UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e
Computação Científica

LUCAS DE OLIVEIRA ALVES MAURICIO

TEORIA DOS NÚMEROS E A CRIPTOGRAFIA RSA

Campinas

2024

Lucas de Oliveira Alves Mauricio

TEORIA DOS NÚMEROS E A CRIPTOGRAFIA RSA

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática Aplicada.

Orientador: José Plínio de Oliveira Santos

Este trabalho corresponde à versão final da Dissertação defendida pelo aluno Lucas de Oliveira Alves Mauricio e orientada pelo Prof. Dr. José Plínio de Oliveira Santos.

Campinas

2024

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

M446t

Mauricio, Lucas de Oliveira Alves, 1999-
Teoria dos números e a criptografia RSA / Lucas de Oliveira Alves Mauricio. – Campinas, SP : [s.n.], 2024.

Orientador: José Plínio de Oliveira Santos.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos números. 2. Criptografia de chaves públicas. 3. Assinaturas digitais. I. Santos, José Plínio de Oliveira, 1951-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: Number theory and the RSA cryptography
Palavras-chave em inglês:
Number theory
Public key cryptography
Digital signatures
Área de concentração: Matemática Aplicada
Titulação: Mestre em Matemática Aplicada
Banca examinadora:
José Plínio de Oliveira Santos [Orientador]
Robson Oliveira da Silva
Aurelio Ribeiro Leite de Oliveira
Data de defesa: 06-02-2024
Programa de Pós-Graduação: Matemática Aplicada

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0001-9088-7618
- Currículo Lattes do autor: http://lattes.cnpq.br/2909405465563545

Dissertação de Mestrado defendida em 06 de fevereiro de 2024 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS

Prof(a). Dr(a). ROBSON OLIVEIRA DA SILVA

Prof(a). Dr(a). AURELIO RIBEIRO LEITE DE OLIVEIRA

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Quero expressar minha profunda gratidão a todos aqueles que desempenharam papéis significativos em minha jornada até aqui. Em primeiro lugar, quero estender meu sincero agradecimento à minha amada família, cujo apoio incansável foi meu alicerce nos momentos mais desafiadores. À minha namorada, expresso minha gratidão pela presença constante e apoio emocional que sempre ofereceu.

Além disso, não posso deixar de agradecer à respeitável instituição que confiou em meu potencial, abrindo as portas para meu crescimento acadêmico e desenvolvimento como pesquisador. Essa oportunidade foi fundamental para a construção do meu conhecimento e habilidades.

Quero estender meus agradecimentos aos colegas de jornada, cuja camaradagem tornou minha experiência ainda mais enriquecedora. Observar que não estava sozinho em algumas situações fortaleceu o sentido de comunidade e solidariedade, proporcionando um ambiente propício para o aprendizado e crescimento mútuo.

Cada um de vocês contribuiu de maneira única para minha jornada, e sou profundamente grato por compartilhar esse capítulo significativo da minha vida com uma rede de apoio tão incrível. Obrigado por fazerem parte dessa trajetória e por tornarem esta conquista ainda mais especial.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

Neste presente trabalho, exploraremos a teoria dos números para fundamentar o estudo da criptografia RSA, que consiste no uso de uma chave pública e uma privada para a codificação e decodificação de uma mensagem. Devido à sua fácil implementação e sua difícil quebra de sigilo, estaremos interessados em descobrir o porquê.

Palavras-chave: Números Inteiros; Congruência; Criptografia; Chave Pública; Chave Privada; Sistema RSA.

Abstract

In this present work, we will explore number theory to underpin the study of RSA cryptography, which involves the use of a public and private key for the encryption and decryption of a message. Due to its ease of implementation and its robust secrecy, we will be interested in uncovering the reasons behind its effectiveness.

Keywords: Integers; Congruence; Cryptography; Public Key; Private Key; RSA System.

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

Os números inteiros têm sido objeto de estudo desde os tempos antigos devido às suas propriedades matemáticas. Sua importância remonta ao princípio da civilização, quando as pessoas perceberam a necessidade de contar objetos, pessoas e animais.

Matemáticos ao longo da história têm dedicado tempo considerável para explorar tais propriedades, desvendando seus mistérios e deixando algumas perguntas que não foram respondidas até hoje. Essas propriedades foram estudadas por matemáticos ao longo dos séculos. Desde gregos como Euclides, até matemáticos mais recentes como Fermat, Euler e Gauss, em que cada geração contribuiu com novas descobertas e teoremas relacionados aos números inteiros.

Essa exploração matemática alcançou muitos avanços, incluindo a aplicação dos números inteiros na criptografia e na segurança da informação e foi com a chegada da era moderna, mais especificamente, dos computadores, que uma pergunta crucial permanecia sem resposta: como transmitir mensagens de conteúdo delicado de maneira segura através dos computadores? Veremos mais à frente que essa questão foi finalmente respondida em 1977 por três matemáticos que implementaram a criptografia RSA.

A criptografia RSA se baseia nas propriedades únicas dos números inteiros para alcançar a segurança na transmissão de dados estabelecida pela dificuldade conhecida como *o problema de fatoração*; o algoritmo RSA foi pioneiro ao permitir tanto a criptografia quanto a autenticação digital, tornando-se uma ferramenta essencial para proteger a privacidade e a integridade das comunicações digitais. Essa característica a transforma em um elemento fundamental de segurança, viabilizando a transmissão segura de informações confidenciais em ambientes de rede, tanto públicos quanto privados.

Portanto, fica evidente que os números inteiros desempenham um papel significativo neste estudo e, a seguir, vamos aprofundar nossa análise em seus resultados para fundamentar nosso estudo na criptografia RSA.

1 Números Inteiros

Temos que a origem e a construção dos números inteiros foi devido à necessidade dos homens de expressarem situações envolvendo problemas de contagem, que posteriormente envolveu situações de lucros e prejuízos. A rigor matemático, a construção de tal conjunto envolveu grandes dificuldades de matemáticos da época, em que mais detalhes pode ser encontrado em (REZENDE; DASSIE, 2010). Nesse contexto, apresentaremos algumas características dos números inteiros que podem ser localizadas em (SANTOS, 1998; IEZZI; DOMINGUES, 1970; HEFEZ, 2016; BURTON, 2010; COUTINHO, 1997).

1.1 Propriedades Básicas

As operações de adição e multiplicação em $\mathbb{Z}$ possuem as seguintes propriedades:

Propriedade 1. *Para todo* $a, a', b, b', c \in \mathbb{Z}$*, temos:*

1. *Se* $a = a'$ *e* $b = b'$*, então:*

$$\begin{cases} a + b = a' + b' \\ a \cdot b = a' \cdot b' \end{cases}$$

2. *(comutatividade)*

$$\begin{cases} a + b = b + a \\ a \cdot b = b \cdot a \end{cases}$$

3. *(Associatividade)*

$$\begin{cases} a + (b + c) = (a + b) + c \\ a \cdot (b \cdot c) = (a \cdot b) \cdot c \end{cases}$$

4. *(Elemento Neutro)*

$$\begin{cases} a + 0 = a \\ a \cdot 1 = a \end{cases}$$

5. *(Simétrico)* $\exists b = (-a)$ *tal que* $a + b = a + (-a) = 0$.

6. *(Distributiva)* $a \cdot (b + c) = ab + cd$.[1]

[1] (HEFEZ, 2016), página 3.

Observação 1. *Note que o conjunto dos números inteiros é particionado em três subconjuntos* $\mathbb{Z} = (-\mathbb{N}) \cup \{0\} \cup \mathbb{N}$*, em que* $-\mathbb{N}$ *é o conjunto simétrico de* $\mathbb{N}$*.*

Proposição 1. $a \cdot 0 = 0$ *para todo* $a \in \mathbb{Z}$*.*[1]

Demonstração. Temos que $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ (1). Por outro lado, $0 = a \cdot 0 - a \cdot 0$ (2). Logo, de (2) e (1), segue que $0 = a \cdot 0 - a \cdot 0 = (a \cdot 0 + a \cdot 0) - a \cdot 0 = a \cdot 0 + (a \cdot 0 - a \cdot 0) = a \cdot 0$.

□

Proposição 2. $\forall a, b, c \in \mathbb{Z}$*, temos que* $a = b \Leftrightarrow a + c = b + c$*.*

Demonstração. ($\Rightarrow$) Segue pelas propriedades dos números inteiros.

($\Leftarrow$) Reciprocamente, se $a + c = b + c$. Somando $-c$ em ambos os lados da igualdade, temos:

$$a + c + (-c) = b + c + (-c) = a + b.$$

□

Exemplo 1. *Para todo* $a \in \mathbb{Z}$*, mostre que* $(-1)a = -a$*.*

Demonstração. De fato, $0 = a \cdot 0 = a \cdot (1 - 1) = a - a = a + (-1)a$. Somando $-a$ em ambos os lados da igualdade, temos que $-a = -a + a + (-1)a = (-1)a$.

□

Propriedade 2. *O conjunto* $\mathbb{N} \subset \mathbb{Z}$ *é fechado para a multiplicação e adição, ou seja, dados quaisquer* $a, b \in \mathbb{N}$*:*

$$a + b \in \mathbb{N} \qquad a \cdot b \in \mathbb{N}.$$[2]

Exemplo 2. $A = \{\cdots, -3, -2, -1\}$ *não é fechado para a multiplicação, pois dados* $-3, -2 \in A$*, temos que* $(-3) \cdot (-2) = 6 \notin A$*.*

Definição 1. *Dados* $a, b \in \mathbb{Z}$*, se* $a \leq b$ *então* $a = b$ *ou* $b - a \in \mathbb{N}$*.*

Se $a \neq b$ então existe $c \in \mathbb{N}$ tal que $b - a = c \Leftrightarrow b = a + c \Leftrightarrow a < b$.

Propriedade 3. (*Tricotomia*)[3] *Dados* $a, b \in \mathbb{Z}$*, apenas uma das possibilidades é válida:*

i) $a = b$*;*

ii) $b - a \in \mathbb{N}$*;*

iii) $a - b \in \mathbb{N}$*.*

[1] Proposição 1 e 2; (HEFEZ, 2016), página 4.
[2] (HEFEZ, 2016), página 6.
[3] Propriedade 3; (HEFEZ, 2016), página 6.

Proposição 3. *$\forall a, b, c \in \mathbb{Z}$, $a < b$ e $b < c$ então $a < c$.*[1]

Demonstração. Se $a < b$ e $b < c$ então $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$. Como $\mathbb{N}$ é fechado em $\mathbb{Z}$, segue que $(b - a) + (c - b) = c - a \in \mathbb{N}$, ou seja, $a < c$.

□

Proposição 4. *Se $a, b, c \in \mathbb{Z}$, então $a < b \Leftrightarrow a + c < b + c$.*

Proposição 5. *Se $a, b \in \mathbb{Z}$ e $c \in \mathbb{N}$, então $a < b \Leftrightarrow a \cdot c < b \cdot c$.*

Proposição 6. *$\forall a, b, c \in \mathbb{Z}$ e $\forall c \in \mathbb{Z} \setminus \{0\}$, então $a = b \Leftrightarrow a + c = b + c$.*

Demonstração. Análogas à demonstração feita acima.

□

Note que $a \leq b$ é um relação de ordem, ou seja:

$$\begin{cases} a \leq a \\ a \leq b,\ b \leq a \Rightarrow a = b \\ a \leq b,\ b \leq c \Rightarrow a \leq c \end{cases}, \forall a, b, c \in \mathbb{Z}.$$

De fato:

1. Seja $a \in \mathbb{Z}$ tal que $a \leq a$, então $a - a = 0 \geq 0$, ou seja, $a = a$.

2. Sejam $a, b \in \mathbb{Z}$ tais que $a \leq b$ e $b \leq a$, então $0 \leq b - a$ (1) e $0 \leq a - b$ (2). Somando (1) e (2), temos que $0 \leq b - a + a - b = 0$. o que implica que $a = b$.

3. Sejam $a, b, c \in \mathbb{Z}$ tais que $a \leq b$ e $b \leq c$, então $0 \leq b - a$ (1) e $0 \leq c - b$ (2). Logo, somando (1) e (2), segue que $0 \leq b - a + c - b = c - a$. Assim, $a \leq c$.

Portanto, $\leq$ é uma relação de ordem.

Definição 2. *(Módulo)*[2] *Seja $a \in \mathbb{Z}$, definimos:*

$$|a| = \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{se } a < 0 \end{cases}$$

O número inteiro $|a|$ é chamado de módulo (ou valor absoluto) de a.

[1] Proposições $3, 4, 5, 6$; (HEFEZ, 2016), páginas $6 - 7$.
[2] (HEFEZ, 2016), página 8.

Propriedade 4. *$\forall a, b \in \mathbb{Z}$ e $r \in \mathbb{N}$, temos:*

i) $|a \cdot b| = |a| \cdot |b|$;

ii) $|a| \leq r \Leftrightarrow -r \leq a \leq r$;

iii) $-|a| \leq a \leq |a|$;

iv) $||a| - |b|| \leq |a \pm b| \leq |a| + |b|$.[1]

1.2 Princípio da Boa Ordenação

As propriedades descritas acima, tanto os conjuntos dos racionais ($\mathbb{Q}$) quanto o conjunto dos reais ($\mathbb{R}$) também o possuem, mas o conjunto dos números inteiros se distingue precisamente pela sua característica de ordenação.

Definição 3. *Dizemos que um subconjunto $S \in \mathbb{Z}$ é limitado inferiormente, se existir $c \in \mathbb{Z}$ tal que $c \leq x$, $\forall x \in S$.*[2]

Dizemos que $a \in S$ é o mínimo de S se $a \leq x$, $\forall x \in S$.

Exemplo 3. *Sejam $S = \{0, 1, 2, 3, 4, 5\}$ e $c = -1$, então:*

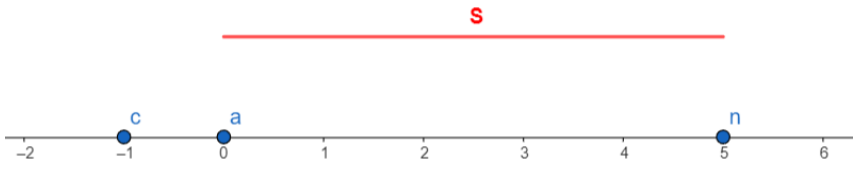


Figura 1: Cota inferior de S.

em que c é chamado de cota inferior de S.

Definição 4. *Se $T \subset \mathbb{Z}$ for limitado superiormente, então $\exists b \notin T$ tal que $b = max\ T$.*

Propriedade 5. *(Princípio da boa ordenação)*[3] *Se $S \subset \mathbb{Z}$, $S \neq \varnothing$ e limitado inferiormente, então $\exists m = min\ S$, em que $m \in S$.*

[1] (HEFEZ, 2016), página 8
[2] (IEZZI; DOMINGUES, 1970), página 30.
[3] (HEFEZ, 2016), página 10.

Exemplo 4. $\mathbb{Q}$ *não satisfaz esse princípio, pois* $S = (0,1) \cap \mathbb{Q} \neq \varnothing$*, em que* S *é limitado inferiormente por zero, mas não existe* $a \in S$ *tal que* $a \leq x$*,* $\forall x \in S$*, haja vista que existem infinitos números racionais entre* 0 *e* 1*.*

Proposição 7. *Não existe nenhum* $n \in \mathbb{Z}$ *tal que* $0 < n < 1$*.*[1]

Demonstração. Suponha por absurdo que exista $n \in \mathbb{Z}$ tal que $0 < n < 1$, em que $S = \{x \in \mathbb{Z} \mid 0 < x < 1\} \neq \varnothing$. Observe que S é limitado inferiormente por $c = 0$, $\forall x \in S$, $x > 0$. Logo, pelo Princípio de Boa Ordenação (PBO), segue que existe $m \in S$ tal que $m = min\ S$, ou seja, $m \leq x$, $\forall x \in S$ e $0 < m < 1$. Multiplicando esta última desigualdade por m, temos:

$$0 < m^2 < m < 1$$

Assim, $m^2 \in S$ e $m^2 < m$, o que é um absurdo pois $m = min\ S$. Portanto, não existe nenhum $n \in \mathbb{Z}$ tal que $0 < n < 1$.

□

Propriedade 6. (*Propriedade Arquimediana*)[2] *Sejam* $a, b \in \mathbb{Z}$*, com* $b \neq 0$*. Então existe* $n \in \mathbb{Z}$ *tal que* $nb > a$*.*

Demonstração. Suponha por absurdo que para todo $n \in \mathbb{Z}$, $a \geq nb$. Seja $S = \{a - nb \mid n \in \mathbb{Z}\}$, note que $S \neq \varnothing$, pois $a - nb \geq 0$, ou seja, $S \subset \mathbb{Z}$. Assim, pelo PBO existe $n_1 \in \mathbb{Z}$ tal que $a - n_1 b$ é o menor elemento de S. Ora, note que $a - ((n_1 + 1)b) = (a - n_1 b) - b < a - n_1 b$. O que é um absurdo, haja vista que n_1 é o menor elemento de S. Portanto, existe $n \in \mathbb{Z}$ tal que $nb > a$.

□

Teorema 1. (*Princípio da indução matemática*)[3] *Seja* S *um subconjunto dos inteiros positivos. Se* S *possui as duas seguintes propriedades:*

i) $1 \in S$

ii) $k + 1 \in S$ *sempre que* $k \in S$

então S *contém todos os inteiros positivos.*

[1] (HEFEZ, 2016), página 10.
[2] (HEFEZ, 2016), página 11.
[3] Teoremas $1, 2, 3$; (HEFEZ, 2016), página 13.

Demonstração. Seja $T = \{x \in \mathbb{Z} \mid x \geq a\}$ e suponha por absurdo que $T \nsubseteq S$. Logo, $T \setminus S \neq \varnothing$ e, como T é limitado inferiormente por a e S um subconjunto de $\mathbb{Z}$ (logo é limitado), segue que $T \setminus S$ é limitado inferiormente. Assim, pelo PBO segue que existe $\exists c \in T \setminus S$ tal que $c = min\ T \setminus S$. Logo, $c \in T$ e $c \notin S$ e ainda $c > a$ (pois a é o menor elemento de T e $c \neq a$). Daí, $c-1 \in T$ e $c-1 \in S$, pois $c-1 \geq a$ e se $c-1 \notin S$, teríamos $c-1 \in T \setminus S$. O que é um absurdo, haja vista que $c \in T \setminus S$ e $c = min\ T \setminus S$. Assim, $c-1 \in S$ e por (ii), segue que $(c-1)+1 = c \in S$, o que é um absurdo, pois $c \in T \setminus S$. Portanto, $T \subset S$.

□

Teorema 2. (*Primeiro Princípio da Indução Finita*) *Sejam $a \in \mathbb{Z}$ e $p(n)$ uma sentença aberta em n. Suponha que:*

(i) *$p(a)$ verdadeiro*

(ii) *$\forall n \geq a$, $p(n)$ é verdadeiro $\Rightarrow p(n+1)$ verdadeiro.*

Então $p(n)$ é verdadeiro $\forall n \geq a$.

