjuntos A e B, definimos uma relação $\mathcal{R}$ de A em B, como sendo um subconjunto de $A \times B$. Dizemos que $a \in A$ se relaciona com $b \in B$ e denotamos por $a\mathcal{R}b$ se $(a,b) \in \mathcal{R}$. Caso contrário, escrevemos $a\ \not\mathcal{R} b$.

▷▷▷ **Exemplo 3.2:** Considere os conjuntos $A = \{1,2,3\}$ e $B = \{a,b\}$. Temos

que:

$$A \times B \;=\; \{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$$

A seguir, listamos algumas das possíveis relações entre A e B:

$$\begin{aligned}
\mathcal{R}_1 &= \{(1,a),(1,b)\}\\
\mathcal{R}_2 &= \{(1,a),(2,b),(2,a)\}\\
\mathcal{R}_3 &= \varnothing\\
\mathcal{R}_4 &= A \times B\\
\mathcal{R}_5 &= \{(3,b)\}
\end{aligned}$$

⋆ Observação 3.3:Neste exemplo, observamos que: $1\mathcal{R}_1 b$, $1\mathcal{R}_1 a$, $2\mathcal{R}_2 b$, $3\,\not\mathcal{R}_2 a$.

⋆ Observação 3.4:Quando $A = B$ e $\mathcal{R}$ é uma relação de A em B, dizemos que $\mathcal{R}$ é uma *relação sobre* A, ou que $\mathcal{R}$ é uma *relação em* A.

3.1.1 Propriedades de uma relação $\mathcal{R}$ em A

Daremos a seguir as principais propriedades que uma relação $\mathcal{R}$ sobre A pode verificar.

(1) Reflexiva: Dizemos que $\mathcal{R}$ é reflexiva, quando **todo** elemento de A se relaciona consigo mesmo, ou seja, $\forall\ x \in A,\ x\mathcal{R}x$, isto é, $(x,x) \in \mathcal{R}$.

▷▷▷ **Exemplo 3.3:** (a) A relação $\mathcal{R} = \{(a,a),(b,b),(c,c),(a,b),(b,c)\}$ sobre $A = \{a,b,c\}$ é reflexiva, pois $a\mathcal{R}a$, $b\mathcal{R}b$ e $c\mathcal{R}c$.

(b) Seja $\mathcal{R}$ uma relação definida no conjunto $\mathbb{Z}$, dos números inteiros, por $x\mathcal{R}y \;\Leftrightarrow\; x = y$.

Temos que $\mathcal{R}$ é reflexiva, pois $x = x$, $\forall x \in \mathbb{Z}$.

(c) Seja $\mathcal{R}$ uma relação definida sobre o conjunto das retas do espaço euclidiano, dada por $r\ \mathcal{R}\ s \;\Leftrightarrow\; r \parallel s$.

$\mathcal{R}$ é reflexiva, pois $r \parallel r$, qualquer que seja a reta.

(d) Considere a relação $\mathcal{R} = \{(a,a),(a,b),(b,a),(b,b),(b,c)\}$ sobre $A = \{a,b,c\}$.

$\mathcal{R}$ não é reflexiva, pois $c\ \not\mathcal{R}c$

(2) Simétrica: Dizemos que $\mathcal{R}$ é simétrica, se dados $x,y \in A$ e $x\mathcal{R}y$, então $y\mathcal{R}x$.

▷▷▷ **Exemplo 3.4:** (a) A relação $\mathcal{R} = \{(a,a),(a,b),(b,a),(c,c)\}$ sobre $A = \{a,b,c\}$ é claramente simétrica.

(b) Seja $\mathcal{R}$ uma relação definida sobre o conjunto das retas do espaço euclidiano, dada por $r \mathcal{R} s \Leftrightarrow r \perp s$.

$\mathcal{R}$ é simétrica, pois se $r \perp s$, então $s \perp r$.

(c) Considere a relação $\mathcal{R} = \{(a,a),(a,b),(b,b),(c,c)\}$ sobre $A = \{a,b,c\}$.

$\mathcal{R}$ não é simétrica, pois $a\mathcal{R}b$ e $b \not\mathcal{R}a$.

(3) Transitiva: Dizemos que $\mathcal{R}$ é transitiva se, dados $x, y, z \in A$, tais que $x\mathcal{R}y$ e $y\mathcal{R}z$, então $x\mathcal{R}z$.

▷▷▷ **Exemplo 3.5:** (a) A relação $\mathcal{R} = \{(a,b),(b,b),(b,c),(a,c),(c,c)\}$ sobre $A = \{a,b,c\}$ é transitiva.

(b) A relação $\mathcal{R}$ definida sobre o conjunto dos triângulos do espaço, dada por: $x\mathcal{R}y \Leftrightarrow x \sim y$ (semelhança), é transitiva. Pois, sendo x, y e z triângulos quaisquer, tem-se: $x \sim y$ e $y \sim z \Rightarrow x \sim z$.

(c) A relação $\mathcal{R} = \{(a,b),(b,a)\}$ sobre $A = \{a,b\}$ não é transitiva, pois $a\mathcal{R}b, b\mathcal{R}a$ e $a \not\mathcal{R}a$.

(4) Antissimétrica: Dizemos que $\mathcal{R}$ é antissimétrica se, dados $x, y \in A$, tais que $x\mathcal{R}y$ e $y\mathcal{R}x$, então $x = y$.

▷▷▷ **Exemplo 3.6:** (a) A relação $\mathcal{R}$ sobre o conjunto dos números reais $\mathbb{R}$, dada por

$$x\mathcal{R}y \Leftrightarrow x \leq y$$

é antissimétrica, pois sendo x e y números reais quaisquer, se $x \leq y$ e $y \leq x$, então $x = y$.

(b) A relação $\mathcal{R} = \{(a,a),(b,b),(c,c),(b,c),(c,b)\}$ sobre $A = \{a,b,c\}$ não é antissimétrica, pois $b\mathcal{R}c$, $c\mathcal{R}b$ mas $b \neq c$.

Definição 3.3 (Relação de Equivalência): Uma relação $\mathcal{R}$ sobre um conjunto $A \neq \varnothing$ recebe o nome de relação de equivalência sobre A se, e somente se, $\mathcal{R}$ é reflexiva, simétrica e transitiva. Ou seja, $\mathcal{R}$ deve cumprir as seguintes propriedades:

(i) Se $x \in A$, então $x\mathcal{R}x$;

(ii) Se $x, y \in A$ e $x\mathcal{R}y$, então $y\mathcal{R}x$;

(iii) Se $x, y, z \in A$, $x\mathcal{R}y$ e $y\mathcal{R}z$, então $x\mathcal{R}z$.

▷▷▷ **Exemplo 3.7:** 1. A relação $\mathcal{R} = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$, sobre $A = \{a,b,c\}$, é uma relação de equivalência.

2. A relação de paralelismo definida para as retas de um espaço euclidiano é uma relação de equivalência, pois sendo r, s e t retas, tem-se:

(i) $r \parallel r$;

(ii) Se $r \parallel s$, então $s \parallel r$;

(iii) Se $r \parallel s$ e $s \parallel t$, então $r \parallel t$.

3. A relação "igual a"no conjunto dos $\mathbb{R}$ é uma relação de equivalência, pois se $x, y, z \in \mathbb{R}$, tem-se:

(i) $x = x$;

(ii) Se $x = y$, então $y = x$;

(iii) Se $x = y$ e $y = z$, então $x = z$.

3.2 Congruência Módulo m em $\mathbb{Z}$

Definição 3.4 (Congruência módulo m em $\mathbb{Z}$): Dados três inteiros a, b e m, dizemos que ***a* é congruente a *b* módulo *m*** e denotamos por $a \equiv b \pmod{m}$ ou por $a \underset{m}{\equiv} b$, se m divide $(a - b)$. Se a não for congruente a b, módulo m, escrevemos $a \not\equiv b \pmod{m}$, ou ainda, $a \underset{m}{\not\equiv} b$.

⋆ Observação 3.5:Note que

$$\begin{aligned} a \underset{m}{\equiv} b &\Leftrightarrow m|(a-b) \\ &\Leftrightarrow a - b = \lambda \cdot m, \text{ para algum } \lambda \in \mathbb{Z} \\ &\Leftrightarrow a = b + \lambda \cdot m, \text{ para algum } \lambda \in \mathbb{Z} \end{aligned}$$

▷▷▷ **Exemplo 3.8:** (a) $22 \equiv 4 \pmod{9}$, pois $9|(22-4)$.

(b) $3 \equiv -6 \pmod{9}$, pois $9|(3+6)$.

(c) $200 \equiv 2 \pmod{9}$, pois $9|(200-2)$.

(d) $13 \not\equiv 5 \pmod{9}$, pois $9 \not| (13-5)$.

Teorema 3.1: Sendo m um inteiro não nulo, a relação de congruência módulo m definida em $\mathbb{Z}$ é uma relação de equivalência em $\mathbb{Z}$, ou seja, satisfaz:

(i) Para todo $a \in \mathbb{Z}$, temos que $a \equiv a \ (mod\ m)$.

(ii) Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \ (mod\ m)$, então $b \equiv a \ (mod\ m)$.

(iii) Para todo $a, b, c \in \mathbb{Z}$, se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então $a \equiv c \ (mod\ m)$.

Demonstração: Para cada $a, b, c \in \mathbb{Z}$, temos:

(i) Como $m|0$, então $m|(a-a)$, ou seja, $a \equiv a \ (mod\ m)$.

(ii) Se $a \equiv b\ (mod\ m)$, então $m|(a-b)$, consequentemente, $m|-(a-b)$, ou seja, $m|(b-a)$. Portanto, $b \equiv a\ (mod\ m)$.

(iii) Se $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$, então $m|(a-b)$ e $m|(b-c)$. Então segue da Proposição 2.4 que $m|[(a-b)+(b-c)]$, isto é, $m|(a-c)$. Portanto, $a \equiv c\ (mod\ m)$.

■

TEOREMA 3.2: Seja m um inteiro não nulo fixado. Dados a,b,$c \in \mathbb{Z}$ e $n \in \mathbb{N}$, temos:

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

(ii)
$$\left.\begin{array}{l} a \equiv b\ (mod\ m) \\ c \equiv d\ (mod\ m) \end{array}\right\} \Rightarrow (a+c) \equiv (b+d)\ (mod\ m)$$

(iii) $a \equiv b\ (mod\ m) \Rightarrow a \cdot c \equiv b \cdot c\ (mod\ m)$

(iv)
$$\left.\begin{array}{l} a \equiv b\ (mod\ m) \\ c \equiv d\ (mod\ m) \end{array}\right\} \Rightarrow (a \cdot c) \equiv (b \cdot d)\ (mod\ m)$$

(v) $a \equiv b\ (mod\ m) \Rightarrow a^n \equiv b^n\ (mod\ m)$

Demonstração:

(i)
$$\begin{array}{rcl} a \equiv b\ (mod\ m) & \Leftrightarrow & m|(a-b) \\ & \Leftrightarrow & m|[(a+c)-(b+c)] \\ & \Leftrightarrow & (a+c) \equiv (b+c)\ (mod\ m) \end{array}$$

(ii)
$$\left.\begin{array}{l} a \equiv b\ (mod\ m) \\ c \equiv d\ (mod\ m) \end{array}\right\} \Rightarrow m|(a-b) \text{ e } m|(c-d)$$

Logo, segue da Proposição 2.4, que $m|[(a-b)+(c-d)]$, ou seja, $m|[(a+c)-(b+d)]$. Portanto, $(a+c) \equiv (b+d)\ (mod\ m)$.