Demonstração. Considere:

$$S = \{n \in \mathbb{Z} \mid p(n) \text{ verdadeiro}\}$$

Por (i) se $p(a)$ for verdadeiro, então $a \in S$, por (ii) e pelo Teorema anterior, segue que se $n \in S \Rightarrow p(n)$ verdadeiro e $n+1 \in S \Rightarrow p(n+1)$ verdadeiro. Logo, $\{n \in \mathbb{Z} \mid n \geq a\} \subset S$, isto é, $p(n)$ é verdadeiro para todo $n \geq a$.

□

Exemplo 5. *Mostre que* $1 + x + x^2 + \cdots + x^{n-1} = \dfrac{x^n - 1}{x - 1}$, $\forall n \in \mathbb{N} \cup \{0\}$.

Demonstração. Seja $n = 0$, então $x^0 = 1 = \dfrac{x-1}{x-1}$. Suponha que $\forall n \in \mathbb{N} \cup \{0\}$, $p(n) = 1 + x + x^2 + \cdots + x^{n-1} = \dfrac{x^n - 1}{x - 1}$ (H.I). Mostremos que para $n+1$ a igualdade é verdadeira, ou seja, $1 + x + x^2 + \cdots + x^{n-1} + x^n = \dfrac{x^{n+1} - 1}{x - 1}$. Com efeito, $1 + x + x^2 + \cdots + x^{n-1} + x^n = (1 + x + x^2 + \cdots + x^{n-1}) + x^n \overset{\text{H.I}}{=} \dfrac{x^n - 1}{x - 1} + x^n = \dfrac{x^n - 1 + x^{n+1} - x^n}{x - 1} = \dfrac{x^{n+1} - 1}{x - 1}$. Portanto, pelo Princípio de Indução Finita, segue que $1 + x + x^2 + \cdots + x^{n-1} = \dfrac{x^n - 1}{x - 1}$, $\forall n \in \mathbb{N} \cup \{0\}$.

□

Teorema 3. (*Segundo Princípio da Indução Finita*) *Seja $p(n)$ uma sentença aberta em n tal que*

(*i*) *$p(a)$ é verdadeiro*

(*ii*) *Se $\forall n \leq k$, $p(n)$ é verdadeiro $\Rightarrow p(k+1)$ é verdadeiro.*

Então $p(n)$ é verdadeiro $\forall n \geq a$.

Demonstração. Análogo ao primeiro princípio.

□

Definição 5. *A sequência de Fibonacci é uma sequência de números naturais em que cada número é encontrado somando-se os dois números anteriores de sua sequência.*

Exemplo 6. *Para todo par de números n e m da sequência de Fibonacci, temos que $u_{n+m} = u_n u_{m+1} + u_{n-1} u_m$.*

Demonstração. Fixando n, mostremos por indução em m. De fato, para $m = 1$, temos que $u_{n+1} = u_n + u_{n-1} = u_n u_2 + u_{n-1} u_1$, haja vista que $u_1 = u_2 = 1$. Suponha que para todo $i \leq m$ a igualdade seja válida, ou seja, $u_{n+m} = u_n u_{m+1} + u_{n-1} u_m$. Mostremos que para $m+1$ a igualdade seja verdadeira, isto é, $u_{n+m+1} = u_n u_{m+2} + u_{n-1} u_{m+1}$. Note que:

$$u_{n+m} = u_n u_{m+1} + u_{n-1} u_m$$
$$u_{n+m-1} = u_n u_m + u_{n-1} u_{m-1}$$

Com efeito, $u_{n+m+1} = u_{n+m} + u_{n+m-1} = u_n u_{m+1} + u_{n-1} u_m + u_n u_m + u_{n-1} u_{m-1} = u_n (u_{m+1} + u_m) + u_{n-1} (u_m + u_{m-1}) = u_n u_{m+2} + u_{n-1} u_{m+1}$. Portanto, pelo princípio de indução, $u_{n+m} = u_n u_{m+1} + u_{n-1} u_m$.

□

1.3 Divisibilidade em $\mathbb{Z}$

Os métodos de divisibilidade são feitos para verificarmos se um determinado número é divisível por outro, a seguir enumeramos alguns resultados nas quais estaremos dispostos a determinar quando isto ocorre e quando não ocorrer, qual será seu resto.

Definição 6. *Sejam $a, b \in \mathbb{Z}$, dizemos que a divide b, denotado por $a \mid b$ se, e somente se, existe um inteiro $c \in \mathbb{Z}$ tal que $b = ac$. Se a não divide b, escrevemos $a \nmid b$.*[1]

[1] (SANTOS, 1998), página 3.

Observação 2. *Note que $a \mid b$ é diferente de $\frac{a}{b}$, haja vista que $a \mid b$ é uma relação entre números e $\frac{a}{b}$ é um número. Além disso, se $a \mid b$ então $\exists c \in \mathbb{Z}$ tal que $b = ac$, em que $c = \frac{b}{a}$.*

Propriedade 7. *Dados a, b, $c \in \mathbb{Z}$, temos:*

(1) $0 \mid 0$;

(2) $1 \mid a$, $a \mid a$, $a \mid 0$, $\forall a \in \mathbb{Z}$;

(3) $0 \mid a \Leftrightarrow a = 0$;

(4) $a \mid b \Leftrightarrow |a| \mid |b|$;

(5) *Se* $a \mid b$ *e* $b \mid c$ *então* $a \mid c$;

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

(7) $a \mid b$ *e* $b \mid a \Leftrightarrow a = b$.[1]

Proposição 8. *Sejam $a, b, c, d \in \mathbb{Z}$, se $a \mid b$ e $c \mid d$ então $ac \mid bd$.*[2]

Demonstração. De fato, se $a \mid b$ e $c \mid d$ então $\exists x_1, x_2 \in \mathbb{Z}$ tais que $b = ax_1$ e $d = cx_2$. Logo, $bd = (ax_1)(cx_2) = ac(x_1x_2)$. Portanto, $ac \mid bd$.

□

Em particular, se $a \mid b$ e $c \mid c$ então $ac \mid bc$.

Proposição 9. *Se $a \mid (b \pm c)$ então $a \mid b \Leftrightarrow a \mid c$.*

Demonstração. Consideremos o caso $b + c$.

($\Rightarrow$) Se $a \mid (b + c)$ e $a \mid b$, então existem $x, y \in \mathbb{Z}$ tais que $b + c = ax$ e $b = ay$. Logo, $c = ax - b = ax - ay = a(x - y) = az$, em que $z = x - y \in \mathbb{Z}$. Assim, $a \mid c$.

($\Leftarrow$) Reciprocamente, se $a \mid c$ e $a \mid b$, então existem $z, w \in \mathbb{Z}$ tais que $c = az$ e $b = aw$. Logo, $b + c = aw + az = a(w + z) = ax$, em que $x = w + z \in \mathbb{Z}$. Assim, $a \mid (b + c)$.

Analogamente temos o caso $b - c$.

□

[1] (HEFEZ, 2016), página 40; (SANTOS, 1998), página 3.
[2] Proposições 8 a 13; (HEFEZ, 2016), páginas 41 – 44.

Proposição 10. *Dados $a, b, c \in \mathbb{Z}$ tal que $a \mid b$ e $a \mid c$, então $\forall x, y \in \mathbb{Z}$, $a \mid bx + cy$.*

Demonstração. Temos que, se $a \mid b$ e $a \mid c$, então existem $z_1, z_2 \in \mathbb{Z}$ tais que $b = az_1$ (I) e $c = az_2$ (II). Multiplicando (I) por x e (II) por y, segue que $bx = az_1x$ e $cy = az_2y$. Somando, temos $bx + cy = az_1x + az_2y = a(z_1x + z_2y) = ar$, em que $r = z_1x + z_2y \in \mathbb{Z}$. Portanto, $a \mid bx + cy$.

□

Proposição 11. *Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ então $a - b \mid a^n - b^n$.*

Demonstração. Por indução em n.

De fato, para $n = 1$, temos que $a - b \mid a - b$, pois existe $c = 1 \in \mathbb{Z}$ tal que $a - b = (a - b) \cdot 1$. Suponha que para todo $n \in \mathbb{N}$ a relação seja válida, ou seja, que $a - b \mid a^n - b^n$ (H.I). Mostremos que para $n + 1$ a relação também é verdadeira, isto é, $a - b \mid a^{n+1} - b^{n+1}$. Com efeito, $a^{n+1} - b^{n+1} = aa^n - bb^n = aa^n - ab^n + ab^n - bb^n = a(a^n - b^n) + b^n(a - b)$. Como $a - b \mid a^n - b^n$ pela (H.I) e $a - b \mid a - b$, segue pela Proposição 10, que $a - b \mid a(a^n - b^n) + b^n(a - b) = a^{n+1} - b^{n+1}$. Portanto, pelo princípio de indução finita $a - b \mid a^n - b^n$.

□

Exemplo 7. *Temos que $10^n - 2^n$ é divisível por 8. De fato, pela proposição anterior e sendo $a = 10$ e $b = 2$, segue que $8 \mid 10^n - 2^n$, $\forall n \in \mathbb{N}$.*

Proposição 12. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Então $a + b \mid a^{2n+1} + b^{2n+1}$.*

Demonstração. Por indução em n.

De fato, para $n = 0$, temos que $a + b \mid a + b$, pois existe $c = 1 \in \mathbb{Z}$ tal que $a + b = (a + b) \cdot 1$. Suponha que para todo $n \in \mathbb{N} \cup \{0\}$ a relação seja válida, ou seja, que $a + b \mid a^{2n+1} + b^{2n+1}$ (H.I). Mostremos que para $n + 1$ a relação também é verdadeira, isto é, $a + b \mid a^{2(n+1)+1} + b^{2(n+1)+1}$. Com efeito, $a^{2n+3} + b^{2n+3} = a^2a^{2n+1} + b^2b^{2n+1} = a^2a^{2n+1} - b^2a^{2n+1} + b^2a^{2n+1} + b^2b^{2n+1} = a^{2n+1}(a^2 - b^2) + b^2(a^{2n+1} + b^{2n+1})$. Como $a + b \mid a^2 - b^2 = (a + b)(a - b)$ e $a + b \mid a^{2n+1} + b^{2n+1}$ pela (H.I). Assim, temos que $a + b \mid a^{2n+1}(a^2 - b^2) + b^2(a^{2n+1} + b^{2n+1}) = a^{2n+3} + b^{2n+3}$. Portanto, pelo princípio de indução finita $a + b \mid a^{2n+1} + b^{2n+1}$.

□

Proposição 13. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então $a + b \mid a^{2n} - b^{2n}$.*

Demonstração. Por indução em n.

De fato, para $n = 1$, temos que $a+b \mid a^2-b^2 = (a+b)(a-b)$. Agora, suponha que a relação seja verdadeira para todo $n \in \mathbb{N}$, ou seja, que $a+b \mid a^{2n}-b^{2n}$ (H.I). Mostremos que a relação é verdadeira para $n+1$, isto é, que $a+b \mid a^{2(n+1)} - b^{2(n+1)}$. Com efeito, $a^{2n+2} - b^{2n+2} = a^2a^{2n} - b^2b^{2n} = a^2a^{2n} - b^2a^{2n} + b^2a^{2n} - b^2b^{2n} = a^{2n}(a^2-b^2) + b^2(a^{2n}-b^{2n})$. Como $a+b \mid a^2-b^2$ e $a+b \mid a^{2n}-b^{2n}$ pela (H.I), segue que $a+b \mid a^{2n}(a^2-b^2)+b^2(a^{2n}-b^{2n}) = a^{2n+2} - b^{2n+2}$. Portanto, pelo princípio de indução, segue que $a+b \mid a^{2n} - b^{2n}$.

□

Teorema 4. *(Divisão Euclidiana)*[1] *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = bq + r, \;\; 0 \leq r < |b|.$$

Demonstração. Primeiro mostremos que existem $q, r \in \mathbb{Z}$ tais que $a = bq+r, \;\; 0 \leq r < |b|$. Considere $S = \{a - by \mid y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$. Pela Propriedade arquimediana, segue que existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$. Logo, $a-nb > 0 \in S$ e assim, $S \neq \varnothing$. Como S é limitado inferiormente por zero, segue do PBO que existe $r \in \mathbb{Z}$ tal que $r = min\ S$. Como $r \in S$, segue existe $q \in \mathbb{Z}$ tal que $r = a - bq \Leftrightarrow a = bq + r$ (1) e segue daí que $r \geq 0$. Mostremos agora que $r < |b|$. Para isso, suponha por absurdo que $r \geq |b|$, isto é, que $r = |b| + s$, em que $s \in \mathbb{N} \cup \{0\}$ (note que $r > s$). Logo, $s = r - |b| \overset{(1)}{=} a - bq - |b| = a - b\,(q \pm 1) \in S$ e $0 \leq s < r$. O que é um absurdo, pois $r = min\ S$. Portanto, existem $q, r \in \mathbb{Z}$ tais que $a = bq + r, \;\; 0 \leq r < |b|$.

Mostremos agora que q e r são únicos. Para isso, sejam $q_1, r_1 \in \mathbb{Z}$, que satisfaça $a = bq_1 + r_1$, $0 \leq r_1 < |b|$. Logo $bq + r = bq_1 + r_1 \Leftrightarrow b\,(q - q_1) = r_1 - r$. Como $r < |b|$ e $r_1 < |b|$, segue que $r_1 - r < |b|$ e daí, $|r_1 - r| < |b|$. Assim, $|b(q_1 - q)| = |b|\,|q - q_1| = |r_1 - r| < |b|$ e isso só é verdade se $|q - q_1| = 0$, isto é, se $q - q_1 = 0 \Leftrightarrow q = q_1$. Logo, $|r_1 - r| = 0 \Leftrightarrow r_1 - r = 0 \Leftrightarrow r_1 = r$. Portanto $\exists! q, r \in \mathbb{Z}$ tal que $a = bq + r, \;\; 0 \leq r < |b|$.

□

Observação 3. *q e r são chamados respectivamente de quociente e resto da divisão de a por b.*

Exemplo 8. ***Algoritmo de Divisão***

[1] (HEFEZ, 2016), página 46.

Entradas: Inteiros positivos a *e* b.

Saída: Inteiros não negativos q *e* r *tais que* $a = bq + r$ *e* $0 \leq r < b$.

```
a = int(input('Digite o dividendo: '))
b = int(input('Digite o divisor: '))
q = 0
r = a
if b == 0:
    print('Não se pode dividir por zero')
while True:
    if r >= b:
        r -= b
        q += 1
    elif r < b:
        print(f'O quociente é {q} e o resto é {r}')
        break

```

Figura 2: Algoritmo de divisão

```
Digite o dividendo: 733
Digite o divisor: 2
O quociente é 366 e o resto é 1

Process finished with exit code 0
```

Figura 3: Exemplo

1.4 Máximo Divisor Comum

O máximo divisor comum, como o próprio nome já expressa, é o maior número que divide simultaneamente dois números os mais, como veremos a seguir.

Definição 7. *Dados* $a, b \in \mathbb{Z}$, *dizemos que* $d \in \mathbb{Z}$ *é o máximo divisor comum entre* a *e* b *(denotado por* $mdc(a, b)$*) se, e somente se:*

(i) $d \geq 0$;

(ii) $d \mid a$ *e* $d \mid b$;

(iii) *Se* $d_1 \mid a$ *e* $d_1 \mid b$ *então* $d_1 \mid d$.[1] $(d_1 \leq d)$

[1](IEZZI; DOMINGUES, 1970), página 39.

Notação: $mdc(a, b) = d$.

Propriedade 8. *Para todo a, b e $d \in \mathbb{Z}$, segue que:*

(1) *Se $mdc(a, b) = d$ e $mdc(a, b) = d_1 \Rightarrow d = d_1$;*

(2) $mdc(a, b) = mdc(b, a)$;

(3) $mdc(a, 0) = |a|$;

(4) $mdc(a, 1) = 1$;

(5) $mdc(0, 0) = 0$;

(6) $mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b) = d$;

(7) $a \mid b \Leftrightarrow mdc(a, b) = |a|$.[1]

Lema 1. *Se $d = mdc(a, b - na)$, então $d = mdc(a, b)$.*[2]

Demonstração. Seja $d = mdc(a, b - na)$, pelas propriedades de mdc temos que $d \geq 0$ e $d \mid a$ e $d \mid b - na$ e pelas propriedades de divisibilidade temos que, se $d \mid a$ então $d \mid na$. Logo, $d \mid b - na + na = b$. Assim $d \mid b$. Agora, tomando $d_1 \in \mathbb{Z}$ tal que $d_1 \mid a$ e $d_1 \mid b$, segue que se $d_1 \mid a$ então $d_1 \mid na$ e assim, $d_1 \mid b - na$. Como por hipótese $d = mdc(a, b - na)$, segue que $d_1 \mid d$. Portanto $d = mdc(a, b)$.

□

Observação 4. *Note que este Lema nos diz que no $mdc(a, b)$, podemos retirar do maior valor, um múltiplo $n \in \mathbb{Z}$ do menor valor, em que o mdc continuará o mesmo.*

Teorema 5. *Sejam $a, b \in \mathbb{Z}$ e $a = bq + r$, $q \in \mathbb{Z}$ e $0 \leq r < |b|$ então $mdc(a, b) = mdc(b, r)$.*[3]

Demonstração. Seja $a = bq + r$, em que $q \in \mathbb{Z}$ e $0 < r < |b|$. Tomando $mdc(a, b)$ e pelo lema anterior, temos:

$$\begin{aligned} mdc(a, b) &= mdc(b, a) \\ &= mdc(b, bq + r) \\ &= mdc(b, r). \end{aligned}$$

[1] (HEFEZ, 2016), páginas $74 - 75$.
[2] (HEFEZ, 2016), página 75.
[3] (SANTOS, 1998), página 7.

□

Exemplo 9. *Mostremos que dado $a \in \mathbb{Z}$, com $a \neq 1$ e $m \in \mathbb{N}$, então* $mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc(a-1, m)$.

Demonstração. Temos que:

$$\begin{aligned} mdc\left(\frac{a^m-1}{a-1}, a-1\right) &= mdc(a^{m-1}+a^{m-2}+\cdots+a+1, a-1) \\ &= mdc((a^{m-1}-1)+\cdots+(a-1)+1+(m-1), a-1) \\ &= mdc((a^{m-1}-1)+\cdots+(a-1)+m, a-1) \end{aligned}$$

Pelas Proposições 9, 10 e 11 segue que $a-1 \mid (a^{m-1}-1)+(a^{m-2}-1)+\cdots+(a-1)$, isto é, $(a^{m-1}-1)+(a^{m-2}-1)+\cdots+(a-1) = n(a-1)$. Logo, $mdc(n(a-1)+m, a-1) = mdc(a-1, n(a-1)+m)$. Daí, pelo Lema 1 e pelo Teorema anterior, segue que $mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc(a-1, m)$.

□

Algoritmo de Euclides para MDC: O objetivo é encontrar o máximo divisor comum de dois inteiros a e b (que podemos supor estritamente positivos), por meio de aplicações sucessivas do algoritmo euclidiano. Suponha que $a > b$. Primeiro vamos aplicar o algoritmo euclidiano para a e b, depois de b e o primeiro resto parcial, e assim por diante, ou seja:

$$\begin{aligned} a &= bq_1 + r_1 \qquad (0 \leq r_1 < b) \\ b &= r_1q_2 + r_2 \qquad (r_2 < r_1) \\ r_1 &= r_2q_3 + r_3 \qquad (r_3 < r_2) \end{aligned}$$

Se r_1 for nulo, então $b = mdc(a, b)$ devido a propriedade (7) de mdc e o processo termina na primeira etapa. Se $r_1 \neq 0$, passa-se à segunda e se raciocina da mesma maneira com relação a r_2. Se $r_2 = 0$, então $r_1 = mdc(a, b)$, devido ao Teorema 5 e a propriedade (7), temos que $mdc(b, r) = mdc(a, b)$. E assim por diante.