(iii) Se $a \equiv b\ (mod\ m)$, então $m|(a-b)$, consequentemente, $m|(a-b) \cdot c$ e desta forma, $m|(ac-bc)$. Portanto, $ac \equiv bc\ (mod\ m)$.

(iv) Se $\left\{\begin{array}{l} a \equiv b\ (mod\ m) \\ c \equiv d\ (mod\ m) \end{array}\right.$, então usando (iii), podemos multiplicar os termos da primeira expressão por c e os da segunda por b, obtendo:

$$\left\{\begin{array}{l} ac \equiv bc\ (mod\ m) \\ bc \equiv bd\ (mod\ m) \end{array}\right. \Rightarrow ac \equiv bd\ (mod\ m), \text{ por transitividade.}$$

(v) A demonstração será feita por indução sobre n.

Se $n = 0$, então o resultado é claramente válido.

Agora, suponha que o resultado seja válido para $n = k$, ou seja, $a^k \equiv b^k \ (mod\ m)$.

Assim, temos que $\begin{cases} a^k \equiv b^k \ (mod\ m) \\ a \equiv b \ (mod\ m) \text{ (hipótese inicial)} \end{cases}$.

Assim, usando (iv), obtemos que $a^{k+1} \equiv b^{k+1} \ (mod\ m)$.

Portanto, pelo princípio da indução finita, temos que o resultado é válido para todo $n \in \mathbb{N}$. ■

⋆ Observação 3.6:A reíproca do item (iii) é falsa. Por exemplo,

$$\begin{aligned} 14 &\equiv 8 \ (mod\ 6) \\ 7 \cdot 2 &\equiv 4 \cdot 2 \ (mod\ 6) \end{aligned}$$

Note que não podemos cancelar o fator comum 2, pois $7 \not\equiv 4 \ (mod\ 6)$.

Teorema 3.3: Sejam a, b, c e m inteiros, $m \geq 2$. Se $a \cdot c \equiv b \cdot c \ (mod\ m)$, sendo m e c primos entre si, então $a \equiv b \ (mod\ m)$.

Demonstração: Se $a \cdot c \equiv b \cdot c \ (mod\ m)$, então $m|(ac - bc)$.
Logo, $m|(a - b) \cdot c$. Como $mdc(m,c) = 1$, segue do Teorema 2.6, que $m|(a - b)$ e, então $a \equiv b \ (mod\ m)$. ■

▷▷▷ **Exemplo 3.9:** Como $42 \equiv 7 \ (mod\ 5)$ e $mdc(5,7) = 1$, podemos concluir que:

$$6 \cdot 7 \equiv 1 \cdot 7 \ (mod\ 5) \ \Rightarrow \ 6 \equiv 1 \ (mod\ 5)$$

Teorema 3.4 (Congruência módulo m e o resto da divisão por m): Sejam a, b e m inteiros, com $m \geq 2$. Então:

(i) Se r é o resto da divisão de a por m, então $a \equiv r \ (mod\ m)$.

(ii) Se $a \equiv s \ (mod\ m)$ e $0 \leq s < m$, então s é o resto da divisão de a por m.

(iii) $a \equiv b \ (mod\ m)$ se, e somente se, os restos das divisões de a e b por m são iguais.

Demonstração:

(1) Pelo algoritmo da divisão, segue que existem inteiros q e r, tais que $a = m \cdot q + r$, com $0 \leq r < m$. Desta forma, $a - r = m \cdot q$, ou seja, $m|(a - r)$. Portanto, $a \equiv r \ (mod\ m)$.

(2) Sendo $a \equiv s \ (mod\ m)$, temos que $a - s = m \cdot q$, para algum $q \in \mathbb{Z}$.

Daí, $a = m \cdot q + s$, com q e s inteiros e $0 \leq s < m$ (por hipótese).

Pelo Teorema 2.2, s é o resto da divisão de a por m, já que o resto e o quociente dessa divisão são únicos.

(3) ($\Rightarrow$) Seja r o resto da divisão de a por m. Pelo item (1), temos que $a \equiv r \ (mod\ m)$. Como $a \equiv b \ (mod\ m)$, usando a propriedade transitiva da relação de equivalência, temos que $b \equiv r \ (mod\ m)$. Como $0 \leq r < m$, pelo item (2), segue que r é o resto da divisão de b por m.

($\Leftarrow$) Seja r o resto das divisões de a e b por m. Pelo item (1) anterior, temos que $a \equiv r \ (mod\ m)$ e $b \equiv r \ (mod\ m)$. Novamente pela transitividade, temos que $a \equiv b \ (mod\ m)$.

■

▷▷▷ **Exemplo 3.10 (Determinando restos via congruências):** .

(a) Calcule o resto da divisão de 2^{100} por 7.

Solução:

$$\begin{aligned} 8 &\equiv 1 \ (mod\ 7) \\ 2^3 &\equiv 1 \ (mod\ 7) \\ (2^3)^{33} &\equiv 1^{33} \ (mod\ 7) \\ 2^{99} &\equiv 1 \ (mod\ 7) \\ 2^{99} \cdot 2 &\equiv 1 \cdot 2 \ (mod\ 7) \\ 2^{100} &\equiv 2 \ (mod\ 7) \end{aligned}$$

Portanto, o resto da divisão de 2^{100} por 7 é 2.

(b) Mostre que $2^{2n+1} + 1$ é divisível por 3, para todo $n \in \mathbb{N}$.

Solução:

$$\begin{aligned} 4 &\equiv 1 \ (mod\ 3) \\ 4^n &\equiv 1^n \ (mod\ 3), \ \forall\ n \in \mathbb{N} \\ 2^{2n} &\equiv 1 \ (mod\ 3) \\ 2^{2n} \cdot 2 &\equiv 1 \cdot 2 \ (mod\ 3) \\ 2^{2n+1} &\equiv 2 \ (mod\ 3) \\ 2^{2n+1} + 1 &\equiv 2 + 1 \ (mod\ 3) \\ 2^{2n+1} + 1 &\equiv 3 \ (mod\ 3) \end{aligned}$$

Agora, sabemos que $3 \equiv 0 \ (mod\ 3)$, e portanto, $2^{2n+1} + 1 \equiv 0 \ (mod\ 3)$. Ou seja, $3|(2^{2n+1} + 1), \ \forall\ n \in \mathbb{N}$.

Definição 3.5 (Função Fi de Euler): Designaremos por $\phi(n)$ o número de elementos de um sistema reduzido de resíduos módulo $n > 1$, que corresponde à quantidade de números naturais entre 1 e $n-1$ que são primos com n. Pondo $\phi(1) = 1$, definimos a função

$$\phi : \mathbb{N} \to \mathbb{N}$$

chamada Função Fi de Euler.

Proposição 3.1: Seja um natural n onde $n \geq 2$. Então $\phi(n) = n - 1$ se, e somente se, n é primo.

Demonstração: De fato, n é primo se, e somente se, $1, 2, \cdots, n-1$ formam um sistema reduzido de resíduos módulo n, o que equivale a dizer que $\phi(n) = n - 1$. ■

Proposição 3.2: Sejam m e n inteiros positivos tais que $mdc(m,n) = 1$. então

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

Demonstração: O resultado é trivial se $m = 1$ ou $n = 1$. Portanto, vamos supor que $m > 1$ e $n > 1$. Considere a seguinte tabela formada pelos números naturais de 1 a $m \cdot n$:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & k & \cdots & n \\ n+1 & n+2 & \cdots & n+k & \cdots & 2n \\ \vdots & \vdots & & \vdots & & \vdots \\ (m-1)n+1 & (m-1)n+2 & \cdots & (m-1)n+k & \cdots & m \cdot n \end{array}$$

Como $mdc(m,n) = 1$, tem-se que $mdc(t, m \cdot n) = 1$ se, e somente se, $mdc(t,m) = mdc(t,n) = 1$. Para calcular $\phi(mn)$ devemos contar quantos dos inteiros na tabela acima são simultaneamente primos com m e n.

O Teorema 3.2, intem (i) implica que se o primeiro elemento da coluna não for primo com n, então todos os elementos da coluna não são primos com n. Portanto, os elementos primos com n estão necessariamente nas colunas restantes que são em número $\phi(n)$, cujos elementos são primos com n. Vejamos agora quais são os elementos primos com m em cada uma das colunas.

Como $mdc(m,n) = 1$, a sequência

$$k, n+k, \cdots, (m-1)n+k$$

forma um sistema completo de resíduos módulo m e, portanto, $\phi(m)$ desses elementos são primos com m. Logo, o número de elementos simultaneamente primos com m e

n é $\phi(m) \cdot \phi(n)$. ■

⋆ Observação 3.7:Das proposições 3.1 e 3.2, concluímos que

$$\phi(m \cdot n) = (m-1) \cdot (n-1)$$

se m e n são primos distintos.

Definição 3.6: Consideremos dois números naturais p e i com $p \geq i$. Chamamos de *número binomial* p sobre i e indicamos por $\begin{pmatrix} p \\ i \end{pmatrix}$ o número dado por:

$$\begin{pmatrix} p \\ i \end{pmatrix} = \frac{p!}{i!(p-i)!}$$

Lema 3.1: Seja p um número primo. Os números binomiais $\begin{pmatrix} p \\ i \end{pmatrix}$, em que $0 < i < p$, são todos divisíveis por p.

Demonstração: Para $i = 1$ o resultado é trivial. Podemos, então, supor $1 < i < p$. Nesse caso, $i! \mid p(p-1)\cdots(p-i+1)$. Como $mdc(i!,p) = 1$, decorre que $i! \mid (p-1)\cdots(p-i+1)$ e o resultado se segue, pois

$$\begin{pmatrix} p \\ i \end{pmatrix} = p\,\frac{(p-1)\cdots(p-i+1)}{i!}$$

Teorema 3.5 (Pequeno Teorema de Fermat): Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.

Demonstração: Se $p = 2$, temos que $a^2 - a = a(a-1)$ é par e, assim, o resultado segue. Suponhamos p ímpar. Nesse caso, basta mostrar o resultado para $a \geq 0$ pois se $a < 0$, $-a > 0$ e $(-a)^p - (-a) = -(a^p - a)$. Provaremos o resultado por indução sobre a.

O resultado vale claramente para $a = 0$, pois $p \mid 0$.

Suponha o resultado válido para a. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + \begin{pmatrix} p \\ 2 \end{pmatrix} a^{p-2} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a$$

.

Pelo Lema 3.1 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p e segue o resultado. ■

3.3 Classe de Equivalência e Conjunto Quociente

DEFINIÇÃO 3.7: Seja $\mathcal{R}$ uma relação de equivalência sobre A. Dado $a \in A$, chama-se **classe de equivalência** determinada por a, módulo $\mathcal{R}$, o seguinte subconjunto de A:

$$\overline{a} = \{x \in A;\ x\mathcal{R}a\}.$$

DEFINIÇÃO 3.8: O conjunto das classes de equivalência módulo $\mathcal{R}$ será indicado por $A/\mathcal{R}$ e chamado de **conjunto quociente** de A por $\mathcal{R}$.

▷▷▷ **Exemplo 3.11:** Considere a relação de equivalência $\mathcal{R} = \{(a,a), (b,b), (c,c), (a,b), (b,a)\}$ sobre $A = \{a, b, c\}$.