Ocorre que, como $b > r_1 > r_2 > \cdots > r_n > 0$, então para algum índice n teremos que $r_{n+1} = 0$. De fato, se todos os elementos de $\{r_1, r_2, \cdots\}$ fossem não nulos, então esse conjunto que é limitado inferiormente, não teria mínimo, o que é impossível. Portanto, segue que $r_n = mdc(r_n, r_{n-1}) = mdc(r_{n-1}, r_{n-2}) = \cdots = mdc(r_1, b) = mdc(a, b)$. Portanto, o *mdc* entre dois valores é o último resto não nulo entre as sucessivas divisões.

Exemplo 10. *(Método Prático) Calcule o mdc de* 4921 *e* 96608. *Temos que:*

	19	1	1	1	2	1	1	13	19
96608	4921	3109	1812	1297	515	267	248	19	1
3109	1812	1297	515	267	248	19	1	0	

Tabela 1: Algoritmo de Euclides Estendido

Portanto $mdc(4921, 96608) = 1$.

Note que no exemplo acima, o Algoritmo de Euclides nos fornece:

$$1 = 248 - 13 \cdot 19$$
$$19 = 267 - 1 \cdot 248$$
$$248 = 515 - 1 \cdot 267$$
$$267 = 1297 - 2 \cdot 515$$
$$515 = 1812 - 1 \cdot 1297$$
$$1297 = 3109 - 1 \cdot 1812$$
$$1812 = 4921 - 1 \cdot 3109$$
$$3109 = 96608 - 19 \cdot 4921$$

Logo:

$$\begin{aligned} 1 &= 248 - 13 \cdot 19 \\ &= 248 - 13(267 - 248) \\ &= 14 \cdot 248 - 13 \cdot 267 \\ &= 14(515 - 267) - 13 \cdot 267 \\ &= 14 \cdot 515 - 27 \cdot 267 \\ &= 14 \cdot 515 - 27(1297 - 2 \cdot 515) \\ &= 68 \cdot 515 - 27 \cdot 1297 \end{aligned}$$

$$= 68(1812 - 1297) - 27 \cdot 1297$$
$$= 68 \cdot 1812 - 95 \cdot 1297$$
$$= 68 \cdot 1812 - 95(3109 - 1812)$$
$$= 163 \cdot 1812 - 95 \cdot 3109$$
$$= 163(4921 - 3109) - 95 \cdot 3109$$
$$= 163 \cdot 4921 - 258 \cdot 3109$$
$$= 163 \cdot 4921 - 258(96608 - 19 \cdot 4921)$$
$$= 5065 \cdot 4921 - 258 \cdot 96608$$

Assim, $mdc(4921, 96608) = 1 = 5065 \cdot 4921 - 258 \cdot 96608$.

Note que conseguimos utilizar o Algoritmo de Euclides para expressar o $mdc(a, b) = d$ na forma $ax + by = d$ e iremos nos referir a tal fato como *Algoritmo de Euclides Estendido.*

Definição 8. *Sejam $a, b, d \in \mathbb{Z}$. definimos:*

$$I(a, b) = \{ax + by | x, y, \in \mathbb{Z}\}$$

e

$$d\mathbb{Z} = \{d \cdot t | t \in \mathbb{Z}\}.$$

Em particular, $I(0, 0) = \{0\}$. Se, a e b não são simultaneamente nulos, então $I(a, b) \cap \mathbb{N} \neq \varnothing$. De fato, $a^2 + b^2 \in I(a, b)$, pois $a^2 + b^2 = a \cdot a + b \cdot b$. Sendo $a \neq 0$ ou $b \neq 0$, então $a^2 + b^2 > 0$, e daí, $a^2 + b^2 \in \mathbb{N}$.

Teorema 6. *Sejam a, $b \in \mathbb{Z}$, ambos não nulos. Se $d = min\,(I(a, b) \cap \mathbb{N})$, então:*

(i) $d = mdc(a, b)$;

(ii) $I(a, b) = d\mathbb{Z}$.[1]

Demonstração. *(i)* Mostremos que $d = mdc(a, b)$. Logo, mostremos que d possui as 3 propriedades de *mdc*.

[1] (HEFEZ, 2016), página 80.

Note que $d = min\,(I(a,b)) \cap \mathbb{N} \geq 0$. Agora, suponha que $d_1 \mid a$ e $d_1 \mid b$. Como $d \in I(a,b)$, segue que existem $x, y \in \mathbb{Z}$ tal que $d = ax + by$. Pelas propriedades de divisibilidade, segue que:

$$\begin{cases} d_1 \mid a \\ d_1 \mid b \end{cases} \Rightarrow \begin{cases} d_1 \mid ax \\ d_1 \mid by \end{cases} \Rightarrow\ d_1 \mid ax + by = d$$

Por último, observe que $a,\ b \in I(a,b)$, pois $a = a \cdot 1 + b \cdot 0$ e $b = a \cdot 0 + b \cdot 1$. Logo, segue que $d \mid a$ e $d \mid b$. Portanto, $d = mdc(a,b)$.

(ii) Mostremos que $I(a,b) = d\mathbb{Z}$.

$(\subset)$ Seja $z \in I(a,b)$, mostremos que se $z \in I(a,b)$ qualquer então $d \mid z$.

Suponha por absurdo que $d \nmid z$, então pela Divisão Euclidiana, temos que:

$$z = dq + r, \text{ com } 0 < r < d.$$

Como $z \in I(a,b)$, segue que existem $x_1, y_1 \in \mathbb{Z}$ tal que $z = ax_1 + by_1$. Por outro lado, como $d \in I(a,b)$, segue que:

$$\begin{aligned} z &= dq + r \\ ax_1 + by_1 &= (ax + by)q + r \\ r &= a(x_1 - xq) + b(y_1 - yq), \qquad 0 < r < d. \end{aligned}$$

Tomando $x_2 = x_1 - xq$ e $y_2 = y_1 - yq$, temos $0 < r = ax_2 + by_2 \in I(a,b) \cap \mathbb{N}$. O que é um absurdo, haja vista que $r < d$ e $d = min\,(I(a,b) \cap \mathbb{N})$. Portanto, $d \mid z$. Assim, segue que existe $t \in \mathbb{Z}$ tal que $z = dt \in d\mathbb{Z}$ e, portanto, $I(a,b) \subset d\mathbb{Z}$.

$(\supset)$ Seja $z \in d\mathbb{Z}$, logo existe $k \in \mathbb{Z}$ tal que $z = dk$. Como $d \in I(a,b)$, segue que existem $a,\ b \in \mathbb{Z}$ tal que $d = ax + by$. Assim, $dk = a(xk) + b(yk) = z$. Tomando $x_1 = xk \in \mathbb{Z}$ e $y_1 = yk \in \mathbb{Z}$, segue que $z = ax_1 + by_1 \in I(a,b)$. Portanto, $d\mathbb{Z} \subset I(a,b)$.

□

Corolário 1. $mdc(na, nb) = nmdc(a,b)$.[1]

[1] (HEFEZ, 2016), página 81.

Demonstração. Observe que:

$$\begin{aligned} I(na, nb) &= \{(na)x + (nb)y | x, y \in \mathbb{Z}\} \\ &= \{n(ax + by) | x, y \in \mathbb{Z}\} \\ &= n\{ax + by | x, y \in \mathbb{Z}\} \\ &= nI(a, b) \end{aligned}$$

Assim:

$$\begin{aligned} mdc(na, nb) &= min\left(I(na, nb) \cap \mathbb{N}\right) \\ &= min\left(nI(a, b) \cap \mathbb{N}\right) \\ &= n \cdot min\left(I(a, b) \cap \mathbb{N}\right) \\ &= n \cdot mdc(a, b) \end{aligned}$$

□

Corolário 2. *Se $d = mdc(a, b)$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*[1]

Demonstração. Temos que:

$$mdc(a, b) = mdc\left(d \cdot \tfrac{a}{d}, d \cdot \tfrac{b}{d}\right) \overset{\text{corolário 1}}{=} d \cdot mdc\left(\tfrac{a}{d}, \tfrac{b}{d}\right)$$

Como por hipótese, $mdc(a, b) = d$, segue que $d \cdot mdc\left(\frac{a}{d}, \frac{b}{d}\right) = mdc(a, b) = d$. Assim, dividindo ambas as igualdades por d, concluímos que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

□

Observação 5. *$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ é válido pois $d \mid a$ e $d \mid b$.*

Definição 9. *Dizemos que a, b são primos entre si se, e somente se, $mdc(a, b) = 1$.*

Proposição 14. *Dados $a, b \in \mathbb{Z}$, dizemos que a e b são primos entre si, se e somente se, $\exists x, y \in \mathbb{Z}$ tal que $ax + by = 1$.*[2]

Demonstração. ($\Rightarrow$) Suponha que a e b são primos entre si, então $mdc(a, b) = 1$. Logo, $1 \mid a$ e $1 \mid b$. Assim, pelas propriedades da divisibilidade, segue que $1 \mid ax + by$, em que x,

[1] (SANTOS, 1998), página 7.
[2] (IEZZI; DOMINGUES, 1970), página 43.

$y \in \mathbb{Z}$. Um número divide 1 se, e somente se $ax + by = 1$.

($\Leftarrow$) Suponha agora que $ax + by = 1$ e que $mdc(a, b) = d$, então $d \mid a$ e $d \mid b$. Pelas propriedades de divisibilidade, existem x, $y \in \mathbb{Z}$ tal que $d \mid ax + by \overset{\text{hip}}{=} 1$. Logo, $d \mid 1$, ou seja, $d = 1$. Portanto, $mdc(a, b) = 1$.

□

Observação 6. *Caso particular da Identidade de Bézout.*

Teorema 7. *(Identidade de Bézout) Se $d = mdc(a, b)$, então existem $x, y \in \mathbb{Z}$ tal que $d = ax + by$.*[1]

Demonstração. Seja $I(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$. Tomemos $c \in I(a, b)$ tal que $c = ax + by$, em que $x, y \in \mathbb{Z}$, seja o menor inteiro em $I(a, b)$. Provemos que $c \mid a$ e $c \mid b$. Para isto suponhamos por absurdo que $c \nmid a$ e $c \nmid b$, então existem $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que $a = cq_1 + r_1$ e $b = cq_2 + r_2$ com $0 < r_1 < c$ e $0 < r_2 < c$. Assim:

$$\begin{aligned} a = cq_1 + r_1 \Leftrightarrow r_1 &= a - (ax + by)q_1 \\ &= a - (axq_1 + byq_1) \\ &= a(1 - xq_1) + b(-yq_1) \in I(a, b) \end{aligned}$$

$$\begin{aligned} b = cq_2 + r_2 \Leftrightarrow r_2 &= b - (ax + by)q_2 \\ &= b - (axq_2 + byq_2) \\ &= a(-xq_2) + b(1 - yq_2) \in I(a, b) \end{aligned}$$

O que é um absurdo, haja vista que c é o mínimo de $I(a, b)$. Logo, $c \mid a$ e $c \mid b$. Como $d = mdc(a, b)$, então $d \mid a$ e $d \mid b$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = dk_1$ e $b = dk_2$. Assim:

$$\begin{aligned} c &= ax + by \\ &= (dk_1)x + (dk_2)y \\ &= d\,(k_1x + k_2y) \end{aligned}$$

[1] (SANTOS, 1998), página 5.

Ou seja, $d \mid c$. Pelas propriedades de divisibilidade, temos que $d \leq c$, o que novamente é um absurdo pois d é o máximo divisor comum, isto é, $d = ax + by$.

□

Definição 10. *Uma Equação Diofantina é uma expressão matemática que envolve uma ou mais incógnitas, cujas soluções são valores inteiros.*

Corolário 3. *Uma equação diofantina $ax + by = c$ tem solução se, e somente se, $d = mdc(a, b)$ é um divisor de c.*[1]

Demonstração. ($\Rightarrow$) De fato, seja c a solução da equação diofantina $ax + by$. Tomando $d = mdc(a, b)$, segue que $d \mid a$ e $d \mid b$. Logo, pelas propriedades de divisibilidade segue que $d \mid ax + by = c$. Assim, $c = dq$, $q \in \mathbb{Z}$ e, portanto, d é um divisor de c.

($\Leftarrow$) Reciprocamente, seja $d = mdc(a, b)$ tal que d é um divisor de c. Pela Identidade de Bézout, segue que existem $x, y \in \mathbb{Z}$ tal que $ax + by = d$ $(*)$. Como d é um divisor de c, ou seja, $c = dk$, $k \in \mathbb{Z}$, segue que multiplicando $(*)$ por k, temos $a(xk) + b(yk) = dk = c$. Portanto, c é solução da equação.

□

Lema 2. *Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*[2]

Demonstração. Se $mdc(a, b) = 1$, então pela Proposição 14 segue que $\exists x,\ y \in \mathbb{Z}$ tal que $ax + by = 1$. Multiplicando esta igualdade por c, temos $axc + byx = c$. Como:

$$\begin{cases} a \mid a \Rightarrow \\ a \mid bc \Rightarrow \end{cases} \begin{cases} a \mid axc \\ a \mid byc \end{cases} \Rightarrow a \mid axc + byc = c$$

Portanto, $a \mid c$.

□

Corolário 4. *Dados $a, b, c \in \mathbb{Z}$ com a e b não nulos, em que $a \mid c$, $b \mid c$ e $d = mdc(a, b)$, então $\dfrac{ab}{d} \mid c$.*[3]

Demonstração. Se $d = mdc(a, b)$, então pela Identidade de Bézout, temos que $\exists x, y \in \mathbb{Z}$ tal que $ax + by = d$. Multiplicando a desigualdade acima por c, temos:

[1] (IEZZI; DOMINGUES, 1970), página 50.
[2] (HEFEZ, 2016), página 82.
[3] (HEFEZ, 2016), página 83.

$$cd = acx + bcy$$

Como $a \mid c$ e $b \mid c$, segue:

$$\begin{cases} a \mid c \\ b \mid c \end{cases} \Rightarrow \begin{cases} ab \mid bc \\ ba \mid ac \end{cases} \Rightarrow \begin{cases} ab \mid bcy \\ ab \mid acx \end{cases} \Rightarrow ab \mid acx + bcy = cd$$

Portanto, $\dfrac{ab}{d} \mid c$.

□

Exemplo 11. *(Divisibilidade por* 6*) Um número é divisível por* 6 *se, e somente se, ele é divisível por* 2 *e* 3*, pois se* $2 \mid c$ *e* $3 \mid c$ *e como* $mdc(2,3) = 1$*. Segue pelo corolário anterior que* $6 \mid c$*.*

Proposição 15. *Sejam* $a, b, c \in \mathbb{Z}$ *então* $mdc(ac, b) = 1$ *se, e somente se,* $mdc(a, b) = mdc(c, b) = 1$*.*

Demonstração. ($\Rightarrow$) De fato se $mdc(ac, b) = 1$, então pela Identidade de Bézout segue que $\exists x, y \in \mathbb{Z}$ tal que $acx + by = 1$. Logo $ax_1 + by = 1$, com $x_1 = cx \in \mathbb{Z}$. Pelo mesmo raciocínio, temos que $cx_2 + by = 1$, com $x_2 = ax \in \mathbb{Z}$. Portanto, $mdc(a, b) = mdc(c, b) = 1$.

($\Leftarrow$) Por outro lado, se $mdc(a, b) = mdc(c, b) = 1$ temos que $\exists x, y, z, w \in \mathbb{Z}$ tais que $ax + by = 1$ e $cw + bz = 1$. Multiplicando as igualdades, temos:

$$(ax + by) \cdot (cw + bz) = 1$$
$$axcw + axbz + bycw + b^2yz = 1$$
$$ac(xw) + b(axz + ycw + byz) = 1$$

Tomando $x_1 = xw \in \mathbb{Z}$ e $y_1 = axz + ycw + byz \in \mathbb{Z}$, temos que $acx_1 + by_1 = 1$. Portanto, $mdc(ac, b) = 1$.

□

Proposição 16. *Dados* $a_1, \cdots, a_n \in \mathbb{Z}$ *não todos nulos, existe o seu mdc e* $mdc(a_1, \cdots, a_n) = mdc(a_1 \cdots, a_{n-2}, mdc(a_{n-1}, a_n))$.[1]

[1] (HEFEZ, 2016), página 84.

Demonstração. Como calculamos o máximo divisor comum entre 2 números, mostraremos por indução para $n \geq 2$.

Para $n = 2$ segue por definição que $mdc(a_1, a_2) = d$. Logo, não há nada a se provar. Agora, suponha que $mdc(a_1, \cdots, a_n) = mdc(a_1 \cdots, a_{n-2}, mdc(a_{n-1}, a_n))$ (H.I). Mostremos que para $n+1$ a igualdade seja verdadeira, ou seja,

$$mdc(a_1, \cdots, a_{n+1}) = mdc(a_1 \cdots, a_{n-1}, mdc(a_n, a_{n+1})).$$

De fato, Seja $d = mdc(a_1, \cdots, a_{n-1}, mdc(a_n, a_{n+1}))$. Logo, $d \mid a_1$, $d \mid a_2$, $\cdots$, $d \mid mdc(a_n, a_{n+1})$. Como d é o máximo divisor comum, segue que $d \mid a_1$, $d \mid a_2$, $\cdots$, $d \mid a_n$, $d \mid a_{n+1}$. Por outro lado, seja d_1 um múltiplo comum de $a_1, \cdots, a_{n+1}$. Logo $d_1 \mid a_1, \cdots, d_1 \mid a_{n+1}$ e ainda $d_1 \mid mdc(a_n, a_{n+1})$. Daí $d_1 \mid d$ e, portanto, o seu mdc existe e $mdc(a_1, \cdots, a_n) = mdc(a_1 \cdots, a_{n-2}, mdc(a_{n-1}, a_n)) = d$.

□

Exemplo 12. *Dados* 3, 4 *e* 9, *segue que* $mdc(3, 4, 9) = mdc(mdc(3, 9), 4) = mdc(3, 4) = 1$.

1.5 Mínimo Múltiplo Comum

O mínimo múltiplo comum (ou *mmc*) corresponde ao menor múltiplo em comum entre dois ou mais números e exploraremos seus resultados a seguir.

Definição 11. *Dizemos que* $m = mmc(a, b)$ *se, e somente se:*

(*i*) $m \geq 0$;

(*ii*) $a \mid m$ *e* $b \mid m$;

(*iii*) *Se* $a \mid m_1$ *e* $b \mid m_1$, *então* $m \mid m_1$.

Propriedade 9. *Dados* $a, b \in \mathbb{Z}$, *temos:*

1. $mmc(a, b) = mmc(-a, b) = mmc(a, -b) = mmc(-a, -b)$;

2. $mmc(a, b) = 0 \Leftrightarrow a = 0$ *ou* $b = 0$.[1]

[1](HEFEZ, 2016), página 89.