Neste caso, temos:

$$\begin{aligned} \overline{a} &= \{a, b\} \\ \overline{b} &= \{b, a\} = \overline{a} \\ \overline{c} &= \{c\} \\ A/\mathcal{R} &= \{\overline{a}, \overline{c}\} = \{\{a, b\}, \{c\}\} \end{aligned}$$

▷▷▷ **Exemplo 3.12:** Sejam $m \in \mathbb{Z} \setminus \{0\}$ e $\mathcal{R}$ a relação de congruência módulo m definida em $\mathbb{Z}$. Temos que:

$$\begin{aligned} \overline{0} &= \{k \in \mathbb{Z};\ k \equiv 0\ (mod\ m)\} = \{\text{inteiros com resto 0 na divisão por } m\} \\ \overline{1} &= \{k \in \mathbb{Z};\ k \equiv 1\ (mod\ m)\} = \{\text{inteiros com resto 1 na divisão por } m\} \\ &\vdots \\ \overline{m-1} &= \{k \in \mathbb{Z};\ k \equiv m-1\ (mod\ m)\} = \{\text{inteiros com resto m-1 na divisão por } m\} \end{aligned}$$

Observe que qualquer número inteiro possui resto r na divisão por m com $0 \leq r \leq m-1$, assim, segue do Teorema 3.4 que qualquer número inteiro pertence a alguma das classes de equivalência listadas acima.

DEFINIÇÃO 3.9: Seja $\mathcal{R}$ a relação de equivalência módulo m definida em $\mathbb{Z}$. Assim:

$$\mathbb{Z}/\mathcal{R} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\} = \mathbb{Z}_m$$

DEFINIÇÃO 3.10 (PARTIÇÃO): Seja A um conjunto não vazio. Diz-se que uma família $\mathcal{P}$ de subconjuntos **não vazios** de A é uma **partição** de A se, e somente se,

(a) dois membros quaisquer de $\mathcal{P}$ ou são iguais, ou são disjuntos;

(b) a união dos membros de $\mathcal{P}$ é igual ao conjunto A.

⋆ Observação 3.8:Podemos denominar **conjunto** pelas palavras **coleção** ou **família** .

▷▷▷ **Exemplo 3.13:** A família de subconjuntos $\mathcal{P} = \{\{1\}, \{2,3\}, \{4\}\}$ é uma partição do conjunto $E = \{1,2,3,4\}$.

De fato, cada um dos três conjuntos que compõem $\mathcal{P}$ são não vazios, dois a dois disjuntos e a união deles é o conjunto E.

▷▷▷ **Exemplo 3.14:** Sejam $P = \{x \in \mathbb{Z};\ x \text{ é par}\}$ e $I = \{x \in \mathbb{Z};\ x \text{ é ímpar}\}$ subconjuntos de $\mathbb{Z}$.

Então $\mathcal{P} = \{P, I\}$ é uma partição de $\mathbb{Z}$, pois P e I são não vazios, $P \cap I = \varnothing$ e $P \cup I = \mathbb{Z}$.

Teorema 3.6: Se $\mathcal{R}$ é uma relação de equivalência sobre um conjunto A, então o conjunto quociente $A/\mathcal{R}$ é uma partição do conjunto A.

Demonstração: Primeiramente, mostraremos que todas as classes de equivalência que compõem $A/\mathcal{R}$ são diferentes do conjunto vazio. Seja $\overline{a} \in A/\mathcal{R}$. Como $\mathcal{R}$ é uma relação de equivalência, temos que $\mathcal{R}$ é reflexiva, assim, aRa, ou seja, $a \in \overline{a}$, portanto $\overline{a} \neq \varnothing$, para todo $\overline{a} \in A/\mathcal{R}$.

Agora, mostraremos que se $\overline{a}, \overline{b} \in A/\mathcal{R}$ são tais que $\overline{a} \cap \overline{b} \neq \varnothing$, então $\overline{a} = \overline{b}$. Seja $y \in \overline{a} \cap \overline{b}$. Então $y \in \overline{a}$ e $y \in \overline{b}$, ou seja, $y\mathcal{R}a$ e $y\mathcal{R}b$. Usando as propriedades simétrica e transitiva, concluímos que $a\mathcal{R}b$. Logo, $a \in \overline{b}$ e dessa forma, $\overline{a} \subset \overline{b}$. Por outro lado, como $\mathcal{R}$ é reflexiva, segue que $b\mathcal{R}a$ e assim, $b \in \overline{a}$, de forma que $\overline{b} \subset \overline{a}$.

Portanto, $\overline{a} = \overline{b}$ e assim, mostramos que classes distintas têm interseção vazia.

Finalmente, mostraremos que $\bigcup_{a \in A} \overline{a} = A$.

Para cada $a \in A$, temos que $\overline{a} \subset A$, portanto $\bigcup_{a \in A} \overline{a} \subset A$.

Por outro lado, sendo x um elemento qualquer de A, então xRx. Daí, $x \in \overline{x}$ e, por conseguinte, $x \in \bigcup_{a \in A} \overline{a}$. Portanto, $A \subset \bigcup_{a \in A} \overline{a}$.

Logo, $\bigcup_{a \in A} \overline{a} = A$. ■

4

Aplicação

Neste capítulo vamos estudar a solução de sistemas de congruências, o chamado *Algoritmo Chinês do Resto*. O capítulo se encerrará com uma aplicação deste algoritmo a um método de criptografia para partilha de senhas. Seu estudo fundamentou-se em Coutinho, 2005.

4.1 Sistemas de Congruências

4.1.1 Equações Lineares

TEOREMA 4.1 (TEOREMA DE INVERSÃO): A classe $\overline{a}$ tem inverso em $\mathbb{Z}_n$ se, e somente se, a e n são primos entre si.

Demonstração: Suponhamos que $\overline{a} \in \mathbb{Z}_n$ tem inverso $\overline{\alpha}$. Desta forma, $\overline{a} \cdot \overline{\alpha} = \overline{1}$, o que equivale a dizer que $a \cdot \alpha - k \cdot n = 1$, para algum $k \in \mathbb{Z}$. Observe que esta última equação implica que o $mdc(a,n) = 1$. Concluímos portanto que se $\overline{a}$ tem inverso em $\mathbb{Z}_n$, então $mdc(a,n) = 1$.

Reciprocamente, suponhamos que a é um inteiro e que $mdc(a,n) = 1$. Então segue do Teorema 2.5, que existem inteiros x_0, y_0 tais que $a \cdot x_0 + n \cdot y_0 = 1$. Essa equação é equivalente a $\overline{a} \cdot \overline{x_0} = \overline{1}$, em $\mathbb{Z}_n$. Concluímos assim, que se $mdc(a,n) = 1$, então $\overline{a}$ tem inverso em $\mathbb{Z}_n$. ■

Agora, iniciaremos o estudo de sistemas de equações lineares no qual abordaremos primeiramente o caso de uma única equação linear.

$$ax \equiv b \quad (mod\, n) \tag{4.1}$$

em que $a, b \in \mathbb{Z}$ e n é um número inteiro positivo. Consideraremos dois casos:

1. Se $\overline{a}$ é invertível em $\mathbb{Z}_n$

   Sejam $\overline{a}$ invertível em $\mathbb{Z}_n$ e $\overline{\alpha}$ o inverso de $\overline{a}$. A equação (4.1) pode ser reescrita como

$$\alpha(ax) \equiv \alpha b \pmod{n}$$

Como $\overline{\alpha a} = \bar{1}$ em $\mathbb{Z}_n$, segue que

$$x \equiv \alpha b \pmod{n}$$

é a solução da equação. Em particular, se n é primo, todo $a \not\equiv 0 \pmod{n}$ possui inverso em $\mathbb{Z}_n$ e (4.1) sempre tem solução.

2. Se $\overline{a}$ não é invertível em $\mathbb{Z}_n$

   Suponha que $\overline{a}$ não possui inverso em $\mathbb{Z}_n$. Nesse caso, temos que $mdc(a,n) \neq 1$. A equação (4.1) tem solução se existirem x, y em $\mathbb{Z}$ tais que

$$ax - ny = b \tag{4.2}$$

   Mas isso só é possível se $mdc(a,n)$ divide b. De fato, se existem $x, y \in \mathbb{Z}$ tais que $ax - ny = b$, então o fato de $d = mdc(a,n)$ implica que $d|a$ e $d|n$, consequentemente, $d|(ax - ny)$, ou seja, $d|b$. Por outro lado, se $d = mdc(a,n)$, então segue do Teorema 2.5 que existem $x_0, y_0 \in \mathbb{Z}$, tais que $ax_0 + ny_0 = d$. Se $d|b$, então $b = r \cdot d$, para algum $r \in \mathbb{Z}$, ou seja, $b = r \cdot (ax_0 + ny_0) = rx_0a + ry_0n$. Fazendo $x = rx_0$ e $-y = ry_0$, obtemos (4.2).

   Concluímos que (4.1) tem solução se, e somente se, b é divisível pelo $mdc(a,n)$. Se $\overline{a}$ tem inverso em $\mathbb{Z}_n$ essa condição é satisfeita, porque nesse caso $mdc(a,n) = 1$.

   Suponhamos que $d = mdc(a,n)$ divide b. Digamos que $a = da'$, $b = db'$ e $n = dn'$. Substituindo em (4.2) e cancelando d,

$$a'x - n'y = b'$$

   Que se converte na equação $a'x \equiv b' \pmod{n'}$; uma nova equação em congruências. Mas cuidado, o módulo mudou. A equação original tinha n como módulo; a nova equação tem módulo n', um divisor de n. Observe que $mdc(a',n') = mdc(a/d, n/d) = 1$, portanto essa última equação sempre tem solução.

▷▷▷ **Exemplo 4.1:** Seja $6x \equiv 4 \pmod{8}$. Como mdc(6,8) = 2 ≠ 1, não podemos inverter $\bar{6}$ em $\mathbb{Z}_8$. Se esta equação tiver solução, então existem inteiros x e y tais que 6x - 8y = 4 o que equivale a 3x - 4y = 2. Isto leva a $3x \equiv 2 \pmod{4}$. Mas $\bar{3}$ é o seu próprio inverso em $\mathbb{Z}_4$. Multiplicando esta última equação por 3, teremos a solução

$$x \equiv 2 \pmod{4} \tag{4.3}$$

Começamos com uma equação módulo 8, mas obtivemos uma solução módulo 4. Para fazermos a conversão, basta converter (4.3) em uma expressão em inteiros (isto é, sem congruências) e analisar como as soluções se comportam módulo 8. Temos

que (4.3) é equivalente a x = 2 + 4k, em que k é um inteiro qualquer. Se k for par, então $k = 2s$ para algum $s \in \mathbb{Z}$, desta forma teremos:

$$\begin{aligned} x &= 2 + 4k \\ x &= 2 + 4(2s) \\ x &= 2 + 8s \\ \therefore\ x &\equiv 2\ (mod\ 8) \end{aligned}$$

Analogamente, se k for ímpar, então $k = 2s + 1$, para algum $s \in \mathbb{Z}$, de modo que:

$$\begin{aligned} x &= 2 + 4k \\ x &= 2 + 4(2s + 1) \\ x &= 6 + 8s \\ \therefore\ x &\equiv 6\ (mod\ 8) \end{aligned}$$

Logo $6x \equiv 4 \quad (mod\, 8)$ possui duas soluções em $\mathbb{Z}_8$: $\bar{2}$ e $\bar{6}$. Observe que a equação é linear, mas tem duas soluções.