Proposição 17. *Dados $a, b \in \mathbb{Z}$ temos que $mmc(a,b)$ existe e vale $mdc(a,b) \cdot mmc(a,b) = |a \cdot b|$.*[1]

Demonstração. Se $a = 0$ ou $b = 0$ a igualdade é trivialmente satisfeita, pois $mdc(a,0) = mdc(0,b) = mmc(0,b) = mmc(a,0) = 0$ e ainda $b \cdot 0 = a \cdot 0 = 0$.
Consideremos o caso em que $a, b \in \mathbb{N}$ (analogamente temos para o caso negativo). Tomemos $m = \dfrac{|ab|}{d} = \dfrac{ab}{d}$, em que $d = mdc(a,b)$. Verifiquemos que $m = mmc(a,b)$. De fato:

(i) $m > 0$, pois $0 < a, b \in \mathbb{N} \Rightarrow d > 0$.

(ii) Se $m = \dfrac{ab}{d}$, então $m = a\left(\dfrac{b}{d}\right)$. Logo por definição de divisibilidade $a \mid m$. Por outro lado, como $m = \dfrac{ab}{d}$, então $m = b\left(\dfrac{a}{d}\right)$ e, portanto, $b \mid m$.

(iii) Seja $m_1 \in \mathbb{N}$ tal que $a \mid m_1$ e $b \mid m_1$. Logo, $m_1 = ar$ e $m_1 = bs$, com $r, s \in \mathbb{N}$. Daí, $ar = bs$. Dividindo a igualdade por d, temos $\dfrac{ar}{d} = \dfrac{bs}{d}$. Logo, $\dfrac{ar}{d} = \dfrac{b}{d}s$ e $\dfrac{a}{d}r = \dfrac{bs}{d}$. Segue da igualdade que $\dfrac{b}{d} \mid \dfrac{ar}{d}$ e $\dfrac{a}{d} \mid \dfrac{bs}{d}$. Pelo Lema 2, temos:

$$\begin{cases} \dfrac{b}{d} \mid r \\ \\ \dfrac{a}{d} \mid s \end{cases} \Rightarrow \begin{cases} a\dfrac{b}{d} \mid ar = m_1 \\ \\ b\dfrac{a}{d} \mid bs = m_1 \end{cases} \Rightarrow \begin{cases} \dfrac{ab}{d} = m \mid m_1 \\ \\ \dfrac{ab}{d} = m \mid m_1 \end{cases}$$

Portanto, $m = \dfrac{ab}{d}$.

□

Corolário 5. *Se a, b são primos entre si, então $mmc(a,b) = |ab|$.*[2]

Demonstração. Pela proposição anterior segue que $mdc(a,b) \cdot mmc(a,b) = |ab|$. Como a e b são primos entre si, temos que $mdc(a,b) = 1$. Portanto $mmc(a,b) = |ab|$.

□

Proposição 18. *(Generalização do mmc) Sejam $a_1, a_2 \cdots, a_n \in \mathbb{Z}^*$, então existe o $mmc(a_1, \cdots, a_n)$ e $mmc(a_1, \cdots, a_n) = mmc(a_1, \cdots, mmc(a_{n-1}, a_n))$.*[3]

Demonstração. Análogo a generalização do máximo divisor comum.

□

[1] (HEFEZ, 2016), página 89.
[2] (HEFEZ, 2016), página 90.
[3] (HEFEZ, 2016), página 91.

1.6 Números Primos

Um número é considerado primo quando é divisível somente por 1 e ele próprio. Tais números têm muitas propriedades, como é possível ver a seguir.

Definição 12. *Dizemos que $p \in \mathbb{N}$, $p > 1$, é um número primo se, e somente se, seus únicos divisores são 1 e p.*[1]

Se $p \in \mathbb{Z}$, seus divisores são ± 1 e $\pm p$.

Alguns números primos são: $2, 3, 5, 7, 11, \cdots$.

Observação 7. (1) *Se p e q são números primos, então $p \mid q \Leftrightarrow p = q$.*

(2) *Se p é primo e $p \nmid a$ então $mdc(p, a) = 1$.*

Exemplo 13. ***Algoritmo de Primalidade***

Entradas: Inteiro positivo n.

Saída: Definição se n é primo ou não.

```
1  from time import sleep
2  print('-'*20)
3  print('Vamos determinar se um número n é primo')
4  print('-'*20)
5  sleep(1.5)
6  n = int(input('Digite uma valor para n (n>0): '))
7  div = 0
8  for divisor in range(1,n+1):
9      if n % divisor == 0:
10         div += 1
11 if div == 2:
12     print(f'{n} é primo')
13 else:
14     print(f'{n} não é primo')
15
```

Figura 4: Algoritmo de Primalidade

[1] (SANTOS, 1998), página 9.

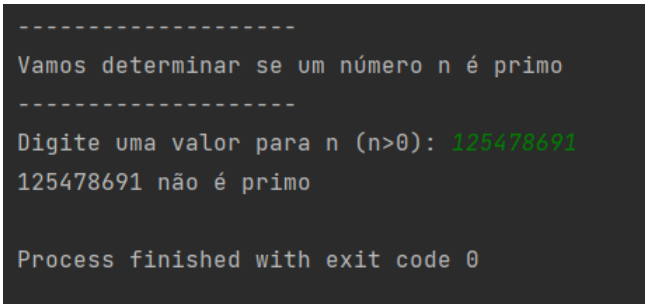


Figura 5: Exemplo

Definição 13. *Se n não é um número primo, então n é um número composto, ou seja, $n = n_1 \cdot n_2$, com $1 < n_1, n_2 < n$.*

Lema 3. *(Lema de Euclides) Se p é um número primo e $p \mid ab$ então $p \mid a$ ou $p \mid b$.*[1]

Demonstração. Seja p primo e que $p \nmid a$. Mostremos que $p \mid b$. Como $p \nmid a$, então $mdc(p, a) = 1$. Pela Identidade de Bézout, segue que $\exists x, y \in \mathbb{Z}$ tal que $ax + py = 1$. Multiplicando por b ambos os lados, temos $b = abx + bpy$. Como por hipótese $p \mid ab$ e $p \mid p$. Então:

$$\begin{cases} p \mid ab \\ p \mid p \end{cases} \Rightarrow \begin{cases} p \mid abx \\ p \mid bpy \end{cases} \Rightarrow p \mid abx + bpy = b$$

Logo, $p \mid b$. Analogamente $p \mid a$. Portanto, se p é um número primo e $p \mid ab$ então $p \mid a$ ou $p \mid b$.

□

Corolário 6. *Se $p \mid a_1 \cdot a_2 \cdots a_n$ e p primo, então $p \mid a_1$, ou $p \mid a_2$, $\cdots$, ou $p \mid a_n$.*[2]

Demonstração. Basta usar o Lema de Euclides.

□

Teorema 8. *(Teorema Fundamental da Aritmética) Todo número $n > 1$ ou é primo ou se escreve de modo único como um produto de primos.*[3]

[1] (SANTOS, 1998), página 9.
[2] (BURTON, 2010), página 40.
[3] (SANTOS, 1998), página 9.

Demonstração. Primeiro mostremos que todo número $n > 1$ ou é primo ou se escreve como um produto de primos, para isto usaremos o segundo princípio de indução sobre n.

Se $n = 2$ e como 2 é primo, então o resultado esta satisfeito. Agora suponha que o resultado seja verdadeiro $\forall n \leq r - 1$ (H.I). Mostremos que o resultado é verdadeiro para r. Se r é primo o resultado já esta satisfeito. Suponha que r não é primo, ou seja, r é composto. Então, existem $n_1, n_2 \in \mathbb{Z}$ tal que $r = n_1 n_2$, em que $1 < n_1, n_2 < r$. Como $n_1, n_2 \leq r - 1$, segue pela (H.I) que $n_1 = p_1 p_2 \cdots p_m$ e $n_2 = p_{m+1} p_{m+2} \cdots p_{m+s}$. Logo, $r = n_1 n_2 = p_1 p_2 \cdots p_m p_{m+1} p_{m+2} \cdots p_{m+s}$, isto é, r se escreve como um produto de primos. Portanto, pelo Princípio de Indução, segue que todo número $n > 1$ ou é primo ou se escreve como um produto de primos.

Mostremos agora a unicidade, para isto suponha que $n = p_1 p_2 \cdots p_r$ e $n = q_1 q_2 \cdots q_s$ com $p_i's$ e $q_i's$ primos. Mostremos que $r = s$. De fato,

$$\begin{aligned} p_1 p_2 \cdots p_r &= q_1 q_2 \cdots q_s \\ p_1 p_2 \cdots p_r &= q_1 \left(q_2 q_3 \cdots q_s\right) \end{aligned} \tag{1}$$

Logo, $q_1 \mid p_1 p_2 \cdots p_r$, pelo Lema de Euclides, segue que $q_1 \mid p_1$ ou $q_1 \mid p_2$, $\cdots$, ou $q_1 \mid p_r$. Sem perda de generalidade, suponha que $q_1 \mid p_1$. Como $p_1 > 1$, segue que $q_1 = p_1$. De (1), temos:

$$\begin{aligned} p_1 p_2 \cdots p_r &= q_1 q_2 \cdots q_s \\ p_2 p_3 \cdots p_r &= q_2 (q_3 \cdots q_s) \end{aligned} \tag{2}$$

Aplicando o mesmo raciocínio, concluímos que $q_2 \mid p_2 p_3 \cdots p_r$. Novamente, pelo Lema de Euclides segue que $q_2 \mid p_2$ ou $q_2 \mid p_3$, $\cdots$, ou $q_2 \mid p_r$ e supondo que $q_2 \mid p_2$. Como $p_2 > 1$, segue que $q_2 = p_2$. Assim de (2):

$$\begin{aligned} p_2 p_3 \cdots p_r &= q_2 q_3 \cdots q_s \\ p_3 p_4 \cdots p_r &= q_3 (q_4 \cdots q_s) \end{aligned}$$

Continuando este raciocínio, podemos concluir que $p_i = q_i$ e $r = s$, pois se

$r \neq s$, supondo por exemplo que $r < s$, depois de r passos, teríamos:

$$1 = q_{r+1} \cdots q_s$$

O que é um absurdo pois, cada q_i são primo, isto é, maiores que 1. Portanto, $p_i = q_i$ e $r = s$.

□

Do teorema anterior, na decomposição de um número inteiro estritamente positivo n em fatores primos, pode se ocorrer de um fator se repetir. Nesse caso, pode-se reunir esses fatores repetidos numa só potência, mediante a notação exponencial. Supondo que os fatores primos distintos $p_1 < p_2 < \cdots < p_r$ $(r \geq 1)$, que podem aparecer α_i vezes $(i = 1, \cdots, n)$, a decomposição pode ser escrita como:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Definição 14. *Denotando por $d(n)$ o número de divisores de n, segue que $d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$.*

Exemplo 14. *Dado $n = 10$, temos que $10 = 5 \cdot 2 = 5^1 \cdot 2^1$. Então, $d(10) = (1+1)(1+1) = 4$. De fato, os divisores de 10 são $1, 2, 5, 10$.*

Definição 15. *Um número n é dito perfeito se, e somente se, a soma de seus divisores é igual a $2 \cdot n$.*

Exemplo 15. *6 é um número perfeito, pois $6 = 3 \cdot 2$ e $d(6) = (1 + 1)(1 + 1) = 4$, sendo seus divisores $1, 2, 3, 6$ e, ainda, $2 \cdot 6 = 12 = 1 + 2 + 3 + 6$.*

Proposição 19. *Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ e $m \mid n$, então $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ com $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \cdots, r$.*[1]

Demonstração. Se $m \mid n$, então $n = mq$, com $q \in \mathbb{Z}$. Logo, $n = \left(p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}\right) q$, então $n = p_1^{\beta_1} \left(p_2^{\beta_2} \cdots p_r^{\beta_r} q\right)$. Assim, $p_1^{\beta_1} \mid n$. Pelo Lema de Euclides, segue que $p_1^{\beta_1}$ divide algum $p_i^{\alpha_i}$, com $i = 1 \cdots, r$ por ser primo com os demais $p_i^{\alpha_i}{}'s$. Como o mesmo raciocínio, concluímos que $p_i^{\beta_i} \mid n$, com $i = 2, \cdots, r$. Novamente pelo Lema de Euclides, temos que

[1] (HEFEZ, 2016), página 124.

$p_i^{\beta_i}$ divide algum $p_i^{\alpha_i}$, em que $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \cdots, r$. Portanto, $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ com $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \cdots, r$.

□

Teorema 9. *Se* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *e* $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ *e* $\gamma = min\{\alpha_i, \beta_i\}$ *e* $\varphi = max\{\alpha_i, \beta_i\}$, *então:*

$$mdc(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} \text{ e } mmc(a,b) = p_1^{\varphi_1} p_2^{\varphi_2} \cdots p_r^{\varphi_r}.$$ [1]

Demonstração. Seja $d = mdc(a,b)$. Como $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ então $d = mdc\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}\right)$. Pela Proposição 16, segue que $d = mdc\left(mdc\left(p_1^{\alpha_1}, p_1^{\beta_1}\right), mdc\left(p_2^{\alpha_2}, p_2^{\beta_2}\right), \cdots, mdc\left(p_r^{\alpha_r}, p_r^{\beta_r}\right)\right)$. Daí, tomando $\gamma = min\{\alpha_i, \beta_i\}$, temos que $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$. Como os $p_i's$ são primos, então $d > 0$.

Por outro lado, como a e b são compostos, então podem ser decompostos em fatores primos. como $d = mdc(a,b)$, segue que $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} \mid a$ e $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} \mid b$. Assim, pelo Lema de Euclides, temos que algum $p_i^{\gamma_i}$ divide a e b, para $i = 1, \cdots, r$.

Seja c um divisor comum de a e b. Logo, $c = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_r^{\varepsilon_r}$, em que $\varepsilon_i \leq min\{\alpha_i, \beta_i\}$. Assim, $c \mid d$ e, portanto $mdc(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$.

Analogamente, segue que $mmc(a,b) = p_1^{\varphi_1} p_2^{\varphi_2} \cdots p_r^{\varphi_r}$.

□

Teorema 10. *Existem infinitos números primos.* [2]

Demonstração. Suponha que existam uma quantidade finita de números primos, vamos denota-los por $p_1, p_2, \cdots, p_r$. Tomemos $n = p_1 p_2 \cdots p_r + 1$. Temos que $p_1 \nmid n$, pois se $p_1 \mid n$ então p_1 dividiria $n - p_1 p_2 \cdots p_r = 1$. O que é um absurdo pois p_1 é primo. O mesmo raciocínio vale para $p_2, p_3, \cdots, p_r$. Logo, os únicos divisores de n são o 1 e o próprio n. Assim, n é primo e $n > p_i$, $\forall i = 1, \cdots, r$. O que é um absurdo pois afirmamos que existiam apenas r números primos. Portanto, existem infinitos números primos.

□

Lema 4. *Se* $n > 1$ *não é divisível por nenhum primo* p *tal que* $p^2 \leq n$ $(p \leq \sqrt{n})$, *então* n *é um número primo.* [3]

[1] (HEFEZ, 2016), página 126.
[2] (BURTON, 2010), página 46.
[3] (HEFEZ, 2016), página 132.

Demonstração. Suponha que exista $n > 1$ e não divisível por nenhum primo p tal que $p^2 \leq n$ e que n não seja primo. Seja q o menor primo que divida n. Logo, $n = qn_1$, em que $q \leq n_1$. Então $q^2 \leq qn_1 = n$, ou seja, $q \mid n$. O que é um absurdo pois n não é divisível por nenhum primo. Portanto, n é primo.

□

Exemplo 16. *Seja $n = 323$, será que n é primo?*

Temos que $\sqrt{323} \cong 17,97$ e os números primos abaixo da raiz são: $2, 3, 5, 7, 11, 13, 17$. *Por verificação temos que* 323 *não é um número primo, pois* $17 \mid 323 = 17 \cdot 19$.

Lema 5. *Seja p um número primo. Os números $\binom{p}{i}$, $0 < i < p$ são todos divisíveis por p.*[1]

Demonstração. Se $i = 1$, então $\binom{p}{1} = \frac{p!}{(p-1)!1!} = p$ e $p \mid p$. Logo, podemos supor que $1 < i < p$ e nesse caso:

$$\binom{p}{i} = \frac{p!}{(p-i)!i!} = \frac{p(p-1)(p-2)\cdots(p-i+1)(p-i)!}{(p-i)!i!}$$
$$= \frac{p(p-1)(p-2)\cdots(p-i+1)}{i!}$$

Como $p > i$, ou seja, não possui nenhum fator i, segue que $mdc(p, i!) = 1$. Assim, pelo Lema 2, segue que $i! \mid p(p-1)(p-2)\cdots(p-i+1)$. Deste modo:

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{i!} = p\left(\frac{(p-1)(p-2)\cdots(p-i+1)}{i!}\right)$$

Portanto, $p \mid \binom{p}{i}$.

□

Teorema 11. (*Pequeno Teorema de Fermat*) *Dado p primo, temos que $p \mid a^p - a$, $\forall a \in \mathbb{Z}$.*[2]

[1] (HEFEZ, 2016), página 135.
[2] (HEFEZ, 2016), página 135.

Demonstração. Indução sobre a.

Note que se $p = 2$, então $2 \mid a^2 - a = a(a-1)$ que é o produto de dois números consecutivos e desta maneira $a(a-1)$ é um número par e assim, divisível por 2. Suponha p primo e ímpar.

Observe que se $a = 0$, então $0^p - 0 = 0$. Daí $p \mid 0$. Suponha agora que $p \mid a^p - a$, $\forall a \in \mathbb{Z}$ (H.I). Mostremos que para $a+1$ o resultado também é verdadeiro, isto é, que $p \mid (a+1)^p - (a+1)$. De fato, usando o Binômio de Newton, temos:

$$(a+1)^p - (a+1) = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + \binom{p}{p} 1 - a - 1 = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1 - a - 1 = (a^p - a) + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a$$

Tomemos $c = \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a$. Pela (H.I) temos que $p \mid a^p - a$ e pelo Lema 5 temos que $p \mid c$. Logo, $p \mid a^p - a + c = (a+1)^p - (a+1)$. Portanto, pelo Princípio de Indução, temos que dado p primo, temos que $p \mid a^p - a$, $\forall a \in \mathbb{Z}$.

□

Corolário 7. *Se p é primo e $p \nmid a$, então $p \mid a^{p-1} - 1$.*[1]

Demonstração. Seja p primo, então pelo P.T.F. (Pequeno Teorema de Fermat) $p \mid a^p - a = a\left(a^{p-1} - 1\right)$. Como $p \nmid a$, segue que $p \mid a^{p-1} - 1$.

□

Observação 8. *O Corolário acima também é chamado de Pequeno Teorema de Fermat.*

Exemplo 17. *Seja $p = 7$ e $a = 2$ e note que $7 \nmid 2$. Logo, pelo P.T.F. temos que $7 \mid 2^6 - 1$. De fato, $2^6 - 1 = 63 = 9 \cdot 7$.*

Proposição 20. *Sejam $1 < a, n \in \mathbb{N}$. Se $a^n + 1$ é primo, então a é par e $n = 2^m$, com $m \in \mathbb{N}$.*[2]

[1] (HEFEZ, 2016), página 136.
[2] (HEFEZ, 2016), página 144.