4.1.2 Teorema Chinês do Resto

Esse teorema é assim chamado porque um dos primeiros lugares em que aparece é o livro *Manual de aritmética do Mestre Sun*, escrito entre 287 d.C. e 473 d.C.. Esse resultado também é mencionado na *Aritmética* de Nicômano de Gerasa. Alguns conceitos sobre anéis se encontram no Apêndice 1.

Lema 4.1: Se a e b são primos entre si, isto é, $mdc(a,b) = 1$, então $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$.

Demonstração: Como $\mathbb{Z}_{ab} \cong \dfrac{\mathbb{Z}}{(ab)\mathbb{Z}}$ e $\mathbb{Z}_a \times \mathbb{Z}_b \cong \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$, é suficiente mostrarmos que $\dfrac{\mathbb{Z}}{(ab)\mathbb{Z}} \cong \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$.

Seja $\varphi : \mathbb{Z} \to \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$, definida por $\varphi(x) = (x + a\mathbb{Z}, x + b\mathbb{Z})$, para todo $x \in \mathbb{Z}$. Claramente temos que φ é um homomorfismo de anéis. Mais ainda,

$$Ker(\varphi) = \{x \in \mathbb{Z};\ \varphi(x) = (0 + a\mathbb{Z}, 0 + b\mathbb{Z})\} = \{x \in \mathbb{Z};\ \varphi(x) = (a\mathbb{Z}, b\mathbb{Z})\}.$$

Se $x \in ker(\varphi)$, então $x \in a\mathbb{Z}$ e $x \in b\mathbb{Z}$. Logo, $a|x$ e $b|x$, o que implica que $mmc(a,b)|x$. Mas, $mmc(a,b) = \dfrac{a \cdot b}{mdc(a,b)} = a \cdot b$. Assim, $x \in ab\mathbb{Z}$, ou seja $Ker(\varphi) \subseteq ab\mathbb{Z}$. A inclusão contrária é imediata. Pelo Primeiro Teorema do Isomorfismo para anéis temos $\dfrac{\mathbb{Z}}{ab\mathbb{Z}} \cong Im(\varphi) \subseteq \mathbb{Z}_a \times \mathbb{Z}_b$.

Como $\dfrac{\mathbb{Z}}{ab\mathbb{Z}} \cong \mathbb{Z}_{ab}$, $\#\left(\dfrac{\mathbb{Z}}{ab\mathbb{Z}}\right) = \#\left(\mathbb{Z}_{ab}\right) = ab = \#\left(\mathbb{Z}_a \times \mathbb{Z}_b\right)$, o que implica que

φ é sobrejetora. ■

TEOREMA 4.2: Se $n \in \mathbb{Z},\ n > 0$ e $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, com p_i's primos distintos, então $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}$

Demonstração: Segue diretamente do lema anterior e indução. ■

Observemos que na demonstração do lema anterior, mostramos que φ é sobrejetora sem exibirmos a pré-imagem de um elemento genérico. Assim, cabe a seguinte pergunta:

- Se $(c+a\mathbb{Z}, d+b\mathbb{Z}) \in \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}$, então qual é o $x \in \mathbb{Z}$ tal que $\varphi(x) = (c+a\mathbb{Z}, d+b\mathbb{Z})$?

Note que:

$$\begin{cases} x + a\mathbb{Z} = c + a\mathbb{Z} \\ x + b\mathbb{Z} = d + b\mathbb{Z} \end{cases} \Rightarrow \begin{cases} x \equiv c\ (mod\ a) \\ x \equiv d\ (mod\ b) \end{cases} \Rightarrow \begin{cases} x = c + a \cdot n_1,\ n_1 \in \mathbb{Z} \\ x = d + b \cdot n_2,\ n_2 \in \mathbb{Z} \end{cases}$$

Por exemplo, $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$, qual é o elemento $x \in \mathbb{Z}$, tal que $\varphi(x) = (\overline{2}, \overline{4})$? Temos que

$$\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 4\ (mod\ 5) \end{cases}$$

Assim, $x = 2 + 3n_1$, com $n_1 \in \mathbb{Z}$ e $x \equiv 4\ (mod\ 5)$. Desta forma:

$$\begin{aligned} x &\equiv 4\ (mod\ 5) \\ 2 + 3n_1 &\equiv 4\ (mod\ 5) \\ 3n_1 &\equiv 2\ (mod\ 5) \\ 2 \cdot 3n_1 &\equiv 2 \cdot 2\ (mod\ 5) \\ n_1 &\equiv 4\ (mod\ 5) \\ n_1 &= 4 + 5n_2,\ \text{para algum } n_2 \in \mathbb{Z}. \end{aligned}$$

Então, $x = 2 + 3(4 + 5n_2) = 14 + 15n_2$, ou seja, $x \equiv 14\ (mod\ 15)$.

COROLÁRIO 4.1 (TEOREMA CHINÊS DO RESTO): Seja $\{m_i\}_{i=1}^k$ um conjunto de k inteiros primos entre si 2 a 2, ou seja, $mdc(m_i, m_j) = 1$, para todo $i \neq j$. Então o sistema de congruências lineares:

$$\begin{cases} x \equiv a_1\ (mod\ m_1) \\ \vdots \\ x \equiv a_k\ (mod\ m_k) \end{cases}$$

onde $a_i \in \mathbb{Z}$, possui uma única solução módulo $n = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

Demonstração: Basta observar que $\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$. ■

4.1.3 Um Exemplo Astronômico

Nesta seção, veremos um exemplo de astronomia que é resolvido através de um sistema de congruências lineares.

Três satélites passarão sobre Alfenas-MG esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo 15 horas e o terceiro 19 horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem simultaneamente sobre Alfenas.

Vamos formular o problema matematicamente.

Chamaremos de x o número de horas, contadas a partir da meia-noite de hoje, quando os três satélites passarão sobre Alfenas. O primeiro satélite passa sobre Alfenas a cada 13 horas, a contar da 1 hora da madrugada. Logo $x = 1 + 13t$, para algum inteiro positivo t. Equivalentemente $x \equiv 1 \pmod{13}$. Para os outros satélites, temos que

$$x \equiv 4 \pmod{15} \quad e \quad x \equiv 8 \pmod{19}.$$

Os três satélites passarão juntos sobre Alfenas para os valores de x que satisfazem simultaneamente as três equações. Isto é, precisamos resolver o sistema

$$\begin{aligned} x &\equiv 1 \pmod{13} \\ x &\equiv 4 \pmod{15} \\ x &\equiv 8 \pmod{19} \end{aligned} \tag{4.4}$$

Observe que não podemos somar ou subtrair as equações entre si, já que os módulos são diferentes. Resolveremos o problema convertendo as equações de congruências em identidades de inteiros. Assim $x \equiv 1 \pmod{13}$ corresponde a $x = 1 + 13t$, que é um inteiro e, portanto, pode ser substituído na equação $x \equiv 4 \pmod{15}$ resultando em

$$1 + 13t \equiv 4 \ (mod\ 15) \text{ ou seja, } 13t \equiv 3 \ (mod\ 15)$$

Mas 13 é invertível módulo 15 e seu inverso é 7. Multiplicando $13t \equiv 3 \ (mod\ 15)$ por 7, e reduzindo os números módulo 15, obtemos

$$t \equiv 6 \ (mod\ 15)$$

Assim t é da forma $t = 6 + 15u$.

Portanto, $x = 1 + 13t \ \Rightarrow \ x = 1 + 13(6 + 15u) \ \Rightarrow \ x = 79 + 195u$.

Desta forma, qualquer número da forma $79 + 195u$ satisfaz as duas primeiras congruências do sistema (4.4). Por fim, vamos substituir $x = 79 + 195u$ na equação $x \equiv 8 \pmod{19}$, obtendo:

$$\begin{aligned} 79 + 195u &\equiv 8 \ (mod\ 19) \\ 195u &\equiv -71 \ (mod\ 19) \\ 195u &\equiv 5 \ (mod\ 19), \text{ pois como } \overline{71} + \overline{5} = \overline{76} = \overline{0} \ \Rightarrow \ -\overline{71} = \overline{5} \\ 5u &\equiv 5 \ (mod\ 19), \text{ pois } 195 \equiv 5 \ (mod\ 19) \end{aligned}$$

Como 5 é invertível módulo 19, podemos cancelá-lo na equação acima obtendo $u \equiv 1 \pmod{19}$ o que nos dá $u = 1 + 19v$, para algum inteiro v. Logo,

$$x = 79 + 195u \ \Rightarrow \ x = 79 + 195(1 + 19v) \ \Rightarrow \ x = 274 + 3705v.$$

Lembrando que x corresponde ao tempo contado a partir da meia-noite, queremos descobrir qual o **menor inteiro positivo** x que satisfaz as equações; esse inteiro é o 274. Portanto, os satélites passarão juntos pela primeira vez 274 horas depois da meia noite de hoje. Isto corresponde a 11 dias e 10 horas. Mas nossa solução nos diz mais. Somando um múltiplo qualquer de **3705** à 274 temos uma nova solução do sistema. Ou seja, os satélites voltarão a passar juntos a cada **3705** horas, que corresponde a 154 dias e 9 horas.

Observe que dividimos a solução desse sistema de 3 equações, de modo a resolver dois sistemas de duas equações. De fato, resolvendo a duas primeiras equações, obtivemos $x = 79 + 195u$. Isto corresponde a uma nova equação, que é $x \equiv 79 \ (mod\ 195)$. Para obter o valor final de x, resolvemos o sistema

$$\begin{aligned} x &\equiv 79 \ (mod\ 195) \\ x &\equiv 8 \ (mod\ 19) \end{aligned}$$

Em geral, a solução de um sistema de muitas equações é obtida através da solução de vários sistemas de duas equações.

4.2 Partilha de Senhas

Imagine que o cofre de um banco é aberto através de uma senha. Um certo número de funcionários desse banco tem acesso ao cofre. Mas o banco deseja, por segurança, que não seja possível abrir o cofre quando há menos de três desses funcionários presentes na agência. Digamos que há na agência 20 funcionários com acesso ao cofre. Como garantir que não será possível abrir o cofre a menos que haja, pelo menos, três desses funcionários presentes na agência?

Para abrir o cofre do banco é necessário conhecer a senha, que é um número s. Queremos partilhar s entre n pessoas. A cada pessoa será dado um elemento (sua "parte"da senha) de um conjunto $\mathbb{S}$ de n pares de inteiros positivos, de modo que, para um inteiro positivo $k \leq n$, previamente escolhido temos:

(1) qualquer subconjunto de $\mathbb{S}$ com k elementos permite determinar s facilmente;

(2) é muito difícil determinar s conhecendo menos que k elementos de $\mathbb{S}$.

A inspiração para a construção do conjunto $\mathbb{S}$ vem do Teorema Chinês do Resto.

DEFINIÇÃO 4.1 (LIMIAR DE UM CONJUNTO): Sejam $\mathcal{L}$ um conjunto de n inteiros positivos, dois a dois primos entre si, $\mathcal{N}$ o produto dos k menores números de $\mathcal{L}$ e $\mathcal{M}$ o produto dos $k-1$ maiores números de $\mathcal{L}$. Diremos que o conjunto $\mathcal{L}$ tem *limiar* k se

$$\mathcal{M} < s < \mathcal{N},$$

onde s é a senha que se quer partilhar entre n pessoas e que poderá ser escolhida como sendo qualquer inteiro no intervalo acima.