Demonstração. Suponha que $1 < a, n \in \mathbb{N}$ e que $a^n + 1$ é primo. Afirmamos que a é par, pois se a fosse ímpar então a^n também seria e $a^n + 1$ seria par, o que é um absurdo pois 2 dividiria $a^n + 1$ e $a^n + 1$ é primo. Mostremos agora que $n = 2^m$. De fato, suponha que n tenha um divisor primo p, com $p \neq 2$. Então $n = p \cdot n_1$, em que $n_1 \in \mathbb{N}$. Daí, pela Proposição 12, temos que $a^{n_1} + 1 \mid (a^{n_1})^p + 1^p = a^{n_1 \cdot p} + 1$, em que $p = 2q + 1$, $q \in \mathbb{N}$, pois p é ímpar. O que é um absurdo pois $a^n + 1$ é primo. Portanto, o único divisor primo de $a^n + 1$ é o 2 e, portanto, $n = 2^m$.

□

Definição 16. *Os números de Fermat são da forma $F_n = 2^{2^n} + 1$, com $n = 0, 1, \cdots$. Os números primos desta forma são chamados de Primos de Fermat.*

Proposição 21. *Sejam $a, n > 1$. Se $a^n - 1$ é primo então $a = 2$ e n é primo.*[1]

Demonstração. Seja $a^n - 1$ primo, com $a, n > 1$. Suponha que $a > 2$, então $a - 1 > 1$. Pela Proposição 11 segue que $a^n - 1 \mid (a^n)^q - 1^q = a^{n \cdot q} - 1$. O que é um absurdo pois $a^n - 1$ é primo. Logo, $a = 2$.

Por outro lado, suponha que n não seja primo, então $n = r \cdot s$, com $r, s > 1$. Novamente pela Proposição 11, temos que $a^r - 1 \mid (a^r)^s - 1$. O que novamente é um absurdo, pois $a^n - 1$ é primo. Portanto n é primo.

□

Definição 17. *Os números de Mersenne são da forma $M_p = 2^p - 1$, com p primo. Os números primos desta forma são chamados de Primos de Mersenne.*

Exemplo 18. *O maior número primo de Mersenne conhecido até o momento é da forma $M_{82589933} = 2^{82589933} - 1$ (encontrado em 2018), com 24.862.084 dígitos.*[2]

2 Aritmética Modular

Na matemática, a aritmética modular é um sistema na qual ao atingir um certo valor tais números retrocedem, como um relógio. Seus aspectos históricos e aplicações cotidianas podem ser visto em (OLIVEIRA, 2017). A seguir, enunciaremos algumas de suas propriedades que podem ser encontrados em (SANTOS, 1998; IEZZI; DOMINGUES, 1970; HEFEZ, 2016; BURTON, 2010; COUTINHO, 1997).

[1] (HEFEZ, 2016), página 145.

[2] https://impa.br/noticias/por-que-a-descoberta-do-maior-numero-primo-importa/

2.1 Congruência

Definição 18. *Dados $a, b \in \mathbb{Z}$, dizemos que a é congruente a b módulo m $(m > 1)$ e denotamos por $a \equiv b \ (mod\ m)$ se $m \mid a - b$. Se $m \nmid a - b$ dizemos que a é incongruente a b módulo m e denotamos por $a \not\equiv b \ (mod\ m)$.*[1]

Exemplo 19. *Dados $a = 21$, $b = 13$ e $m = 2$, temos que $21 = 2 \cdot 10 + 1$ e $13 = 2 \cdot 10 + 1$. Logo, $21 \equiv 13 \ (mod\ 2)$.*

Proposição 22. *Dados $a, b, c \in \mathbb{Z}$ e $m > 1$, temos:*

(1) *$a \equiv a \ (mod\ m)$;*

(2) *Se $a \equiv b \ (mod\ m)$, então $b \equiv a \ (mod\ m)$;*

(3) *Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então $a \equiv c \ (mod\ m)$.*[2]

Demonstração. (i) De fato $a - a = 0$ e $m \mid 0 = a - a$, logo $a \equiv a \ (mod\ m)$.

(ii) Se $a \equiv b \ (mod\ m)$, então $m \mid a - b$, ou seja, $a - b = mk$, $k \in \mathbb{Z}$. Logo, $b - a = m(-k)$, isto é, $m \mid b - a$ e, portanto, $b \equiv a \ (mod\ m)$.

(iii) Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então $m \mid a - b$ e $m \mid b - c$. Logo, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a - b = mk_1$ (1) e $b - c = mk_2$ (2). Somando (1) e (2), temos $a - c = a + b - (b + c) = mk_1 - mk_2 = m\,(k_1 - k_2)$. Daí, $m \mid a - c$ e, portanto, $a \equiv c \ (mod\ m)$.

□

Observação 9. *Note que pela proposição acima que a congruência é uma relação de equivalência.*

Proposição 23. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$ tal que $a \equiv b \ (mod\ m)$, então:*

(1) *$a + c \equiv b + c \ (mod\ m)$;*

(2) *$a - c \equiv b - c \ (mod\ m)$;*

[1] (SANTOS, 1998), página 32.
[2] (IEZZI; DOMINGUES, 1970), página 54.

(3) $ac \equiv bc \ (mod \ m)$.[1]

Demonstração. (1) Se $a \equiv b \ (mod \ m)$ então $m \mid b - a$, isto é, $b - a = mk$, $k \in \mathbb{Z}$. Note que, $mk = b-a = b+c-(a+c)$, ou seja, $m \mid b+c-(a+c)$. Portanto, $a+c \equiv b+c \ (mod \, m)$.

(2) Análogo ao (1), basta somar $-c$.

(3) Se $a \equiv b \ (mod \ m)$ então $b - a = mk$, $k \in \mathbb{Z}$. Multiplicando ambos os lados por c, temos $c(b - a) = bc - ac = c(mk) = m(ck)$. Assim $ac \equiv bc \ (mod \ m)$.

□

Proposição 24. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$ tais que $a \equiv b \ (mod \ m)$ e $c \equiv d \ (mod \ m)$, então:*

(1) $a + c \equiv b + d \ (mod \ m)$;

(2) $a - c \equiv b - d \ (mod \ m)$;

(3) $ac \equiv bd \ (mod \ m)$.

Demonstração. (1) Se $a \equiv b \ (mod \ m)$ e $c \equiv d \ (mod \ m)$, então $m \mid a - b$ e $m \mid c - d$, ou seja, $a - b = mr$ e $c - d = ms$, $r, s \in \mathbb{Z}$. Somando as igualdades, temos que $a - b + c - d = mr + ms = m(r + s)$. Assim, $m \mid a - b + c - d = (a + c) - (b + d)$ e, portanto, $a + c \equiv b + d \ (mod \ m)$.

(2) Análogo ao (1), basta subtrair.

(3) Se $a \equiv b \ (mod \ m)$ e $c \equiv d \ (mod \ m)$, então $m \mid a - b$ e $m \mid c - d$. Logo:

$$\begin{cases} m \mid a - b \\ m \mid c - d \end{cases} \Rightarrow \begin{cases} m \mid d(a - b) \\ m \mid a(c - d) \end{cases} \Rightarrow m \mid da - db + (ac - ad) = ac - db$$

Assim, $m \mid ac - bd$ e, portanto, $ac \equiv bd \ (mod \ m)$.

□

Corolário 8. *Dado $n \in \mathbb{N}$, se $a \equiv b \ (mod \ m)$, então $a^n \equiv b^n \ (mod \ m)$.*[2]

[1] Proposições 23 e 24; (SANTOS, 1998), página 33.
[2] (HEFEZ, 2016), página 168.

Demonstração. De fato, dado $n = 1$, temos $n \in \mathbb{N}$, se $a \equiv b \ (mod\ m)$ que por hipótese é válido. Suponhamos que para todo $n \in \mathbb{N}$ a relação é satisfeita, ou seja, $a^n \equiv b^n \ (mod\ m)$ (H.I). Mostremos que para $n + 1$ a relação também é verdadeira, isto é, $a^{n+1} \equiv b^{n+1} \ (mod\ m)$. Com efeito, pela (H.I) temos que $a^n \equiv b^n \ (mod\ m)$ e pela Proposição anterior, temos $a^n a \equiv b^n b \ (mod\ m)$, ou seja, $a^{n+1} \equiv b^{n+1} \ (mod\ m)$. Portanto, pelo Princípio da Indução se $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$.

□

Teorema 12. *Sejam p primo e $a \in \mathbb{Z}$, então $a^p \equiv a \ (mod\ p)$ e se $p \nmid a$ então $a^{p-1} \equiv 1 \ (mod\ p)$.*[1]

Demonstração. De fato, pelo P.T.F. temos que $p \mid a^p - a$ e se $p \nmid a$ então $p \mid a^{p-1-1}$. Logo, por definição de congruência temos que $a^p \equiv a \ (mod\ p)$ e se $p \nmid a$ então $a^{p-1} \equiv 1 \ (mod\ p)$.

□

Teorema 13. *Sejam p primo e $a, b \in \mathbb{Z}$, temos que $(a \pm b)^p \equiv a^p \pm b^p \ (mod\ p)$.*

Demonstração. Mostremos primeiro o caso $(a + b)^p \equiv a^p + b^p \ (mod\ p)$.

Pelo Teorema anterior, temos que $(a + b)^p \equiv a + b \ (mod\ p)$. Por outro lado, novamente pelo Teorema anterior, temos que $a^p \equiv a \ (mod\ p)$ e que $b^p \equiv b \ (mod\ p)$. Somando as desigualdades anteriores, segue que $a^p + b^p \equiv a + b \ (mod\ p)$. Como a congruência é uma relação de equivalência, segue pela transitividade que $(a + b)^p \equiv a^p + b^p \ (mod\ p)$.

Analogamente, temos o caso $(a - b)^p \equiv a^p - b^p \ (mod\ p)$.

□

Exemplo 20. *Ache o resto da divisão de 237^{100} por 11. Temos que 11 é primo, então pelo P.T.F. temos que $a^{p-1} \equiv 1 \ (mod\ p)$, ou seja, $237^{10} \equiv 1 \ (mod\ 11)$. Logo, $237^{10q} \equiv 1 \ (mod\ 11)$, $q \in \mathbb{Z}$. Tomando $q = 10$, temos: $237^{100} \equiv 1 \ (mod\ 11)$. Portanto o resto da divisão de 237^{100} por 11 é 1.*

Proposição 25. *Sejam $a, b, c \in \mathbb{Z}$ e $m > 1$ tal que $a + c \equiv b + c \ (mod\ m)$, então $a \equiv b \ (mod\ m)$.*[2]

[1] Teoremas 12 e 13; (HEFEZ, 2016), página 168.
[2] (HEFEZ, 2016), página 169.

Demonstração. Com efeito, se $a + c \equiv b + c \ (mod\ m)$ então $m \mid a + c - (b + c) = a - b$, isto é, $a \equiv b \ (mod\ m)$.

□

Proposição 26. *Sejam $a, b, c \in \mathbb{Z}$ e $m > 1$ então $ac \equiv bc \ (mod\ m) \Leftrightarrow a \equiv b \ (mod\ m_1)$, em que $m_1 = \dfrac{m}{d}$ e $d = mdc(c, m)$.*[1]

Demonstração. ($\Rightarrow$) Se $ac \equiv bc \ (mod\ m)$ então $m \mid ac - bc$ e $ac - bc = c(a - b) = mk$, $k \in \mathbb{Z}$. Dividindo a igualdade por $d = mdc(c, m)$ temos que $\left(\dfrac{c}{d}\right)(a - b) = \left(\dfrac{m}{d}\right)k$. Logo, $\left(\dfrac{m}{d}\right) \mid \left(\dfrac{c}{d}\right)(a - b)$. Como o $mdc\left(\dfrac{m}{d}, \dfrac{c}{d}\right) = 1$, segue que eles são coprimos. Daí, $\left(\dfrac{m}{d}\right) \mid a - b$. Portanto, $a \equiv b \ \left(mod\ \dfrac{m}{d}\right)$.

($\Leftarrow$) Analogamente temos a volta.

□

Exemplo 21. *Seja $18 \equiv 12 \ (mod\ 6)$, temos que $18 = 3 \cdot 6$ e $12 = 4 \cdot 3$. Logo, $3 \cdot 6 \equiv 4 \cdot 3 \ (mod\ 6)$. Pela Proposição anterior, segue que $6 \equiv 4 \ \left(mod\ \dfrac{6}{3}\right)$, ou seja, $6 \equiv 4 \ (mod\ 2)$.*

Corolário 9. *Se $mdc(c, m) = 1$, então $ac \equiv bc \ (mod\ m) \Leftrightarrow a \equiv b \ (mod\ m)$.*

Demonstração. Segue de imediato da proposição anterior.

□

Definição 19. *Um Sistema Completo de Resíduos módulo m (S.C.R.) é qualquer conjunto de números inteiros cujos os restos da divisão por m são $0, 1, 2, \cdots, m-1$, sem repetições e em uma ordem qualquer.*[2]

Observação 10. *Em um S.C.R. módulo m, todos os seus elementos são incongruentes módulo m.*

Proposição 27. *Sejam $a, k, m \in \mathbb{Z}$ com $m > 1$ e $mdc(k, m) = 1$. Se $\{a_1, a_2, \cdots, a_m\}$ é um S.C.R. módulo m, então $\{a + ka_1, a + ka_2, \cdots, a + ka_m\}$ também é um S.C.R. módulo m.*[3]

[1] (HEFEZ, 2016), página 170.
[2] (HEFEZ, 2016), página 167.
[3] (HEFEZ, 2016), página 170.

Demonstração. De fato, se $\{a_1, a_2, \cdots, a_m\}$ é um S.C.R., então $a_i \equiv a_j \ (mod\ m)$ se, e somente se, $i = j$. Como $mdc(k, m) = 1$, segue que $ka_i \equiv ka_j \ (mod\ m)$. Daí, $a + ka_i \equiv a + ka_j \ (mod\ m)$, $\forall i = j$. Portanto,

$$\{a + ka_1, a + ka_2, \cdots, a + ka_m\}$$

também é um S.C.R. módulo m.

□

Exemplo 22. *Temos que* $\{0, 1, 2, 3, 4\}$*, assim como* $\{5, 11, 22, 33, 44\}$ *são um S.C.R módulo* 5*.*

Proposição 28. *Sejam* $a, b \in \mathbb{Z}$ *com* $m > 1$ *e* $m_1, m_2 \cdots, m_r > 1$*, então temos que:*

(1) $a \equiv b \ (mod\ m)$ *e* $n \mid m$*, então* $a \equiv b \ (mod\ n)$*;*

(2) $a \equiv b \ (mod\ m_i)$, $\forall i = 1, \cdots, n \Leftrightarrow a \equiv b \ (mod\ r)$*, em que* $r = mmc(m_1, \cdots, m_n)$*.*

(3) *Se* $a \equiv b \ (mod\ m)$ *então* $mdc(a, m) = mdc(b, m)$.[1]

Demonstração. (1) Se $a \equiv b \ (mod\ m)$, então $m \mid b - a$. Como $m \mid n$ e $m \mid b - a$, segue que $n \mid b - a$, ou seja, $a \equiv b \ (mod\ n)$.

(2) Seja $r = mmc(m_1, \cdots, m_n)$, se $a \equiv b \ (mod\ m_i)$, $\forall i = 1, \cdots, n$ então $m_i \mid b - a$, $\forall i = 1, \cdots, n$. Pela definição de mmc, segue que $r \mid b - a$. Assim, $a \equiv b \ (mod\ r)$.

(3) Se $a \equiv b \ (mod\ m)$ então $m \mid b - a$, ou seja, $b - a = mk$, $k \in \mathbb{Z}$. Logo, $b = a + mk$. Pelas propriedades de mdc, temos:

$$\begin{aligned} mdc(b, m) &= mdc(a + mk, m) \\ &= mdc(m, (a + mk) - k \cdot m) \\ &= mdc(m, a) \end{aligned}$$

□

[1] (HEFEZ, 2016), página 171.

Exemplo 23. *Encontre o menor inteiro positivo múltiplo de* 6 *que deixa resto* 6 *quando divididos por* $2, 3, 4, 5$. *Primeiro precisamos achar um* $x \in \mathbb{Z}$ *que satisfaça:*

$$6x \equiv 6 \ (mod\ 2)$$
$$6x \equiv 6 \ (mod\ 3)$$
$$6x \equiv 6 \ (mod\ 4)$$
$$6x \equiv 6 \ (mod\ 5)$$

Como $mmc(2, 3, 4, 5) = 60$, *temos que* $6x \equiv 6 \ (mod\ 60)$. *Dividindo a relação por* 6 *segue que* $x \equiv 1 \ (mod\ 10)$. *Logo* $10 \mid x - 1$ *e assim* $\exists y \in \mathbb{Z}$ *tal que* $x - 1 = 10y$, *ou seja,* $x - 10y = 1$. *Observe que uma solução particular desse sistema é tomando* $x = 11$ *e* $y = 1$. *Note também que* $x = 11$ *é o menor positivo que satisfaz essa relação. Logo* $11 \equiv 1 \ (mod\ 10)$ *e, portanto:*

$$66 \equiv 6 \ (mod\ 2)$$
$$66 \equiv 6 \ (mod\ 3)$$
$$66 \equiv 6 \ (mod\ 4)$$
$$66 \equiv 6 \ (mod\ 5)$$

Proposição 29. *Sejam* $a, m \in \mathbb{Z}$, $m > 1$. *A congruência* $ax \equiv 1 \ (mod\ m)$ *tem solução se, e somente se,* $mdc(a, m) = 1$. *Além disso, se* x_0 *for uma solução então a solução geral da congruência será* $x \equiv x_0 \ (mod\ m)$.[1]

Demonstração. ($\Rightarrow$) Suponha que a congruência $ax \equiv 1 \ (mod\ m)$ tem uma solução x_0. Se $ax_0 \equiv 1 \ (mod\ m)$ então $m \mid ax_0 - 1$ e ainda $ax_0 - 1 = my_0 \Leftrightarrow ax_0 + m(-y_0) = 1$, $y_0 \in \mathbb{Z}$. Logo, $mdc(a, m) = 1$.

($\Leftarrow$) Reciprocamente, se $mdc(a, m) = 1$ então $\exists x_1, y_1, \in \mathbb{Z}$ tal que $ax_1 + my_1 = 1 \Leftrightarrow ax_1 - 1 = m(-y_1)$. Logo, $m \mid ax_1 - 1$ e, portanto, $ax_1 \equiv 1 \ (mod\ m)$, isto é, a congruência tem solução.

Por outro lado, sejam x_1, x_2 soluções da congruência. Então:

$$\begin{cases} ax_1 \equiv 1 \ (mod\ m) \\ ax_2 \equiv 1 \ (mod\ m) \end{cases} \Rightarrow ax_1 \equiv ax_2 \ (mod\ m)$$

[1] (HEFEZ, 2016), página 194.

Como $mdc(a, m) = 1$, temos que $x_1 \equiv x_2 \ (mod\ m)$. Portanto, qualquer x_i que seja solução então a solução geral da congruência será dado por $x \equiv x_0 \ (mod\ m)$.

□

Definição 20. *Um Sistema de Resíduos Reduzido (S.R.R.) módulo m é um conjunto $\{r_1, r_2, \cdots, r_k\}$ de inteiros tal que:*

(*i*) $mdc(r_i, m) = 1$, $\forall i = 1, \cdots, k$

(*ii*) $r_i \not\equiv r_j \ (mod\ m)$ *se* $i \neq j$

(*iii*) *Para cada* $n \in \mathbb{Z}$ *tal que* $mdc(n, m) = 1$ *existe* $i \in \{1, 2, \cdots, k\}$ *tal que* $n \equiv r_i \ (mod\ m)$.[1]

Exemplo 24. *Temos que um S.C.R módulo* 6 *é dado por* $\{0, 1, 2, 3, 4, 5\}$. *Um S.R.R. módulo* 6 *são os números em que* $mdc(6, s) = 1$, $s \in \{0, 1, 2, 3, 4, 5\}$, *ou seja, coprimos. Assim, temos que o S.R.R. módulo* 6 *é* $\{1, 5\}$.

Definição 21. *Denominaremos por $\varphi(m)$ o número de elementos de um S.R.R. módulo m ($m > 1$) que corresponde a quantidade de números entre* 0 *a* $m-1$ *que são primos com m. Dado $\varphi(1) = 1$, definimos:*

$$\varphi : \mathbb{N} \to \mathbb{N}$$
$$\varphi(n) = s$$

em que s e a quantidade de números naturais menores que n que são primos com n.[2]

Exemplo 25. *Dados* $m = 3, n = 10$, *temos que* $\varphi(3) = 2$ *e* $\varphi(10) = 4$

Observação 11. (1) *Pela definição concluímos que* $\varphi(m) \leq m - 1$, $\forall m \geq 2$.
(2) *Dado p primo, temos que* $\varphi(p) = p - 1$, *pois* $\{1, 2 \cdots, p - 1\}$ *são primos com p.*

Proposição 30. *Sejam* $r_1, r_2, \cdots, r_{\varphi(m)}$ *um S.R.R. módulo m e seja* $a \in \mathbb{Z}$ *tal que* $mdc(a, m) = 1$. *Então,* $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ *é um S.R.R. módulo m.*[3]

[1] (HEFEZ, 2016), página 194.
[2] (HEFEZ, 2016), página 195.
[3] (HEFEZ, 2016), página 197.

Demonstração. De fato, se $r_1, r_2, \cdots, r_{\varphi(m)}$ é um S.R.R. módulo m segue por definição que $r_i \not\equiv r_j \ (mod\ m)$, $\forall i \neq j$. Como $mdc(a, m) = 1$, então $ar_i \not\equiv ar_j \ (mod\ m)$, $\forall i \neq j$. Portanto, $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ é um S.R.R. módulo m.

□

Teorema 14. (*Teorema de Euler*) *Sejam $m, a \in \mathbb{Z}$, $m > 1$, com $mdc(a, m) = 1$, então $a^{\varphi(m)} \equiv 1 \ (mod\ m)$.*[1]

Demonstração. Considere um S.R.R. módulo m dado por $r_1, r_2, \cdots, r_{\varphi(m)}$. Pela proposição anterior segue que $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ também é um S.R.R. módulo m. Como $mdc(a, m) = 1$, segue que:

$$\left.\begin{array}{l} ar_1 \equiv r_1 \ (mod\ m) \\ ar_2 \equiv r_2 \ (mod\ m) \\ \quad\vdots \\ ar_{\varphi(m)} \equiv r_{\varphi(m)} \ (mod\ m) \end{array}\right. \Rightarrow ar_1 ar_2 \cdots ar_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \ (mod\ m)$$

Como $ar_1 ar_2 \cdots ar_{\varphi(m)} = a^{\varphi(m)} \left(r_1 r_2 \cdots r_{\varphi(m)}\right)$ e como $mdc(r_i, m) = 1$, com $i = 1, \cdots, \varphi(m)$, pois r_i é um S.R.R. módulo m então $mdc((r_1 r_2 \cdots r_{\varphi(m)}, m) = 1$. Assim:

$$a^{\varphi(m)} \left(r_1 r_2 \cdots r_{\varphi(m)}\right) \equiv r_1 r_2 \cdots r_{\varphi(m)} \ (mod\ m) \Leftrightarrow a^{\varphi(m)} \equiv 1 \ (mod\ m)$$

□

Observação 12. *Note que se $m = p$ e p primo, então $a^{\varphi(p)} \equiv 1 \ (mod\ p) \Leftrightarrow a^{p-1} \equiv 1 \ (mod\ p)$.*

Proposição 31. *Sejam $a, b \in \mathbb{N}$ tal que $mdc(a, b) = 1$. Logo, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.*[2]

Demonstração. Se $a = b = 1$ ou $a = 1$ ou $b = 1$ o resultado é de imediato, pois $\varphi(1 \cdot 1) = \varphi(1) = 1$ e que $\varphi(a \cdot 1) = \varphi(a)$, $\varphi(1 \cdot b) = \varphi(b)$. Suponha que $a > 1$ ou $b > 1$ e considere a seguinte tabela dos naturais de 1 até ab:

[1] (HEFEZ, 2016), página 197.
[2] (HEFEZ, 2016), página 199.

1	2	$\cdots$	k	$\cdots$	b
$b+1$	$b+2$	$\cdots$	$b+k$	$\cdots$	$2b$
$2b+1$	$2b+2$	$\cdots$	$2b+k$	$\cdots$	$3b$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$(a-1)b+1$	$(a-1)b+2$	$\cdots$	$(a-1)b+k$	$\cdots$	$(a-1)b+b=ab$

Para encontrar $\varphi(ab)$, vamos determinar os números que são simultaneamente primos com a e b, ou seja, $mdc(ab,c)=1$ e, pelas propriedades de mdc, segue que $mdc(ab,c)=1$ se, e somente se, $mdc(a,c)=mdc(b,c)=1$.

Note que se algum elemento pertencente a coluna não for primo com b então o restante da coluna não será primo com b, pois este número somado com múltiplos de b não será primo com b. Logo, os elementos primo com b estarão nas colunas restantes, formando $\varphi(b)$ elementos.

Por outro lado, como $mdc(a,b)=1$ e pela Proposição 27, a sequência $k, b+k, \cdots, (a-1)b+k$ formam um S.C.R. módulo a. Assim, $\varphi(a)$ desses elementos são primos com a. Portanto, os números que são primos simultaneamente com a e b é dado por $\varphi(a)\cdot\varphi(b)$, ou seja, $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$.

□

Exemplo 26. *Dado $n=6$, segue que $\varphi(6)=\varphi(3\cdot 2)=\varphi(3)\cdot\varphi(2)=(3-1)\cdot(2-1)=2$.*

Proposição 32. *Se p é primo e $r\in\mathbb{N}$. Então $\varphi(p^r)=p^r-p^{r-1}=p^r\left(1-\dfrac{1}{p}\right)$.*[1]

Demonstração. Temos que $\varphi(p^r)$ é a quantidade de elementos menores que p^r que são primos com p^r. De 1 até p^r, temos p^r números naturais. Excluindo os múltiplos de p^r, ou seja, $p, 2p, \cdots, p^{r-1}p$. Logo, temos p^{r-1} números naturais. Assim, $\varphi(p^r)=p^r-p^{r-1}$.

□

Exemplo 27. *Dado 5^3, segue que $\varphi(5^3)=5^3-5^2=125-25=100$ números entre 0 a 5^2 que são primos com 5^3.*

Proposição 33. *Seja $m>1$ tal que $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, então:*

$$\varphi(m)=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

[1] Proposições 32 e 33;(HEFEZ, 2016), página 82.

Demonstração. De fato, se $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, então

$$\begin{aligned}
\varphi(m) &= \varphi\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\right) \\
&= \varphi\left(p_1^{\alpha_1}\right) \varphi\left(p_2^{\alpha_2}\right) \cdots \varphi\left(p_r^{\alpha_r}\right) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

□

Observação 13. *Note que:*

$$\begin{aligned}
\varphi(m) &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\
&= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_r^{\alpha_r - 1}\left(p_1 - 1\right)\left(p_2 - 1\right) \cdots \left(p_r - 1\right).
\end{aligned}$$

Exemplo 28. *Encontre o resto da divisão de* 5^{320} *por* 34. *Temos que* $mdc(5, 34) = 1$, *logo pelo Teorema de Euler, segue que* $5^{\varphi(34)} \equiv 1 \ (mod\ 34)$ *e que* $\varphi(34) = \varphi(2)\varphi(17) = 1 \cdot 16 = 16$. *Assim,* $5^{16 \cdot q} \equiv 1 \ (mod\ 34)$. *Tomando* $q = 20$, *segue que* $5^{320} \equiv 1 \ (mod\ 34)$. *Portanto, o resto da divisão de* 5^{320} *por* 34 *é* 1.

Proposição 34. *Dados* $a, m \in \mathbb{Z}$, *com* $m \geq 2$. *Então* $\exists h \in \mathbb{N}$ *tal que* $a^h \equiv 1 \ (mod\ m)$ *se, e somente se,* $mdc(a, m) = 1$.[1]

Demonstração. ($\Rightarrow$) Suponha que existe $h \in \mathbb{N}$ tal que $a^h \equiv 1 \ (mod\ m)$. Se $h = 1$, então $a \equiv 1 \ (mod\ m)$, ou seja, $m \mid a - 1$. Logo, $a - 1 = mq \Leftrightarrow a + mq = 1$, $q \in \mathbb{Z}$. Daí, pelo Teorema de Bézout, $mdc(a, m) = 1$. Se $h > 1$, segue pela Proposição 29 que a congruência $ax \equiv 1 \ (mod\ m)$ tem solução se, e somente se, $mdc(a, m) = 1$. Tomando $x = a^{h-1}$, temos o resultado.

($\Leftarrow$) Reciprocamente, se $mdc(a, m) = 1$ segue pelo Teorema de Euler que $a^{\varphi(m)} \equiv 1 \ (mod\ m)$. Tomando $h = \varphi(m) \in \mathbb{N}$, temos o resultado.

□

[1] (HEFEZ, 2016), página 201.

Proposição 35. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. Então, $ab \equiv 1 \pmod{m}$ se, e somente se, $mdc(a, m) = 1$, isto é, b é o inverso de a módulo m.*

Demonstração. ($\Rightarrow$) Se $ab \equiv 1 \pmod{m}$, então $m \mid ab - 1$, ou seja, $ab - 1 = mk$, $k \in \mathbb{Z}$. Logo, $ab + m(-k) = 1$. Assim, essa solução diofantina tem solução se, e somente se, $mdc(a, m) = 1$.

($\Leftarrow$) Por outro lado, se $mdc(a, m) = 1$, pela Identidade de Bézout segue que $ax + my = 1 \Leftrightarrow ax - 1 = m(-y)$ e, portanto, $ax \equiv 1 \pmod{m}$. Tomando $x = b$, o resultado segue.

□

2.2 Congruências Lineares

Proposição 36. *Sejam x_0, y_0 uma solução da equação $aX+bY = c$, em que $mdc(a, b) = 1$. Então as soluções $x, y \in \mathbb{Z}$ são da forma:*

$$x = x_0 + tb \text{ e } y = y_0 - ta,\ t \in \mathbb{Z}.$$

Demonstração. Sejam $x, y \in \mathbb{Z}$ uma outra solução da equação $aX + bY = c$. Então, $ax + by = c$ e $ax_0 + by_0 = c$. Logo:

$$ax + by = ax_0 + by_0 \Leftrightarrow a(x - x_0) = b(y_0 - y) \tag{3}$$

De (3), segue que $b \mid a(x - x_0)$. Como $mdc(a, b) = 1$, temos que $b \mid x - x_0$. Assim, $x - x_0 = bt \Leftrightarrow x = x_0 + tb$, $t \in \mathbb{Z}$. Novamente por (3) e do fato que $mdc(a, b) = 1$, temos que $a \mid y_0 - y$. Portanto, $y_0 - y = ta \Leftrightarrow y = y_0 - ta$, $t \in \mathbb{Z}$.

□

Proposição 37. *Dados $a, b, m \in \mathbb{Z}$, a congruência $ax \equiv b\ (mod\ m)$ tem solução se, e somente se, $d = mdc(a, m)$ divide b. E ainda que, se x_0 for uma solução de $ax \equiv b\ (mod\ m)$, então todo $x \in \mathbb{Z}$, $x \equiv x_0\ (mod\ m)$.*[1]

Demonstração. Seja x solução da congruência. Então $ax \equiv b\ (mod\ m)$. Logo $m \mid ax - b$ e ainda que $ax - b = my \Leftrightarrow ax - my = b, y \in \mathbb{Z}$, que tem solução se, e somente se, $mdc(a, m)$ divide b.

[1] (HEFEZ, 2016), página 212.

Por outro lado, se x_0 é uma solução de $aX \equiv b\ (mod\ m)$, então:

$$\begin{cases} ax \equiv b\ (mod\ m) \\ ax_0 \equiv b\ (mod\ m) \end{cases} \Rightarrow ax \equiv ax_0\ (mod\ m)$$

Como $mdc(a, m) = 1$, temos $x \equiv x_0\ (mod\ m)$.

□

Exemplo 29. *Dado* $2x \equiv 5\ (mod\ 7)$*, segue que* 6 *é uma solução. Tomando* $x_0 = 6$*, segue que* $x \equiv 6\ (mod\ 7)$*, ou seja,* $x - 6 = 7q \Leftrightarrow x = 6 + 7q$*,* $q \in \mathbb{Z}$*, é solução geral da equação. Assim, escolhendo valores para* q*, automaticamente, obtemos infinitas de soluções.*

Teorema 15. *Sejam* $a, b, m \in \mathbb{Z}$*, com* $m > 1$ *e que* $d = mdc(a, m) \mid b$*. Se* x_0 *é uma solução da congruência* $aX \equiv b\ (mod\ m)$*, então:*

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

formam um sistema de soluções da congruência duas a duas incongruentes módulo m*.*[1]

Demonstração. Considere $\bar{x}$ uma solução qualquer de $aX \equiv b\ (mod\ m)$. Logo, $a\bar{x} \equiv b\ (mod\ m)$ e como por hipótese x_0 também é uma solução, então $ax_0 \equiv b\ (mod\ m)$. Por transitividade, temos que $a\bar{x} \equiv ax_0\ (mod\ m)$ e dado $d = mdc(a, m)$, segue que $\bar{x} \equiv x_0\ \left(mod\ \frac{m}{d}\right)$, ou seja, $\bar{x} - x_0 = \frac{m}{d}k$, $k \in \mathbb{Z}$. Pela divisão euclidiana entre k e d, temos $k = dq + r$ com $0 \leq r < d$. Logo, $\bar{x} = x_0 + \frac{m}{d}(dq + r) = x_0 + mq + r\frac{m}{d}$. Agora observe o seguinte, $\bar{x} = x_0 + mq + r\frac{m}{d} \equiv x_0 + r\frac{m}{d}\ (mod\ m)$ (pois $mq \equiv 0(mod\ m)$), com $0 \leq r \leq d - 1$.

Mostremos agora que estas soluções são duas a duas incongruentes.

De fato, note que se $x_0 + r\frac{m}{d} \equiv x_0 + s\frac{m}{d}\ (mod\ m)$, então $r\frac{m}{d} \equiv s\frac{m}{d}\ (mod\ m)$, com $0 \leq r, s < d$. Multiplicando a desigualdade por $\frac{m}{d}$, segue que $0 \leq r\frac{m}{d}, s\frac{m}{d} < m$. Logo, $\left|r\frac{m}{d} - s\frac{m}{d}\right| = \frac{m}{d}|r - s| < \frac{m}{d} \cdot d = m$. Assim, $m \nmid \left|r\frac{m}{d} - s\frac{m}{d}\right|$ se $r \neq s$. Portanto, $x_0 + r\frac{m}{d} \equiv x_0 + s\frac{m}{d}\ (mod\ m)$ são incongruentes dois a dois.

□

Exemplo 30. *Dada a congruência* $4X \equiv 8\ (mod\ 12)$*, temos que* $mdc(4, 12) = 4$*. Logo, existem* 4 *soluções. Note que* $x_0 = 2$ *é uma solução. Assim, pelo Teorema anterior, segue que as soluções são:* $2, 5, 8, 11$*.*

[1] (HEFEZ, 2016), página 213.

Corolário 10. *Se $a, b, m \in \mathbb{Z}$, $m > 1$ e $mdc(a, m) = 1$ então a congruência $aX \equiv b \ (mod\ m)$ tem somente uma solução.*

Demonstração. De fato, pelo Teorema anterior que temos $d - 1$ soluções distintas. Daí, como $mdc(a, m) = 1 = d$, segue que a congruência possui apenas uma solução.

□

Teorema 16. (*Teorema de Wilson*) *Se p é primo então $(p-1)! \equiv -1 \ (mod\ p)$.*[1]

Demonstração. O resultado é válido para $p = 2$ e $p = 3$, pois:

$$(2-1)! = 1 \equiv -1 \ (mod\ 2)$$
$$(3-1)! = 2 \equiv -1 \ (mod\ 3)$$

Suponha agora $p \geq 5$. Para qualquer $i \in \{1, 2, \cdots, p-1\}$ podemos afirmar que $ix \equiv 1 \ (mod\ p)$, ou seja, $\exists! j \in \{1, 2, \cdots, p-1\}$ tal que $i \cdot j \equiv 1 \ (mod\ p)$. Em contrapartida, temos que $i^2 \equiv 1 \ (mod\ p) \Leftrightarrow p \mid i^2 - 1 \Leftrightarrow p \mid (i+1)(i-1)$. Como p é primo, temos que $p \mid i+1$ ou $p \mid i-1$, então $i = 1$ ou $i = p-1$. Retirando esses valores, temos que de 2 a $p-2$ temos uma quantidade par de elementos, haja vista que $p \geq 5$ primo é impar e como $\exists! j \in \{1, 2, \cdots, p-1\}$ tal que $i \cdot j \equiv 1 \ (mod\ p)$, segue que $2 \cdot 3 \cdots (p-2) \equiv 1 \ (mod\ p)$. Multiplicando a congruência por 1 e $p-1$, segue que $1 \cdot 2 \cdots (p-2) \cdot (p-1) = (p-1)! \equiv p - 1 \equiv -1 \ (mod\ p)$.

□

Proposição 38. *Toda congruência linear $ax \equiv b \ (mod\ m)$ que tem solução é equivalente a uma congruência da forma $x \equiv c \ (mod\ n)$.*[2]

Demonstração. De fato, se $ax \equiv b \ (mod\ m)$ tem solução, então $mdc(a, m) = d \mid b$. Logo, $d \mid a$ e $d \mid m$, ou seja, $a = a'd$, $m = dn$, com $a', n \in \mathbb{Z}$. Como $d \mid b$, então $\exists b' \in \mathbb{Z}$ tal que $b = b'd$. Assim, $a' = \dfrac{a}{d}$, $n = \dfrac{m}{d}$ e $b' = \dfrac{b}{d}$. Multiplicando a congruência por d, temos $a'x \equiv b' \ (mod\ n)$ em que $mdc(a', n) = 1$ e, multiplicando novamente a congruência por $a'' \in \mathbb{Z}$ tal que $a'' \cdot a' = 1$, temos $x \equiv c \ (mod\ n)$, em que $c = a' \cdot b'$.