▷▷▷ **Exemplo 4.2:** Seja $\mathcal{L} = \{11,13,17,19,23\}$, vejamos se este conjunto possui limiar 2. Pela definição anterior, temos que:

$$\begin{aligned} \mathcal{N} &= 11 \cdot 13 = 143 \text{ (o produto dos 2 menores números de } \mathcal{L}) \\ \mathcal{M} &= 23 \text{ (o produto do 2-1 maiores números de } \mathcal{L}, \text{ ou seja, o próprio 23)} \end{aligned}$$

Como $\mathcal{M} < \mathcal{N}$, segue que $\mathcal{L}$ possui limiar 2 e o valor da senha s pode ser escolhido como sendo qualquer inteiro no intervalo (23,143).

⋆ OBSERVAÇÃO 4.1:A condição $\mathcal{M} < s < \mathcal{N}$ implica que o produto de k ou mais elementos de $\mathcal{L}$ é sempre maior ou igual a $\mathcal{N}$ e o produto de menos de k elementos é sempre menor ou igual a $\mathcal{M}$.

DEFINIÇÃO 4.2: Seja $\mathcal{L}$ um conjunto de n inteiros positivos, dois a dois primos entre si e com limiar k. Definimos o conjunto $\mathbb{S}$ como sendo

$$\mathbb{S} = \{(m,s_m), \text{ onde } m \in \mathcal{L} \text{ e } s_m \text{ é a forma reduzida de } s \text{ módulo } m\}$$

Note que o fato de termos um conjunto com limiar $k \geq 1$ implica que $s > m$, para qualquer $m \in \mathcal{L}$ e portanto, sempre temos $s_m < s$, qualquer que seja $m \in \mathcal{L}$.

▷▷▷ **Exemplo 4.3:** Com relação ao conjunto $\mathcal{L} = \{11,13,17,19,23\}$ do Exemplo 4.2, escolhendo o valor da senha como sendo $s = 30$ $(23 < s < 143)$, temos

$$\begin{aligned} \mathbb{S} &= \{(m,s_m), \text{ onde } m \in \mathcal{L} \text{ e } s_m \text{ é a forma reduzida de } s \text{ módulo } m\} \\ \mathbb{S} &= \{(11,30_{11}), (13,30_{13}), (17,30_{17}), (19,30_{19}), (23,30_{23})\} \\ \mathbb{S} &= \{(11,8), (13,4), (17,13), (19,11), (23,7)\} \end{aligned}$$

Voltando ao nosso problema inicial, suponhamos que mais de k funcionários se encontram no banco. Isso equivale a dizer que são conhecidos t dentre os pares $\mathbb{S}$ onde $t \geq k$. Denotaremos estes pares por $(m_1,s_1), \cdots, (m_t,s_t)$. Vamos resolver os

sistema de congruências

$$\begin{aligned} x &\equiv s_1 \quad (mod\, m_1) \\ x &\equiv s_2 \quad (mod\, m_2) \\ &\vdots \\ x &\equiv s_t \quad (mod\, m_t) \end{aligned} \tag{4.5}$$

De acordo com o Teorema Chinês do Resto, o sistema acima possui uma única solução em $\mathbb{Z}_{m_1 \cdot \ldots \cdot m_t}$, logo possui uma única solução inteira x_0 menor que $m_1 \cdot \ldots \cdot m_t$.

Observe que da maneira como foi construído o sistema acima, s é uma solução, mais ainda, como $t \geq k$, então $m_1 \cdot \ldots \cdot m_t \geq \mathcal{N} > s$.

Ou seja, s é uma solução do sistema (4.5) com a propriedade de ser menor do que $m_1 \cdot \ldots \cdot m_t$. Portanto, a unicidade do Teorema Chinês do Resto nos garante que $s = x_0$.

▷ ▷ ▷ **Exemplo 4.4:** Suponhamos que em um banco apenas 5 funcionários possuem acesso ao cobre e que pelo menos dois desses devem estar presentes para que o cofre possa ser aberto.

O conjunto $\mathcal{L}$ deve ter 5 elementos e seu limiar deve ser 2. O conjunto

$$\mathcal{L} = \{11{,}13{,}17{,}19{,}23\}$$

do exemplo 4.2 satisfaz as condições desejadas e escolhendo a senha do cofre como sendo $s = 30$, o exemplo 4.3 nos fornece:

$$\mathbb{S} = \{(11{,}8), (13{,}4), (17, 13), (19, 11), (23, 7)\},$$

desta forma, cada funcionário receberá uma senha pessoal que será um dos pares ordenados do conjunto acima.

Suponhamos que dois funcionários possuam as senhas (11,8) e (13,4) e desejam obter a senha. Para isso, é preciso resolver o sistema:

$$\begin{cases} x \equiv 8 \ (mod\ 11) \\ x \equiv 4 \ (mod\ 13) \end{cases}$$

Assim, $x = 8 + 11n$, com $n \in \mathbb{Z}$ e $x \equiv 4 \ (mod\ 13)$. Desta forma:

$$\begin{aligned} x &\equiv 4 \ (mod\ 13) \\ 8 + 11n &\equiv 4 \ (mod\ 13) \\ 11n &\equiv -4 \ (mod\ 13) \\ 11n &\equiv 9 \ (mod\ 13) \\ 6 \cdot 11n &\equiv 6 \cdot 9 \ (mod\ 13) \\ 66n &\equiv 54 \ (mod\ 13) \\ n &\equiv 2 \ (mod\ 13) \end{aligned}$$

Segue que $n = 2 + 13t$, com $t \in \mathbb{Z}$. Portanto, a solução geral do sistema é $x = 8 + 11 \cdot (2 + 13t) \Rightarrow x = 30 + 143t$, em que t é um inteiro positivo, isto é $x \equiv 30 \ (mod\ 143)$. Assim, determinamos que $s = 30$ é o valor correto da senha.

5

Criptografia RSA

A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. Todo processo de codificação é composto de duas etapas básicas: a codificação da mensagem e a decodificação da mensagem. Decodificar é o que um destinatário legítimo do código faz para ler a mensagem. A base teórica do processo de implantação da criptografia moderna é a aritmética modular, já estudada séculos antes por Euler, Gauss, Fermat entre outros.

O mais conhecido dos métodos de criptografia é o RSA que foi inventado em 1978 por Rivest, Shamir e Adleman. A implementação desse método de criptografia depende de dois primos distintos grandes p e q. Para codificar uma mensagem usando o RSA é suficiente conhecer o produto $n = pq$, denominado chave de decodificação (que é pública). Já, o processo de decodificação só é possível quando se conhecem os primos p e q. Como o processo de criptografia é implementado com números grandes, os cálculos são realizados por meio de computação algébrica, assunto que não será abordado nesse trabalho.

Estudaremos neste capítulo o sistema de criptografia RSA. Baseado em Coutinho, 2005 será feita uma abordagem da implementação, viabilidade e segurança desse sistema bem como seu processo de assinatura.

5.1 Implementação do Método

5.1.1 Pré-codificação

O processo de pré-codificação consiste em transformar a mensagem a ser codificada em uma sequência numérica. Para realizar a pré-codificação, converte-se letras em números usando a seguinte correspondência:

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

⋆ Observação 5.1:O espaço entre duas palavras é substituído pelo número 99.

▷▷▷ **Exemplo 5.1:** A frase

Paraty é Linda

convertida em números, fica

25102710293499149921182313 10

Feita a conversão da mensagem em números, deve-se agora determinar os parâmetros do sistema RSA que serão usados no processo de codificação. Estes parâmetros são dois primos distintos, que denotaremos por p e q. Coloquemos $n = pq$.

Para encerrar o processo de pré-codificação, a mensagem (já transformada em números) é quebrada em blocos que devem ser menores que n.

⋆ Observação 5.2:A escolha dos blocos não é única. É desejável que o bloco não comece por zero pois isso traria problemas no processo de decodificação.

▷▷▷ **Exemplo 5.2:** Se escolhermos $p = 11$ e $q = 13$, então $n = 143$. Assim, cada bloco da mensagem deve ser menor que 143. Colocando em blocos a mensagem do Exemplo 5.1, temos:

25 - 102 - 7 - 102 - 93 - 49 - 91 - 49 - 92 - 118 - 23 - 13 - 10

5.1.2 Codificação

A codificação da mensagem é feita usando n, que é o produto dos primos p e q, e um número inteiro positivo e inversível módulo $\phi(n)$. Ou seja, $mdc(e,\phi(n)) = 1$. Como p e q são primos, sabemos da Observação 3.7 que

$$\phi(n) = (p-1)(q-1)$$

O par (n, e) é a *chave de codificação* do sistema RSA. No processo de pré-codificação, a mensagem foi quebrada em blocos que serão codificados separadamente. Vamos denotar cada bloco por b e cada bloco codificado por $C(b)$. Assim:

$$C(b) = a$$

em que

$$b^e \equiv a \ (mod\ n)$$

▷▷▷ **Exemplo 5.3:** Vamos codificar o segundo bloco do Exemplo 5.2. Já temos que $p = 11$ e $q = 13$ assim:

$$\phi(n) = (11 - 1)(13 - 1) = 120$$

Adotando $e = 7$, segue que

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv -81 \cdot 138 \equiv 62 \cdot (-5) \equiv -310 \equiv -24 \equiv 119 \ (mod\ 143)$$

Assim, $C(102) = 119$

5.1.3 Decodificação

A decodificação da mensagem é processada a partir de dois números: n e o inverso de e em $\phi(n)$, que denotaremos por d. O par (n, d) é chamado de *chave de decodificação*. Sendo a o bloco codificado da mensagem, $D(a)$ será o resultado do processo de decodificação. Segue que:

$$D(a) = k$$

em que

$$a^d \equiv k \ (mod\ n)$$

⋆ Observação 5.3:Sendo b o bloco inicial da mensagem, teremos $k = b$, o que será demonstrado adiante. Em outras palavras, decodificando um bloco da mensagem codificada, espera-se encontrar o bloco correspondente da mensagem original.

▷▷▷ **Exemplo 5.4:** Vamos decodificar o bloco codificado no Exemplo 5.3. Para tanto, necessitamos calcular d. Como d é o inverso de e em $\phi(n)$, temos que:

$$d \cdot 7 \equiv 1 \ (mod\ 120)$$

Como $120 = 7 \cdot 17 + 1$, temos que $120 + 7 \cdot (-17) = 1$. Logo, $d = -17$. Como $-17 \equiv 103 \ (mod\ 120)$, temos que $d = 103$. Portanto, para decodificar o bloco mencionado, devemos resolver a equação:

$$119^{103} \equiv k \ (mod\ 143)$$

Através da computação algébrica , concluímos que $k = 102$ e $D(119) = 102$

5.2 Viabilidade do Método

Como visto, o método de criptografia só é útil se, decodificando um bloco codificado, obtemos o bloco correspondente da mensagem original. Sendo $C(b) = a$ o bloco codificado, queremos mostrar que $D(a) = b$, ou seja, $D(C(b)) = b$ para todo b entre

1 e n.