□

[1] (SANTOS, 1998), página 65.
[2] (HEFEZ, 2016), página 214.

Exemplo 31. *Dada a congruência* $3x \equiv 2\ (mod\ 5)$*, procuraremos qual número de* 1 *a* 4 *que multiplicado por* 3 *é côngruo a* 1*, ou seja,* $3x \equiv 1\ (mod\ 5)$*. Tomando* $x = 2$*, temos que* $3 \cdot 2 = 6 \equiv 1(mod\ 5)$*. Daí, como* $mdc(3, 5) = 1$*, multiplicando* $3x \equiv 2\ (mod\ 5)$ *por* 2 *temos* $x \equiv 4\ (mod\ 5)$*.*

Proposição 39. *O sistema de congruência* $X \equiv c_1\ (mod\ m_1)$*,* $X \equiv c_2\ (mod\ m_2)$ *admite solução se, e somente se,* $c_1 \equiv c_2\ (mod\ d)$*, em que* $d = mdc(m_1, m_2)$*. Além disso, dada uma solução* a *do sistema temos que* a' *também é solução se, e somente se,* $a' \equiv a\ (mod\ m)$*, em que* $m = mmc(m_1, m_2)$*.*[1]

Demonstração. Primeiro, mostremos que a sistema de congruência admite solução se, e somente se, $c_1 \equiv c_2\ (mod\ d)$. Seja x uma solução do sistema, então $x \equiv c_1\ (mod\ m_1)$ e $x \equiv c_2\ (mod\ m_2)$. Logo, $x - c_1 = m_1k_1$ e $x - c_2 = m_2k_2$ com $k_1, k_2 \in \mathbb{Z}$. Subtraindo as igualdades, segue que $m_1k_1 - m_2k_2 = c_2 - c_1$. Por sua vez, essa equação diofantina terá solução se, e somente se, $d = mdc(m_1, m_2) \mid c_1 - c_2$, isto é, $c_1 \equiv c_2\ (mod\ d)$.

Mostremos agora que dada uma solução a do sistema temos que a' também é solução se, e somente se, $a' \equiv a\ (mod\ m)$, em que $m = mmc(m_1, m_2)$.

($\Rightarrow$) Sejam a e a' soluções do sistema, então pela transitividade temos que $a \equiv c_1 \equiv a'\ (mod\ m_1)$ e $a \equiv c_2 \equiv a'\ (mod\ m_2)$. Daí, pela Proposição 28, segue que $a \equiv a'\ (mod\ m)$, em que $m = mmc(m_1, m_2)$.

($\Leftarrow$) Reciprocamente, se $a' \equiv a\ (mod\ m)$, em que $m = mmc(m_1, m_2)$. Como a é solução do sistema $X \equiv c_1\ (mod\ m_1)$, $X \equiv c_2\ (mod\ m_2)$, segue por transitividade que $a' \equiv a \equiv c_1\ (mod\ m_1)$ e $a' \equiv a \equiv c_2\ (mod\ m_2)$.

□

Teorema 17. (*Teorema do Resto Chinês*) *Suponha que* $mdc(m_i, m_j) = 1$*,* $\forall i, j = 1, \cdots, r$ *com* $i \neq j$*. Então o sistema*

$$X \equiv c_i\ (mod\ m_i), i = 1, \cdots, r \tag{1}$$

tem uma única solução módulo $M = m_1m_2 \cdots m_r$ *dado por:*

$$x = M_1y_1c_1 + M_2y_2c_2 + \cdots + M_ry_rc_r,$$

[1] (HEFEZ, 2016), página 219.

em que $M_i = \dfrac{M}{m_i}$ *e* y_i *é solução de* $M_i y_i \equiv 1 \ (mod\ m_i)$, $i = 1, \cdots, r$.[1]

Demonstração. Mostremos inicialmente que x é solução de (1).

Mostremos que é satisfeita a primeira equação do sistema. De fato, se $M_1 y_1 \equiv 1 \ (mod\ m_1)$ então $M_1 y_1 c_1 \equiv c_1 \ (mod\ m_1)$, pois se $mdc(m_i, m_j) = 1$, $\forall i \neq j$, segue que $mdc(m_1, M_1) = 1$. Como $M_2 = \dfrac{M}{m_2} = m_1 m_3 \cdots m_r$, então $m_1 \mid M_2$ e ainda que $M_2 y_2 c_2$ é múltiplo de m_1. Então a congruência $M_2 y_2 c_2 \equiv 0 \ (mod\ m_1)$. Utilizando o mesmo raciocínio, concluímos que $m_1 \mid M_j$, para $j \neq 1$, ou seja, $M_j y_j c_j \equiv 0 \ (mod\ m_1)$. Daí, somando as congruências, temos:

$$M_1 y_1 c_1 + M_2 y_2 c_2 + \cdots + M_r y_r c_r = x \equiv c_1 \ (mod\ m_1)$$

Mostremos que x satisfaz c_2. Como $m_2 \mid M_j$, $j \neq 2$ e pelo fato que $M_2 y_2 c_2 \equiv c_2 \ (mod\ m_2)$, segue que:

$$\begin{aligned} M_1 y_1 c_1 &\equiv 0 \ (mod\ m_2) \\ M_2 y_2 c_2 &\equiv c_2 \ (mod\ m_2) \\ &\vdots \\ M_r y_r c_r &\equiv 0 \ (mod\ m_2) \end{aligned}$$

Somando as congruência, temos $x \equiv c_2 \ (mod\ m_2)$. Continuando este mesmo raciocínio, concluímos que $x \equiv c_i \ (mod\ m_i)$, com $i = 1, \cdots, r$.

Mostremos agora que x é a única solução módulo $M = m_1 m_2 \cdots m_r$.

Seja $\bar{x}$ uma outra solução do sistema $X \equiv c_i \ (mod\ m_i)$, $i = 1, \cdots, r$. Então $\bar{x} \equiv c_i \ (mod\ m_i)$ e pelo fato de x também ser solução do sistema de congruência, segue pela transitividade que $\bar{x} \equiv x \ (mod\ m_i)$, $i = 1, \cdots, r$. Logo, pela Proposição 28 temos que $\bar{x} \equiv x \ (mod\ M)$, em que $M = mmc(m_1, m_2, \cdots, m_r)$. Como $mdc(m_i, m_j) = 1$, $\forall i \neq j$, segue que $M = mmc(m_1, m_2, \cdots, m_r) = m_1 \cdot m_2 \cdot m_r$.

□

Exemplo 32. *No primeiro século de nossa era, o matemático chinês Sun-Tsu propôs o seguinte problema "Qual é o números que deixa resto* 2, 3 *e* 2 *quando divididos res-*

[1] (HEFEZ, 2016), página 217.

pectivamente por 3, 5 *e* 7*?" Através do Teorema do Resto Chinês, vamos determinar a solução.*

Temos que:

$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 2 \ (mod\ 7)$$

em que $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $M = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$ *e* $c_1 = 2$, $c_2 = 3$, $c_3 = 2$.

Logo, y_1 *é solução de* $M_1 y_1 \equiv 1 \ (mod\ m_1)$*, isto é* $35y_1 \equiv 1 \ (mod\ 3)$*. Como* $35 \equiv 2 \ (mod\ 3)$*, segue que* $2y_1 \equiv 1 \ (mod\ 3)$*. Procuraremos agora um número de* $1, \cdots, m_1 - 1$ *que multiplicado por* 2 *é côngruo a* 1 *módulo* 3*. Por verificação temos que* $y_1 = 2$.

Aplicando este mesmo raciocínio, temos que $21y_2 \equiv 1 \ (mod\ 5) \Leftrightarrow y_2 \equiv 1 \ (mod\ 5)$*. Procurando um número de* $1, \cdots, m_2 - 1$ *que multiplicado por* 1 *é côngruo a* 1 *módulo* 5*, temos que* $y_2 = 1$.

Ainda, $15y_3 \equiv 1 \ (mod\ 7) \Leftrightarrow y_3 \equiv 1 \ (mod\ 7)$*. Procurando um número de* $1, \cdots, m_3 - 1$ *que multiplicado por* 1 *é côngruo a* 1 *módulo* 7*, temos que* $y_3 = 1$.

Assim, pelo Teorema do Resto Chinês segue que:

$$\begin{aligned} x &= M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 \\ &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \\ &= 233 \end{aligned}$$

Portanto $233 \equiv 23 \ (mod\ 105)$ *e qualquer solução é da forma* $x = 23 + 105t$, $t \in \mathbb{Z}$.

3 Criptografia RSA

Criptografia deriva da palavra grega kriptos, significando "*escrita oculta*", e a ocultação de mensagens já era empregada desde a Grécia Antiga. Tais estratégias eram utilizadas com o objetivo de garantir segurança e privacidade, ocultando mensagens diante das pessoas e permitindo que somente seu legítimo destinatário fosse capaz de decifrá-las.

O mais famoso sistema de criptografia foi utilizado na Roma antiga por Júlio

César, cujo sistema consistia em substituir cada letra do alfabeto por outra, conforme segue:

a	b	c	d	e	f	g	h	i	j	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P

n	o	p	q	r	s	t	u	v	x	w	y	z
Q	R	S	T	U	V	X	W	Y	Z	A	B	C

Tabela 2: Cifra de César

Denominada "*Cifra de César*" o alfabeto de César consistia em substituir a letra correspondente pela terceira letra em sua frente no alfabeto.

Exemplo 33. *Vejamos como ficaria a seguinte palavra: programa de pós graduação em matemática aplicada. Como a língua utilizada na época era o latim, traduzindo a frase, temos: graduati progressio in mathematica applicata. Aplicando a cifra, segue que:*

g r a d u a t i p r o g r e s s i o

J U D G W D X L S U R J U H V V L R

i n m a t h e m a t i c a

L Q P D X K H P D X L F D

a p p l i c a t a

D S S O L F D X A

Este tipo de cifra é chamado de *cifra por substituição simples* e mais detalhes de outros tipos de criptografia pode ser encontrado em (SINGH, 2004).

A seguir estaremos interessados em entender o funcionamento da criptografia RSA, para mais detalhes verifique (HEFEZ, 2016; SOUZA, ; COUTINHO, 1997; BURTON, 2010; SPINA, 2014; PAGLIUSI, 1998; BRESSOUD et al., 2000).

3.1 O sistema RSA

Na criptografia existem dois tipos de chaves: a simétrica, em que ambas as partes concordam com a mesma chave para estabelecer os parâmetros tanto para a codificação quanto para a decodificação; o que apresenta dois desafios quando pensados em

larga escala: o primeiro, é a necessidade de transmitir essa chave de forma segura para o destinatário da mensagem; o segundo é que essa chave precisa ser compartilhada por várias partes, o que aumenta o risco de interceptação.

Por outro lado, a criptografia assimétrica envolve o uso de pares de chaves, sendo uma pública para criptografar mensagens e outra privada para descriptografar a mensagem recebida e é com essas chaves que o sistema RSA foi implementado. Cada usuário deste sistema possui seu próprio conjunto de chaves, o que elimina a necessidade de compartilhar a mesma chave entre várias partes e assim garantir a segurança das comunicações.

Foram Whitfield Diffie e Martin Hellman em 1976 os responsáveis por introduzir a ideia do primeiro sistema criptográfico de chave pública, que posteriormente inspirou o desenvolvimento do algoritmo RSA por Ronald Rivest, Adi Shamir e Leonard Adleman em 1977 (HEFEZ, 2016).

O princípio deste sistema se baseia na facilidade de encontrar dois números primos grandes p e q (onde cada um conta com 100 dígitos ou mais) e ao mesmo tempo na dificuldade prática em fatorar o produto desses primos.

Como dito no sistema assimétrico, cada usuário possui um par de chaves: uma chave pública (n, e) e uma chave privada (n, d). A chave pública está disponível para quem deseja enviar uma mensagem, enquanto a chave privada, também conhecida como chave de decodificação, é mantida em posse exclusiva do destinatário final.

O primeiro passo para utilizar o método RSA envolve a conversão da mensagem em uma sequência de números. Para simplificar, suponhamos que a mensagem original seja um texto que contenha apenas palavras, sem números. Portanto, a mensagem é composta apenas pelas palavras e pelos espaços entre elas.

Logo, utilizando a seguinte tabela de conversão, obtemos o número correspondente de cada letra:

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	X	W	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 3: Tabela de Conversão

Não utilizamos a tabela começando do 1 em diante para evitar ambiguidades. Por exemplo, se a tabela começasse do 1, teríamos que $a = 1$, $b = 2$ e $l = 12$. Logo, para evitar este tipo de situação, utilizamos a tabela acima e, o espaço entre as duas palavras será substituído pelo número 99 quando feita a conversão. Considere as seguintes palavras: criptografia RSA. Convertendo, temos:

$$1327182529241627101518109927 2810$$

Antes de prosseguir, é necessário definir os parâmetros do sistema RSA que serão utilizados. Esses parâmetros consistem em dois números primos distintos, denotados por p e q, nos quais $p \cdot q = n$. A próxima etapa envolve a divisão em blocos do número resultante no exemplo anterior. Mas com cuidado, pois para a escolha dos blocos, é necessário que tomemos algumas precauções, como por exemplo, que o bloco comece por 0, pois isso se torna necessário para evitar complicações durante a decodificação, pois o zero representa uma letra e há o risco de perdê-la nos processos de codificação e decodificação. Dessa forma, tomando, por exemplo, $p = 11$ e $q = 13$, obtemos $n = 143$. Dessa forma, a mensagem mencionada no exemplo anterior pode ser dividida nos seguintes blocos (em que cada bloco é menor do que n):

$$13 - 27 - 18 - 25 - 29 - 24 - 16 - 27$$
$$10 - 15 - 18 - 10 - 99 - 27 - 28 - 10$$

Definido a pré-decodificação, passaremos para a codificação. Para codificamos a mensagem precisamos de n e de um $e \in \mathbb{N}$ tal que $mdc(e, \varphi(n)) = 1$, ou seja, inversível módulo $\varphi(n)$. Note que, como $n = pq$ com p e q primos. Então $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$. Chamaremos o par (n, e) de *chave de codificação* (ou pública) do sistema que estamos usando. Para codificar a mensagem, procederemos codificando cada bloco separadamente. A mensagem codificada será então formada pela sequência dos blocos previamente codificados.

Tendo a chave de codificação (n, e), veremos como codificar cada um dos blocos. Seja b um inteiro positivo menor que n tal que b é um bloco pré codificado, vamos denotar o bloco codificado por $C(b)$, na qual $C(b)$ é o resto da divisão de b^e por n, isto é:

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

Voltando ao exemplo anterior, temos que $p = 11$, $q = 13$ e $n = 143$. Logo, $\varphi(n) = 120$. Tomando $e = 7$ o menor inteiro tal que o $mdc(120, 7) = 1$ (e, portanto, inversível) temos para cada um dos blocos pré codificados:

$$13^7 \equiv 52^2 \cdot 13 \equiv 117 \ (mod\ 143)$$
$$27^7 \equiv 14 \ (mod\ 143)$$
$$18^7 \equiv 138 \ (mod\ 143)$$
$$25^7 \equiv 64 \ (mod\ 143)$$
$$29^7 \equiv 94 \ (mod\ 143)$$
$$24^7 \equiv 106 \ (mod\ 143)$$
$$16^7 \equiv 3 \ (mod\ 143)$$
$$10^7 \equiv 10 \ (mod\ 143)$$
$$15^7 \equiv 115 \ (mod\ 143)$$
$$99^7 \equiv 44 \ (mod\ 143)$$
$$28^7 \equiv 63 \ (mod\ 143)$$

Codificando todos os blocos da mensagem, temos:

$$117 - 14 - 143 - 64 - 94 - 106 - 3 - 14$$
$$10 - 115 - 143 - 10 - 44 - 14 - 63 - 10$$

Agora, vamos examinar o processo de decodificação de um bloco da mensagem codificada. Para realizar essa operação, precisamos de duas informações essenciais: o valor de n e o inverso de e módulo $\varphi(n)$, que iremos representar como d, em que $d \in \mathbb{N}$. Esse par de valores, (n, d), é conhecido como a *chave de decodificação* (ou privada). Suponha que a seja um bloco da mensagem codificada; então, $D(a)$ será o resultado obtido após o processo de decodificação, isto é, $a^d \equiv D(a) \ (mod\ n)$.

Tendo em vista que $\varphi(n)$ e e são conhecidos, então basta aplicar o Algoritmo de Euclides Estendido. Como $\varphi(n) = 120$ e $e = 7$, segue que dividindo $\varphi(n)$ por e, temos:

$$120 = 7 \cdot 17 + 1 \Leftrightarrow 1 = 120 + 7(-17)$$

Ou seja, o inverso de 7 módulo 120 é -17. Como d tem que pertencer aos naturais, então d tem que ser positivo. Logo, $d = 120 - 17 = 103$. Assim, para decodificar o bloco 117, calculamos 117^{103} módulo 143. Fazendo os cálculos, temos:

$$\begin{aligned}
117^{103} &\equiv -26^{103} \ (mod\ 143) \\
&\equiv -\underbrace{26^5 \cdots 26^5}_{20 \text{ vezes}} \cdot 26^3 \ (mod\ 143) \\
&\equiv -\underbrace{78 \cdots 78}_{20 \text{ vezes}} \cdot 26^3 \ (mod\ 143) \\
&\equiv -78^5 \cdot 78^5 \cdot 78^5 \cdot 78^5 \cdot 26^3 \ (mod\ 143) \\
&\equiv -78 \cdot 78 \cdot 78 \cdot 78 \cdot 26^3 \ (mod\ 143) \\
&\equiv -78 \cdot 26^3 \ (mod\ 143) \\
&\equiv -130 \equiv 13 \ (mod\ 143)
\end{aligned}$$

Fazendo os devidos cálculos para cada um dos blocos, obtemos:

$$\begin{aligned}
14^{103} &\equiv 27 \ (mod\ 143) \\
138^{103} &\equiv 18 \ (mod\ 143) \\
64^{103} &\equiv 25 \ (mod\ 143) \\
94^{103} &\equiv 29 \ (mod\ 143) \\
106^{103} &\equiv 24 \ (mod\ 143) \\
3^{103} &\equiv 16 \ (mod\ 143) \\
10^{103} &\equiv 3 \ (mod\ 143) \\
10^{103} &\equiv 10 \ (mod\ 143) \\
115^{103} &\equiv 15 \ (mod\ 143) \\
44^{103} &\equiv 99 \ (mod\ 143) \\
63^{103} &\equiv 28 \ (mod\ 143)
\end{aligned}$$

Portanto:

$$13 \ - \ 27 \ - \ 18 \ - \ 25 \ - \ 29 \ - \ 24 \ - \ 16 \ - \ 27$$

$$10 \ - \ 15 \ - \ 18 \ - \ 10 \ - \ 99 \ - \ 27 \ - \ 28 - 10$$

que correspondem a mensagem original.

Teorema 18. *Sejam p e q números primos distintos tal que $n = pq$. Considere um sistema RSA com parâmetros (n, e) para a codificação e (n, d) para a decodificação. Para qualquer inteiro positivo b tal que $b < n$, a operação de decodificação $D(C(b))$ é congruente a b módulo n, ou seja, $D(C(b)) \equiv b \pmod{n}$.*

Demonstração. Seja b um inteiro positivo tal que $b < n$, ou seja, $1 \leq b \leq n - 1$. Pelo algoritmo RSA, a operação de codificação é definida por $C(b) \equiv b^e \pmod{n}$, em que e é a chave pública e, a operação de decodificação é definida por:

$$D(C(b)) \equiv (b^e)^d \equiv b^{ed} \pmod{n} \tag{1}$$

em que d é a chave privada. Novamente por definição do algoritmo RSA, como d é o inverso de e módulo $\varphi(n)$, segue que $de \equiv 1 \pmod{\varphi(n)}$, isto é, $de - 1 = k\varphi(n) \Leftrightarrow de = k\varphi(n) + 1 = k(p-1)(q-1) + 1$, $k \in \mathbb{Z}$. Voltando a (1), temos:

$$b^{k\varphi(n)+1} \equiv b^{\varphi(n)k} \cdot b \pmod{n}$$

Agora, observe o seguinte:

Se $p \nmid b$, como p é primo segue pelo Teorema de Fermat que $b^{\varphi(p)} = b^{p-1} \equiv 1 \ (mod \ p)$. Logo, $(b^{p-1})^{k(q-1)} \equiv 1 \ (mod \ p)$ e, portanto, $b^{k(p-1)(q-1)}b \equiv b \ (mod \ p)$. Por outro lado, se $p \mid b$, então $b \equiv 0 \ (mod \ p)$. Daí, $b^{k(p-1)(q-1)+1} \equiv 0 \equiv b \ (mod \ p)$. Portanto, a congruência $b^{k(p-1)(q-1)+1} \equiv b \ (mod \ p)$ vale para qualquer valor de b.

Analogamente, temos que $b^{k(p-1)(q-1)+1} \equiv b \ (mod \ q)$. Daí, pela Proposição 28 temos $b^{k(p-1)(q-1)+1} = b^{k\varphi(n)+1} = b^{ed} \equiv b \ (mod \ n)$, em que $n = mmc(p, q) = pq$. Portanto, dado um sistema RSA sempre obtemos o bloco original após a codificação e a subsequente decodificação.

□

Observação 14. *Note que não podemos usar o Teorema de Euler pois nem sempre podemos afirmar que $mdc(b, n) = 1$, isto é, que $b^{\varphi(n)} \equiv 1 \pmod{n}$.*

Já a nossa confiança no sistema RSA repousa na quantidade de tempo esperada em que um computador leva para se fatorar o produto de dois números primos grandes, como podemos ver na imagem abaixo (Disponível em (PROBLEM, 2012)).

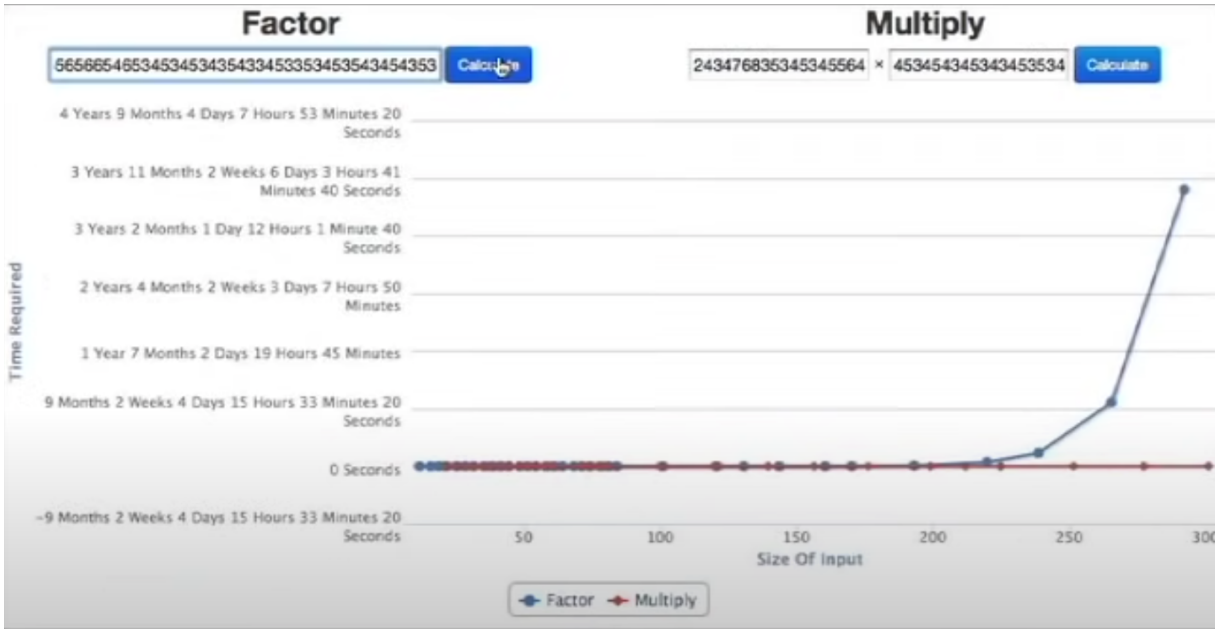


Figura 6: Tempo de Fatoração

Outro fator a ser considerado na segurança do sistema é a escolha dos primos p e q. Suponha que desejamos implementar o RSA com a chave pública (n, e) de modo que n seja um inteiro com aproximadamente r algarismos. Para construir n, escolha o primo p entre $\frac{4r}{10}$ e $\frac{45r}{100}$ algarismos, em seguida, escolha q próximo de $\frac{10^r}{p}$. O tamanho da chave recomendado atualmente para uso pessoal é de 768 bits (o que pode mudar). Isso significa que n terá aproximadamente 231 algarismos e que os primos p e q terão 104 e 127 algarismos, respectivamente, mais detalhes podem ser visto em ((COUTINHO, 1997), seção 5, capítulo 11).

Exemplo 34. ***Algoritmo do Funcionamento do RSA***

Vamos imaginar que queremos enviar uma mensagem usando um programa que simula parte do processo do algoritmo RSA. Para isso, o programa precisa seguir alguns passos simples:

1. *Leitura do Texto: Primeiramente, o programa deve ler o texto que desejamos cifrar, levando em consideração uma tabela de conversão específica (ver páginas 49 e 50 para referência).*

2. *Pré-decodificação: Após a leitura, é necessário realizar uma pré-decodificação do texto para prepará-lo para o próximo passo.*

3. *Aplicação do Algoritmo RSA: Em seguida, o programa realiza uma simulação do algoritmo RSA, aplicando os conceitos de criptografia para proteger a mensagem.*

4. *Retorno à Forma Original: Por fim, o programa reverte o processo, retornando a mensagem à sua forma original. Isso significa desfazer a pré-decodificação e restaurar o texto cifrado à sua versão original.*

Para acessar o código, consultar (MAURICIO, 2023) (Programa realizado em python).

Observação 15. *Pacotes usados para geração do programa: pandas, sympy e random. Também é preciso criar uma tabela de conversão para ser feita a leitura das letras e seus números correspondentes.*

3.2 Assinatura Digital

A assinatura digital nada mais é que uma maneira de assegurar de que a mensagem originada em uma determinada parte seja realmente deferida pela própria, haja vista que no sistema que estamos usando (RSA) os dados de codificação de qualquer instituição são públicos. Isso significa que qualquer pessoa pode enviar uma mensagem criptografada a ela. Por isso, precisamos de uma garantia adicional de segurança, é aí que a assinatura digital entra em cena. Vejamos seu funcionamento.

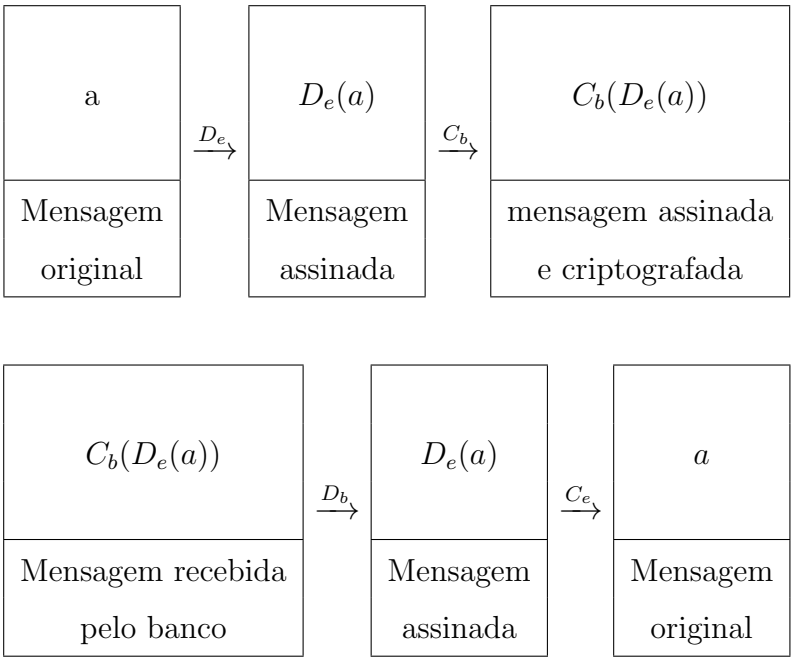
Suponha que somos uma empresa e desejamos encaminhar uma mensagem a um banco, para isso considere o seguinte: as funções de codificação e decodificação da empresa (C_e e D_e) e as funções correspondentes do banco (C_b e D_b) e seja a um bloco da mensagem que a empresa deseja enviar ao banco.

No entanto, para enviar a mensagem assinada, a empresa faz algo um pouco diferente. Em vez de enviar $C_b(a)$, eles enviam $C_b(D_e(a))$. Em outras palavras, primeiro aplicam a função de decodificação da empresa a a e, em seguida, codificam o resultado usando a função de codificação do banco.

Quando o banco recebe o bloco $C_b(D_e(a))$, ele aplica sua função de decodificação para obter $D_e(a)$. Em seguida, ele aplica a função C_e de codificação da empresa a esse bloco para recuperar a, que é o bloco original da mensagem. Note que a função C_e é pública, ou seja, conhecida por todos.

Agora, por que isso é suficiente para garantir ao banco que a mensagem tem origem autorizada? O banco aplica a sequência de funções C_eD_b aos blocos da mensagem recebida. Se a mensagem resultante fizer sentido, isso significa que a mensagem original foi codificada aplicando as funções C_bD_e aos seus blocos. No entanto, observe que a função D_e é conhecida apenas pela empresa. Portanto, se a mensagem fizer sentido, deve ter origem na empresa. Garantindo assim que a mensagem é legítima e originou-se de uma empresa autorizada.

Em resumo, temos:



Exemplo 35. *Digamos que Lucas deseja enviar uma mensagem para Julia contendo a seguinte mensagem: te escondem um segredo. Para isto, Lucas decide enviar tal mensagem utilizando a criptografia RSA. Conhecendo suas respectivas chaves públicas e privadas* (n_l, e_l), (n_l, d_l), (n_j, e_j) *e* (n_j, d_j) *tais que*

$$\begin{array}{ccc} p_l = 131 & & p_j = 109 \\ q_l = 191 & & q_j = 193 \\ n_l = 25021 & & n_j = 21037 \\ \varphi(n_l) = 24700 & e & \varphi(n_j) = 20736 \\ e_l = 3 & & e_j = 5 \\ d_l = 16467 & & d_j = 16589 \end{array}$$

Verifiquemos os passos deste envio.

Primeiro, da tabela de conversão, temos:

29149914281224231314229930229928141627141324

Como $n_l = 22999$*, então a mensagem pode ser particionada da seguinte forma:*

$2914 - 9914 - 2812 - 2423 - 1314 - 2299 - 3022 - 9928 - 1416 - 2714 - 1324$

Assinando a mensagem e utilizando a chave pública (n_j, e_j) *de Julia, temos:*

$$2914^{16467} \equiv 12906 \pmod{25021} \qquad 12906^5 \equiv 16773 \pmod{21037}$$
$$9914^{16467} \equiv 14471 \pmod{25021} \qquad 14471^5 \equiv 12486 \pmod{21037}$$
$$2812^{16467} \equiv 10140 \pmod{25021} \qquad 10140^5 \equiv 8200 \pmod{21037}$$
$$2423^{16467} \equiv 13476 \pmod{25021} \qquad 13476^5 \equiv 1794 \pmod{21037}$$
$$1314^{16467} \equiv 19553 \pmod{25021} \qquad 19553^5 \equiv 1649 \pmod{21037}$$
$$2299^{16467} \equiv 17332 \pmod{25021} \qquad 17332^5 \equiv 982 \pmod{21037}$$
$$3022^{16467} \equiv 3557 \pmod{25021} \qquad 3557^5 \equiv 18144 \pmod{21037}$$
$$9928^{16467} \equiv 738 \pmod{25021} \qquad 738^5 \equiv 17234 \pmod{21037}$$
$$1416^{16467} \equiv 1036 \pmod{25021} \qquad 1036^5 \equiv 310 \pmod{21037}$$
$$2714^{16467} \equiv 16746 \pmod{25021} \qquad 16746^5 \equiv 13457 \pmod{21037}$$
$$1324^{16467} \equiv 15881 \pmod{25021} \qquad 15881^5 \equiv 17189 \pmod{21037}$$

Logo a mensagem recebida por Julia, contém os seguintes blocos: $16773 - 12486 - 8200 - 1794 - 1649 - 982 - 18144 - 17234 - 310 - 13457 - 17189$*. Julia ao receber esta mensagem, aplica respectivamente sua chave privada e a chave pública de Lucas, para descobrir a mensagem. Assim:*

$$16773^{16589} \equiv 12906 \pmod{21037} \qquad 12906^3 \equiv 2914 \pmod{25021}$$
$$12486^{16589} \equiv 14471 \pmod{21037} \qquad 14471^3 \equiv 9914 \pmod{25021}$$
$$8200^{16589} \equiv 10140 \pmod{21037} \qquad 10140^3 \equiv 2812 \pmod{25021}$$
$$1794^{16589} \equiv 13476 \pmod{21037} \qquad 13476^3 \equiv 2423 \pmod{25021}$$
$$1649^{16589} \equiv 19553 \pmod{21037} \qquad 19553^3 \equiv 1314 \pmod{25021}$$
$$982^{16589} \equiv 17332 \pmod{21037} \qquad 17332^3 \equiv 2299 \pmod{25021}$$
$$18144^{16589} \equiv 3557 \pmod{21037} \qquad 3557^3 \equiv 3022 \pmod{25021}$$
$$17234^{16589} \equiv 738 \pmod{21037} \qquad 738^3 \equiv 9928 \pmod{25021}$$
$$310^{16589} \equiv 1036 \pmod{21037} \qquad 1036^3 \equiv 1416 \pmod{25021}$$
$$13457^{16589} \equiv 16746 \pmod{21037} \qquad 16746^3 \equiv 2714 \pmod{25021}$$
$$17189^{16589} \equiv 15881 \pmod{21037} \qquad 15881^3 \equiv 1324 \pmod{25021}$$

Portanto, ao utilizar a assinatura digital, Julia teve certeza que o remetente desta mensagem foi o Lucas. Desta maneira só resta descobrir o que lhe escondem...

Observação 16. *Note que o receptor da mensagem precisa que o produto de fatores primos n seja maior que os blocos criptografados, pois caso contrário o receptor não conseguirá obter a mensagem proposta.*

3.3 Conclusão

Concluímos que o sistema de criptografia RSA necessita de algumas escolhas e a principal vantagem deste procedimento é que a criptografia de uma mensagem não requer o conhecimento dos dois primos p e q, mas apenas de seu produto n. Portanto, não há necessidade de que ninguém, exceto o destinatário da mensagem, saiba os fatores primos que são necessários para o processo de descriptografia.

Fatorar é computacionalmente mais difícil do que distinguir entre números primos e compostos. Com tempo de computação ilimitado e algum algoritmo de fatoração incrivelmente eficiente, o criptossistema RSA poderia ser quebrado, haja vista que toda tentativa de se quebrar o algoritmo, se baseia na fatoração do número n ou de achar os blocos pré codificados a partir da forma reduzida de b^e módulo n, em que ninguém conseguiu desenvolver tal método, mais detalhes podem ser visto em ((COUTINHO, 1997), seção 4, capítulo 11).

A escolha criteriosa dos números primos p e q emerge como um elemento crucial da segurança do sistema RSA. A complexidade do algoritmo reside, em grande medida, na dificuldade associada à fatoração do produto destes primos, tornando a seleção estratégica desses números uma consideração de máxima importância. O procedimento delineado para construir n adiciona uma camada adicional de rigor ao processo, fornecendo diretrizes claras para a escolha de p e q, otimizando assim a robustez do sistema.

Como podemos observar, esse método de criptografia desempenha um papel crucial na garantia da segurança da transmissão de dados. Enquanto pudermos transmitir informações de maneira segura usando a criptografia RSA, essa técnica continuará sendo uma parte essencial do cenário tecnológico. Afinal, sua capacidade de proteger nossas comunicações e informações confidenciais é fundamental para garantir a privacidade e a integridade dos dados na era digital.

Referências

BRESSOUD, D. M. et al. *A course in computational number theory*. [S.l.]: Key College/Springer, 2000.

BURTON, D. *EBOOK: Elementary Number Theory*. [S.l.]: McGraw Hill, 2010.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. [S.l.]: IMPA, 1997.

HEFEZ, A. Aritmética. *Coleção PROFMAT. Sociedade Brasileira de*, 2016.

IEZZI, G.; DOMINGUES, H. *Álgebra moderna: teoría y problemas*. [S.l.]: Saraiva Educação SA, 1970.

MAURICIO, L. O. A. *Algoritmo RSA*. 2023. Disponível em: ⟨https://drive.google.com/drive/folders/1QuDVXpaY4gyKXgeV7JRhFpBfxrs3uh8P?usp=sharing⟩.

OLIVEIRA, C. Congruência modular e aplicações. 2017.

PAGLIUSI, P. S. *Introdução de Mecanismos de Segurança em Sistemas de Correio Eletrônico*. Tese (Doutorado) — Dissertação de Mestrado em Ciência da Computação, Instituto de de Computação . . . , 1998.

POR que a descoberta do maior número primo importa? Online. Disponível em: ⟨Acessadoem16/08/2023,\url{https://impa.br/noticias/por-que-a-descoberta-do-maior-numero-primo-importa}.⟩

PROBLEM, A. of the. *Public Key Cryptography: RSA Encryption Algorithm*. 2012. Disponível em: ⟨https://www.youtube.com/watch?v=wXB-V_Keiu8⟩.

REZENDE, W. M.; DASSIE, B. A. Epistemologia dos números relativos: uma reflexão necessária e atual para a sala de aula de matemática. *Boletim GEPEM*, n. 57, 2010.

SANTOS, J. P. de O. *Introdução à teoria dos números*. [S.l.]: Instituto de Matemática Pura e Aplicada, 1998.

SINGH, S. *O livro dos códigos*. [S.l.]: Editora Record, 2004.

SOUZA, B. A. d. Teoria dos numeros e o rsa. 2004.

SPINA, A. V. *Números primos e criptografia*. Tese (Doutorado) — [sn], 2014.