Sabemos, dos processos de codificação e decodificação definidos anteriormente, que

$$C(b) \equiv b^e \ (mod\ n) \text{ e } D(a) \equiv a^d \ (mod\ n)$$

Assim,

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

Ou seja, definidos os parâmetros p, q e $n = pq$ e ainda a chave de codificação (n, e) e a chave de decodificação (n, d), devemos mostrar que:

$$1 \ \leq \ b \ \leq \ n-1 \ \Rightarrow \ b^{ed} \equiv b \ (mod\ n)$$

No entanto, devemos mostrar apenas que $b^{ed} \equiv b \ (mod\ n)$, uma vez que, no processo de pré-codificação, b foi tomado no intervalo entre 1 e n.

⋆ Observação 5.4:Comentamos anteriormente que a mesagem deve ser quebrada em blocos menores que n e devem ser mantidos separados. Agora fica evidente a justificativa de tais comentários.

Sabe-se que $n = pq$ em que p e q são primos distintos. Como d é o inverso de e módulo $\phi(n)$, temos que

$$ed \equiv 1 \ (mod\ \phi(n))$$

ou seja $ed = 1 + k\phi(n), \ k \ \in \ \mathbb{Z}$. Assim,

$$ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$$

Logo

$$\begin{aligned} b^{ed} &\equiv b^{1+k(p-1)(q-1)} \ (mod\ p) \\ b^{ed} &\equiv b \cdot b^{k(p-1)(q-1)} \ (mod\ p) \\ b^{ed} &\equiv b \cdot (b^{p-1})^{k(q-1)} \ (mod\ p) \end{aligned} \tag{5.1}$$

Se p divide b, é evidente que $b^{ed} \equiv b \ (mod\ p)$. Suponhamos então que p não divide b. Segue então, pelo Teorema 3.5 que

$$p|(b^p - b) = b(b^{p-1} - 1)$$

e assim

$$b^{p-1} \equiv 1 \ (mod\ p). \tag{5.2}$$

Logo, de (5.1) e (5.2) concluímos que $b^{ed} \equiv b \ (mod\ p)$. Portanto, essa última congruência é válida para qualquer valor de b.

Analogamente, se q divide b, então $b^{ed} \equiv b \ (mod\ q)$. Se q não divide b, temos que

$$b^{q-1} \equiv 1 \ (mod\ q) \tag{5.3}$$

e ainda

$$\begin{aligned} b^{ed} &\equiv b^{1+k(p-1)(q-1)} \ (mod\ q) \\ b^{ed} &\equiv b \cdot b^{k(p-1)(q-1)} \ (mod\ q) \\ b^{ed} &\equiv b \cdot (b^{q-1})^{k(p-1)} \ (mod\ q) \end{aligned} \tag{5.4}$$

De (5.3) e (5.4) temos que $b^{ed} \equiv b \ (mod\ q)$.

Portanto, $b^{ed} - b$ é divisível por p e por q e, assim, também é divisível por pq uma vez que $mdc(p,q) = 1$. Como $n = pq$, concluímos que

$$b^{ed} \equiv b \ (mod\ n), \text{para qualquer } b \in \mathbb{Z}.$$

5.3 Segurança do Método

O sistema RSA de criptografia é de chave pública. Sendo assim, a chave de codificação (n, e) é acessível a qualquer usuário. A segurança do método se dá no fato de que é difícil calcular d quando apenas n e e são conhecidos. Nesta seção abordaremos tal dificuldade.

Na prática, d pode ser obtido aplicando o algoritmo euclidiano estendido a $\phi(n)$ e e. Em contrapartida, para obter $\phi(n)$, precisamos de p e q que podem ser obtidos fatorando n. Mas n é um número grande (por exemplo, 250 algarismos) e sendo assim, não existe algoritmo eficiente para fatorá-lo, tornando o feito muito difícil.

Suponhamos que $\phi(n)$ fora encontrado sem fatorar n. Conhecidos $n = pq$ e $\phi(n) = (p-1)(q-1)$, teremos:

$$\begin{aligned} \phi(n) &= (p-1)(q-1) \\ &= pq - (p+q) + 1 \\ &= n - (p+q) - 1 \\ p+q &= n - \phi(n) + 1 \end{aligned} \tag{5.5}$$

Contudo

$$\begin{aligned}(p+q)^2 - 4n &= p^2 + q^2 + 2pq - 4pq \\ &= (p-q)^2 \\ p-q &= \sqrt{(p+q)^2 - 4n} \end{aligned} \tag{5.6}$$

De (5.5) e (5.6), calculamos facilmente p e q, ou seja, fatoramos n. Logo, não é possível imaginar que consigamos achar $\phi(n)$ sem fatorar n, porque se ambos são conhecidos, também conhecemos os fatores de n.

Ademais, suponhamos que haja um algoritmo que calcule d diretamente a partir de n e e. Como $ed \equiv 1 \ (mod \ \phi(n))$, isto implica que conhecemos um múltiplo de $\phi(n)$. Isto também seria suficiente para fatorar n.

Por fim, encontrar b a partir da forma reduzida de b^e módulo n sem encontrar d requer um processo de tentativa-impraticável quando n é grande. Diante de todo o exposto, acredita-se que quebrar o RSA e fatorar n sejam equivalentes, tornando o método bastante seguro.

5.4 Processo de Assinatura

Em todo processo de mensagem eletrônica há, obviamente, o remetente e o destinatário. Este último necessita de uma garantia de que a mensagem teve origem no remente autorizado. Para tanto, faz-se um processo de assinatura eletrônica da mensagem.

Denotemos por C_r e D_r as funções de codificação e decodificação, respectivamente, do remetente e C_d e D_d as funções de codificação e decodificação, respectivamente, do destinatário. Seja b o bloco da mensagem a ser enviado. Ao invés do remetente enviar

$$C_d(b)$$

é enviado

$$C_d(D_r(b))$$

Tendo recebido o bloco $C_d(D_r(b))$, o destinatário aplica a função de decodificação obtendo

$$D_d(C_d(D_r(b))) = D_r(b)$$

e a este último bloco aplica a função codificação do remetente para obter b:

$$C_r(D_r(b)) = b$$

⋆ Observação 5.5:C_r é público e por isso é conhecido do destinatário.

6

Aplicação da Criptografia no Ensino Médio

6.1 Importância da Aplicação

Em geral, o conceito de número primo é introduzido nas escolas no 5º e 6º anos do Ensino Fundamental. Porém, isso é feito de modo superficial uma vez que, nessa fase do aprendizado, o aluno não tem conhecimento e maturidade para aprofundar no assunto sendo, portanto, um momento inoportuno para tal. A maioria dos alunos acaba decorando os primeiros números primos e a sua definição não se atentando para sua importância e aplicabilidade. No Ensino Médio (mais precisamente no 3º ano), podemos aprofundar o estudo da Teoria dos Números uma vez que, nessa fase, os alunos estão mais maduros e aptos ao entendimento das definições e propriedades que cercam os números inteiros.

As escolas que aderem à Olimpíada Brasileira de Matemática (OBM) ou à Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), na maioria das vezes, trabalham temas ligados à Teoria dos Números tais como primalidade, algoritmo de Euclides, congruência entre outros com alunos do ciclo básico de ensino. Nesse sentido, a OBM e a OBMEP são grandes motivadoras para que os alunos se interessem e estudem tais conteúdos.

Esse capítulo traz uma proposta para alunos do terceiro ano do Ensino Médio e visa o aprofundamento no tema de números primos e o estudo do conceito de congruência e suas propriedades culminando no método de criptografia RSA. Para tanto, sugerimos uma abordagem teórica e uma atividade prática com os alunos.

6.2 Abordagem Teórica do Método

Primeiramente, deve ser feito com a turma uma abordagem teórica sobre alguns tópicos da Teoria dos Números bem como o método de Criptografia RSA. Essa abordagem pode ser feita em sete aulas. Nessas aulas trabalharemos teoria e exemplos relacionados a cada tema. O professor deve ter a sensibilidade de saber até que ponto aprofundar a teoria uma vez que o público alvo pode ser heterogêneo e não ter muita

afinidade com a disciplina.

(1) Na primeira aula, será abordado o Algoritmo da Divisão Euclidiana, o conceito de múltiplos e divisores e a definição de mínimo múltiplo comum e máximo divisor comum.

(2) A segunda aula será dedicada aos números primos: sua definição e alguns tópicos relevantes à aplicação do método criptográfico. Deverá ser discutida a existência e a infinidade desses números, o Lema de Euclides e o Teorema Fundamental da Aritmética.

(3) A congruência módulo m será trabalhada na terceira e quarta aulas. Aqui será definida a congruência, estudada suas principais propriedades e apresentado os sistemas de congruência.

(4) A aula 5 será dedicada ao método de criptografia. Será trabalhada a pré-codificação, a codificação e a decodificação. Não será abordada a demonstração bem como a segurança e assinatura do método. Isso pode ser trabalhado em aulas especiais e com uma turma mais restrita.

(5) As aulas 6 e 7 serão dedicadas à atividade com os alunos.

Os planos de aula detalhados encontram-se no Apêndice 2.

6.3 Descrição da Atividade

A turma será divida em duplas e cada duas duplas "disputará" entre si codificando e decodificando uma mensagem sugerida pelo professor. Metade das duplas ficará responsável pela codificação da mensagem e a outra metade com a decodificação da mesma. Cada dupla estará sujeita ao ônus ou bônus de seus erros e acertos, respectivamente, previamente combinados com o professor. Por exemplo, pode ser feita a atribuição ou não de pontos extras aos alunos.

Descrevamos a atividade com duas duplas que designaremos por *dupla 1* e *dupla 2*:

(1) O professor atribuirá à *dupla 1* a mensagem

Paraty é Linda

sem que a *dupla 2* tenha conhecimento dessa mensagem.

(2) *dupla 1* deverá pré-codificá-la e codificá-la obtendo

25 - 102 - 7 - 102 - 93 - 49 - 91 - 49 - 92 - 118 - 23 - 13 - 10

na pré-codificação e

64 - 119 - 6 - 119 - 102 - 36 - 130 - 36 - 27 - 79 - 23 - 117 - 10

como codificação.

(3) A *dupla 2* receberá a mensagem codificada e terá que decodificá-la encontrando

25 - 102 - 7 - 102 - 93 - 49 - 91 - 49 - 92 - 118 - 23 - 13 - 10

e assim obter a mensagem original sugerida pelo professor.

(3) Se a mensagem obtida pela *dupla 2* for idêntica à mensagem original, as duplas levam o bônus da "disputa".

(4) Se a mensagem obtida pela *dupla 2* for diferente à original, cabe ao professor encontrar o erro cometido. Se o erro estiver na codificação, a *dupla 1* será onerada conforme o combinado; se o erro foi na decodificação, o ônus fica para a *dupla 2*.

Após o encerramento da atividade, é interessante que o professor refaça a mesma (com uma mensagem diferente) alternando o trabalho das duplas, ou seja, as duplas que codificaram ficarão responsáveis pela decodificação e vice-versa.

7

Apêndices

7.1 Apêndice 1: Introdução à Teoria de Anéis

Nessa seção, encontra-se a abordagem de alguns resultados sobre a teoria de anéis. Sua discussão basea-se em Gonçalves, 2015.

Definição 7.1 (Grupo Abeliano): Um sistema matemático constituído de um conjunto não vazio G e uma operação $(\star)$ sobre G é chamado *grupo abeliano* se essa operação satisfaz as seguintes propriedades:

(i) *Associativa*: $(a \star b) \star c = a \star (b \star c)$ quaisquer que sejam $a, b, c \in G$;

(ii) *Existência do elemento neutro*: existe um elemento $e \in G$ tal que $a \star e = e \star a = a$ qualquer que seja $a \in G$;

(iii) *Existência de simétricos*: para todo $a \in G$ existe um elemento $a' \in G$ tal que $a \star a' = a' \star a = e$;

(iv) *Comutativa*: $a \star b = b \star a$ quaisquer que sejam $a, b \in G$.

Definição 7.2 (Anel): Um anel é um conjunto $(R, \star, \triangle)$ onde $\star$ e $\triangle$ são operações binárias sobre R satisfazendo:

(i) (R,$\star$) é um grupo abeliano.

(ii) $\triangle$ é associativa, ou seja, $(a \triangle b) \triangle c = a \triangle (b \triangle c)$, para todo a, b, c $\in R$.

(iii) $\begin{cases} a \triangle (b \star c) = (a \triangle b) \star (a \triangle c) \\ (a \star b) \triangle c = (a \triangle c) \star (b \triangle c) \end{cases}$, para todo a, b, c $\in R$.

▷▷▷ **Exemplo 7.1:** $(\mathbb{Z}, +, \cdot)$ é um anel. De fato:

(i) ($\mathbb{Z}$,+) é abeliano.

(ii) O produto é associativo, ou seja, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo a, b, c $\in \mathbb{Z}$.

(iii) $\begin{cases} a \cdot (b+c) = a \cdot b + a \cdot c \\ (a+b) \cdot c = a \cdot c + b \cdot c \end{cases}$, para todo a, b, c $\in \mathbb{Z}$.

▷▷▷ **Exemplo 7.2:** $(\mathbb{Z}_m, \oplus, \odot)$ é um anel. De fato:

(i) $(\mathbb{Z}_m, \oplus)$ é grupo abeliano.

(ii) $\overline{a} \odot (\overline{b} \odot \overline{c}) = \overline{a} \odot (\overline{bc}) = \overline{abc} = (\overline{ab}) \odot \overline{c} = (\overline{a} \odot \overline{b}) \odot \overline{c}$, para todo a, b, c $\in \mathbb{Z}_m$

(iii) $\overline{a} \odot (\overline{b} \oplus \overline{c}) = \overline{a} \odot (\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} \oplus \overline{ac} = (\overline{a} \odot \overline{b}) \oplus (\overline{a} \odot \overline{c})$, para todo a, b, c $\in \mathbb{Z}_m$. De forma análoga, mostramos que $(\overline{a} \oplus \overline{b}) \odot \overline{c} = (\overline{a} \odot \overline{c}) \oplus (\overline{b} \odot \overline{c})$.

Definição 7.3 (Subanel): Seja S um conjunto não vazio de um anel $(R, \star, \triangle)$. Dizemos que $(S, \star, \triangle)$ é um subanel de $(R, \star, \triangle)$ se $(S, \star, \triangle)$ for um anel.

Teorema 7.1: Seja S um subconjunto não vazio de um anel $(R, \star, \triangle)$. Então $(S, \star, \triangle)$ é um subanel de $(R, \star, \triangle)$ se, e somente se, as seguintes condições são satisfeitas:

(i) Se $a, b \in S$, então $a \star b^{-1} \in S$.

(ii) Se $a, b \in S$, então $a \triangle b \in S$

Demonstração:

($\Rightarrow$) Como $(S, \star, \triangle)$ é um subanel de $(R, \star, \triangle)$, segue que $(S, \star, \triangle)$ é um anel. Logo, $(S,\star)$ é um grupo abeliano e consequentemente, a condição (i) é satisfeita.

Também pelo fato de $(S, \star, \triangle)$ ser um anel, temos que a operação $\triangle$ é binária sobre S, satisfazendo assim, a condição (ii).

($\Leftarrow$) Como $S \subset R$, $S \neq \varnothing$ e a condição (i) é válida, então temos que $(S,\star)$ é um subgrupo de $(R,\star)$. Como todo subgrupo de um grupo abeliano é abeliano, então $(S,\star)$ é um grupo abeliano.

Como $S \subset R$ e a segunda operação de S e R coincidem, o fato de $\triangle$ ser associativa em R garante que ela também o é em S.

A distributividade de $\triangle$ em relação a $\star$ em S segue de maneira análoga. ■

Definição 7.4 (Homomorfismo de Anéis): Sejam $(R, \star, \triangle)$ e $(S, \diamond, \wedge)$ anéis. Uma função $f : R \to S$ é um homomorfismo se $f(a \star b) = f(a) \diamond f(b)$ e $f(a \triangle b) = f(a) \wedge f(b)$, para todo a,b $\in R$.

⋆ Observação 7.1:Se a função $f : R \to S$ for bijetora, então f é dita um isomorfismo. Neste caso, R e S são ditos isomorfos. (NOTAÇÂO: $R \cong S$)

▷▷▷ **Exemplo 7.3:** $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_m, \oplus, \odot)$ dada por $f(a) = \overline{a}$ é um homomorfismo de anéis, ou seja $\mathbb{Z} \cong \mathbb{Z}_m$, pois:
$f(a+b) = \overline{a+b} = \overline{a} \oplus \overline{b} = f(a) \oplus f(b)$, para todo a,b $\in \mathbb{Z}$ e
$f(a \cdot b) = \overline{a \cdot b} = \overline{a} \odot \overline{b} = f(a) \odot f(b)$, para todo a,b $\in \mathbb{Z}$

▷▷▷ **Exemplo 7.4:** $f : \mathbb{Z} \to M_2(\mathbb{Z})$, dada por $f(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ é um homomorfismo de anéis, ou seja $\mathbb{Z} \cong M_2(\mathbb{Z})$. De fato:
$f(a+b) = \begin{bmatrix} a+b & 0 \\ 0 & a+b \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = f(a) + f(b)$, para todo a,b $\in \mathbb{Z}$
e
$f(a \cdot b) = \begin{bmatrix} a \cdot b & 0 \\ 0 & a \cdot b \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \cdot \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = f(a) \cdot f(b)$, para todo a,b $\in \mathbb{Z}$.

Definição 7.5 (Ideal): Sejam $(R, \star, \triangle)$ um anel e $(S, \star, \triangle)$ um subanel de $(R, \star, \triangle)$. Dizemos que S é um ideal de R se $r \triangle x \in S$ e $x \triangle r \in S$, para todo $x \in S$ e $r \in R$.

▷▷▷ **Exemplo 7.5:** $I = (5\mathbb{Z}, +, \cdot)$ é um ideal de $(\mathbb{Z}, +, \cdot)$. De fato:

(i) I é um subanel de $(\mathbb{Z}, +, \cdot)$.

(ii) Seja $r \in \mathbb{Z}$ e $x \in 5\mathbb{Z}$. Daí, segue $x = 5k$, $k \in \mathbb{Z}$. Logo, $r \cdot x = r \cdot 5k = 5(rk) \in 5\mathbb{Z}$ e $x \cdot r = 5k \cdot x = 5(kx) \in 5\mathbb{Z}$.

Teorema 7.2: Seja $f : (R, \star, \triangle) \to (S, \diamond, \wedge)$ um homomorfismo e S' um subanel de S. Então $f^{-1}(S')$ é um subanel de R.

Demonstração: Temos que $f(e_R) = e_S \in S' \Rightarrow e_R \in f^{-1}(S')$, logo $f^{-1}(S') \neq \varnothing$.
Agora, mostraremos que se a_1 e $a_2 \in f^{-1}(S')$, então $a_1 \star a_2^{-1} \in f^{-1}(S')$.De fato, $f(a_1 \star a_2^{-1}) = f(a_1) \diamond f(a_2^{-1}) = f(a_1) \diamond (f(a_2))^{-1} \in S' \Rightarrow a_1 \star a_2^{-1} \in f^{-1}(S')$.
Por fim, basta mostrar que se a_1 e $a_2 \in f^{-1}(S')$, então $a_1 \triangle a_2 \in f^{-1}(S')$.Temos que $f(a_1 \triangle a_2) = f(a_1) \wedge f(a_2) \in S' \Rightarrow a_1 \triangle a_2 \in f^{-1}(S')$.
Portanto,
$f^{-1}(S')$ é subanel de R. ■

Corolário 7.1: Se $f : (R, \star, \triangle) \to (S, \diamond, \wedge)$ é um homomorfismo, então $f^{-1}(\{e_S\})$ é um subanel de R.

DEFINIÇÃO 7.6 (KERNEL): O subanel $f^{-1}(\{e_S\})$ do Corolário 7.1, é chamado de núcleo (ou kernel) de f. (NOTAÇÃO: $ker(f)$).

DEFINIÇÃO 7.7 (ANEL QUOCIENTE): Sejam $(R, \star, \triangle)$ um anel e I um ideal de R. O anel $(\frac{R}{I}, \diamond, \wedge)$ é denominado anel quociente de R por I.

TEOREMA 7.3 (PRIMEIRO TEOREMA DO ISOMORFISMO): Seja $f : (R, \star, \triangle) \to (S, \diamond, \wedge)$ um homomorfismo. Então

$$\frac{R}{kerf} \cong Im(f)$$

Demonstração: Defina $\varphi : \frac{R}{kerf} \to Im(f)$ dada por $\varphi(r \star kerf) = f(r)$

1. A função φ está bem definida:

   Se $r \star kerf = r' \star kerf$, então: $(r')^{-1} \in kerf$. Daí, temos que:

   $$f((r')^{-1} \star r) = e_s \in S \text{ e ainda}$$
   $$(f(r'))^{-1} \diamond f(r) = e_s \in S. \text{ Logo:}$$
   $$f(r) = f(r') \text{ e pontanto}$$
   $$\varphi(r \star kerf) = \varphi(r' \star kerf).$$

2. A função φ é homomorfismo:
   De fato:

   Sejam $r_1, r_2 \in R$
   $\varphi[(r_1 \star kerf) \star (r_2 \star kerf)] = \varphi[(r_1 \star r_2) \star kerf)] = f(r_1 \star r_2) = f(r_1) \diamond f(r_2) = \varphi(r_1 \star kerf) \diamond \varphi(r_2 \star kerf)$ e

   $\varphi[(r_1 \triangle kerf) \triangle (r_2 \triangle kerf)] = \varphi[(r_1 \triangle r_2) \triangle kerf)] = f(r_1 \triangle r_2) = f(r_1) \wedge f(r_2) = \varphi(r_1 \triangle kerf) \wedge \varphi(r_2 \triangle kerf)$

3. A função φ é injetora:
   De fato:
   Sejam $r_1, r_2 \in R$

   Se $\varphi(r_1 \star kerf) = \varphi(r_2 \star kerf)$, então $f(r_1) = f(r_2)$, Assim:

   $$(f(r_2))^{-1} \diamond f(r_1) = e_S \Rightarrow$$

$$f(r_2^{-1} \star r_1) = e_S \Rightarrow$$
$$r_2^{-1} \star r_1 \in kerf \Rightarrow$$
$$r_1 \star kerf = r_2 \star kerf$$

4. A função φ é sobrejetora:

   Seja $y \in Im(f)$, então $y = f(r)$ para algum $r \in R$. Como $r \star Ker(f) \in R/Ker(f)$ e $\varphi(r \star Ker(f)) = f(r) = y$, segue que φ é sobrejetora.

■

▷▷▷ **Exemplo 7.6:** Seja $f : (\mathbb{Z}_4, \oplus, \odot) \to (\mathbb{Z}_2, \oplus, \odot), talque f(\overline{0}) = \overline{0}, f(\overline{1}) = \overline{1}, f(\overline{2}) = \overline{1}$ e $f(\overline{3}) = \overline{1}$.

(i) f e um homomorfismo.

(ii) $Im(f) = \mathbb{Z}_2$

(iii) $kerf = \{\overline{0}, \overline{2}\}$

Pelo Primeiro Teorema do Isomorfismo, temos:

$$\frac{\mathbb{Z}_4}{\{\overline{0}, \overline{2}\}} \cong \mathbb{Z}_2$$

7.2 Apêndice 2: Planos de Aula

7.2.1 Aula 1

1. **Tema:** Múltiplos e Divisores.
2. **Objetivo:** Trabalhar com os alunos conceitos básicos acerca dos números inteiros tais como divisão Euclidiana, múltiplos, divisores, mínimo múltiplo comum e máximo divisor comum.
3. **Recursos e Materiais:** Lousa, pincel e lista de exercícios.
4. **Duração:** Cinquenta minutos.
5. **Desenvolvimento:**

   - Fazer uma breve abordagem histórica com ênfase na Grécia Antiga citando Euclides e os *"Elementos"*.
   - Abordar o Algoritmo da Divisão Euclidiana chamando atenção para o resto e sua relação com o quociente, uma vez que ele será bastante útil no entendimento do método criptográfico. Apresentar alguns exemplos numéricos.

- Definir múltiplos e divisores. Trabalhar com exemplos numéricos. Chamar atenção para a quantidade finita de divisores e infinita de múltiplos.
- Ensinar aos alunos o método para se calcular a quantidade de divisores de um número inteiro.
- Definir mínimo múltiplo comum e abordar o método para seu cálculo usando fatoração numérica.
- Definir máximo divisor comum e abordar o método para seu cálculo. Pode-se trabalhar com os alunos o método da fatoração numérica e o método das divisões sucessivas (Exemplo 2.11).
- Apresentar aos alunos o Teorema 2.8. Trabalhar com exemplo numérico.
- Resolver com os alunos os exercícios apresentados na subseção 7.2.5.

7.2.2 Aula 2

1. **Tema:** Números Primos.
2. **Objetivo:** Trabalhar o conceito de números primos, discutir sua infinidade e alguns teoremas que o cercam.
3. **Recursos e Materiais:** Lousa, pincel e lista de exercícios.
4. **Duração:** Cinquenta minutos.
5. **Desenvolvimento:**

   - Definir número primo e comentar sobre sua infinidade (caso haja interesse da turma, demonstrar).
   - Definir número composto.
   - Definir números primos entre si. Mostrar alguns exemplos numéricos.
   - Apresentar, utilizando um exemplo numérico, o Crivo de Eratóstenes.
   - Comentar sobre o teste da raiz para verificação da primalidade de um número.
   - Apresentar aos alunos o Lema 2.1 (Lema de Euclides). Comentar sua reciprocidade e trabalhar alguns exemplos.
   - Enunciar o Teorema 2.7 (Teorema Fundamental da Aritmética). Trabalhar alguns exemplos numéricos.
   - Resolver com os alunos os exercícios apresentados na subseção 7.2.5.

7.2.3 Aulas 3 e 4

1. **Tema:** Congruência.
2. **Objetivo:** Definir Congruência Módulo m em $\mathbb{Z}$. Estudar suas propriedades e a resolução de sistemas de congruência.

3. **Recursos e Materiais:** Lousa, pincel e lista de exercícios.
4. **Duração:** Uma hora e quarenta minutos.
5. **Desenvolvimento:**
    - Definir Relação de Equivalência. Apresentar aos alunos alguns exemplos.
    - Definir Congruência Módulo m $\mathbb{Z}$. Comentar que a congruência é uma relação de equivalência. Fazer alguns exmeplos numéricos.
    - Apresentar aos alunos e Teorema 3.2 exemplificando-o numericamente.
    - Abordar o Teorema 3.4.
    - Definir a Função Fi de Euler.
    - Apresentar as Proposições 3.1 e 3.2 e propor alguns exemplos aos alunos.
    - Apresentar aos alunos o Teorema 3.5 (Pequeno Teorema de Fermat).
    - Definir Sistema de Congruência e apresentar um exemplo aos alunos.
    - Resolver o exemplo apresentado no item anterior.
    - Resolver com os alunos os exercícios apresentados na subseção 7.2.5.

7.2.4 Aula 5

1. **Tema:** Criptografia.
2. **Objetivo:** Apresentar aos alunos o método de criptografia: da pré-codificação à decodificação bem como sua viabilidade.
3. **Recursos e Materiais:** Lousa, pincel e projetor de slides.
4. **Duração:** Cinquenta minutos.
5. **Desenvolvimento:**
    - Fazer uma breve abordagem histórica sobre a criptografia.
    - Discutir com os alunos a importância do método de criptografia para segurança de mensagens eletrônicas.
    - Explicar aos alunos, através de um exemplo, como funciona o processo de pré-codificação. Comentar sobre a escolha dos primos e a importância de dividir a mensagem em blocos.
    - Explicar como funciona o processo de codificação da mensagem. Neste momento pode ser usado algum programa computacional (com o auxílio do projetor) para o cálculo do resto e obtenção da mensagem codificada.
    - Explicar como funciona o processo de decodificação. Assim como no item anterior, o recurso computacional pode ser usado.
    - Mostrar a viabilidade do método.
    - Comentar que pode ser realizado um processo de assinatura, sem entrar em muitos detalhes.

7.2.5 Exercícios Propostos

Aula 1

1. Quantos divisores positivos possui o número 4500?

2. (ENEM/2014) Durante a Segunda Guerra Mundial, para decifrarem as mensagens secretas, foi utilizada a técnica de decomposição em fatores primos. Um número N é dado pela expressão $2^x \cdot 5^y \cdot 7^z$ na qual x, y e z são números inteiros não negativos. Sabe-se que N é múltiplo de 10 e não é múltiplo de 7. O número de divisores de N, diferentes de N é:

   (a) $x \cdot y \cdot z$

   (b) $(x+1)(y+1)$

   (c) $x \cdot y \cdot z - 1$

   (d) $(x+1)(y+1)z$

   (e) $(x+1)(y+1)(z+1) - 1$

3. (UEL-PR) Considere dois rolos de barbante, um com $96m$ e outro com $150m$ de comprimento. Pretende-se cortar todo o barbante dos dois rolos em pedaços de mesmo comprimento. O menor número de pedaços que poderá ser obtido é:

   (a) 38

   (b) 41

   (c) 43

   (d) 52

   (e) 55

4. (UPF-RS) Três didades resolveram realizar um evento no ano 2000. A cidade A decidiu que, a partir de então, ele se realizará de 5 em 5 anos; a cidade B decidiu que ele se repetirá de 3 em 3 anos; e a cidade C, de 6 em 6 anos. As cidades A, B e C realizarão novamente o evento no mesmo ano em:

   (a) 2014

   (b) 2090

   (c) 2030

   (d) 2021

   (e) 2006

5. Sejam a, b e d números inteiros. Suponha que d divide a. Mostre que:

   (a) Se d também divide b, então d divide $a - b$.

   (b) Se d também divide $a + b$, então d divide b.

   (c) Se d também divide $a - b$, então d divide b.

6. (OBMEP/2006) Da igualdade $9174532 \cdot 13 = 119268916$ pode-se concluir que um dos números abaixo é divisível por 13. qual é este número?

   (a) 119268903

   (b) 119268907

   (c) 119268911

   (d) 119268913

   (e) 119268923

Aula 2

1. Considere todos os números primos maiores que 30 e menores que 40. A soma desses números é:

   (a) 55

   (b) 68

   (c) 101

   (d) 118

   (e) 75

2. Verifique se o número 329 é primo.

3. (BB/20105) O número natural $2^{103} + 2^{102} + 2^{101} + 2^{100}$ é divisível por

   (a) 6

   (b) 10

   (c) 14

   (d) 22

   (e) 26

4. (ENC/98) Uma das afirmativas abaixo sobre números naturais é falsa. Qual é ela?

   (a) Dado um número primo, existe sempre um número primo acima dele.

   (b) Se dois números não primos são primos entre si, um deles é ímpar.

   (c) Um número primo é sempre ímpar.

   (d) O produto de três números naturais consecutivos é múltiplo de 6.

   (e) A soma de três números naturais consecutivos é múltiplo de 3.

5. Determine se existem inteiros positivos x e y que satisfaçam a equação $30^x \cdot 35^y = 21^x \cdot 140 \cdot 5^{2x}$

6. (OBMEP/2007) Quais números naturais m e n satisfazem a $2^n + 1 = m^2$?

Aulas 3 e 4

1. Ache o resto da divisão de 7^{10} por 51.
2. Para todo $n \in \mathbf{N}$, mostre que $101^{6n} - 1$ é divisível por 70.
3. Mostre que $42|a^7 - a$ para todo número natural a.
4. Determine o valor de $\phi(58)$.
5. Resolva, quando possível, as congruências:
   (a) $3X \equiv 5$ $(mod\ 7)$
   (b) $12X \equiv 36$ $(mod\ 28)$
   (c) $151X \equiv 11$ $(mod\ 245)$
6. Ache todos os números inteiros que deixam restos 2, 3 e 4 quando divididos por 3, 4 e 5, respectivamente.

8

Considerações Finais

Este trabalho foi de grande importância uma vez que contribuiu para aprimorar meu aprendizado acerca da teoria dos números, sua importância e a necessidade de se trabalhar esse conteúdo, ainda com mais empenho, no ensino médio.

O objetivo proposto na dissertação foi atingido, uma vez que o estudo de alguns tópicos da Teoria dos Números e da Álgebra abordados foi importante para o entendimento de algumas aplicações desta área como o Teorema Chinês do Resto e sua aplicação num método de criptografia para partilha de senhas e criptografia RSA. Este trabalho é uma complementação do trabalho de conclusão de curso (TCC) da graduação, trabalho este que já previa o estudo de um exemplo de criptografia. Trabalhos futuros podem incorporar o estudo aqui realizado a fim de implementar outras aplicações para alunos de ensino médio ou fundamental.

Bibliografia

[1] Coutinho, Severino Collier: *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2005, ISBN 9788524401249.

[2] Gonçalves, Adilson: *Introdução à Álgebra*. Rio de Janeiro: IMPA, 2015, ISBN 9788524401084.

[3] Hefez, Abramo: *Aritmética*. Rio de Janeiro: SBM, 2014, ISBN 9788585818920.

[4] Landau, Edmund: *Teoria Elementar dos Números*. Rio de Janeiro: Moderna, 2002, ISBN 8573931744.

[5] Milies, Francisco César Polcino e Sonia Pitta Coelho: *Uma Introdução à Matemática*. São Paulo: Edusp, 2003, ISBN 9788531404580.

[6] Oliveira Santos, José Plínio de: *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2015, ISBN 9788524401428.

[7] Ribenboim, Paulo: *Números Primos: Mistérios e Recordes*. Rio de Janeiro: IMPA, 2001, ISBN 9788524401688.

[8] Sampaio, João Carlos Vieira e Paulo Antônio Silvani Caetano: *Introdução à Teoria dos Números: um Curso Breve*. São Carlos: EdUFSCar, 2007, ISBN 8576001276.