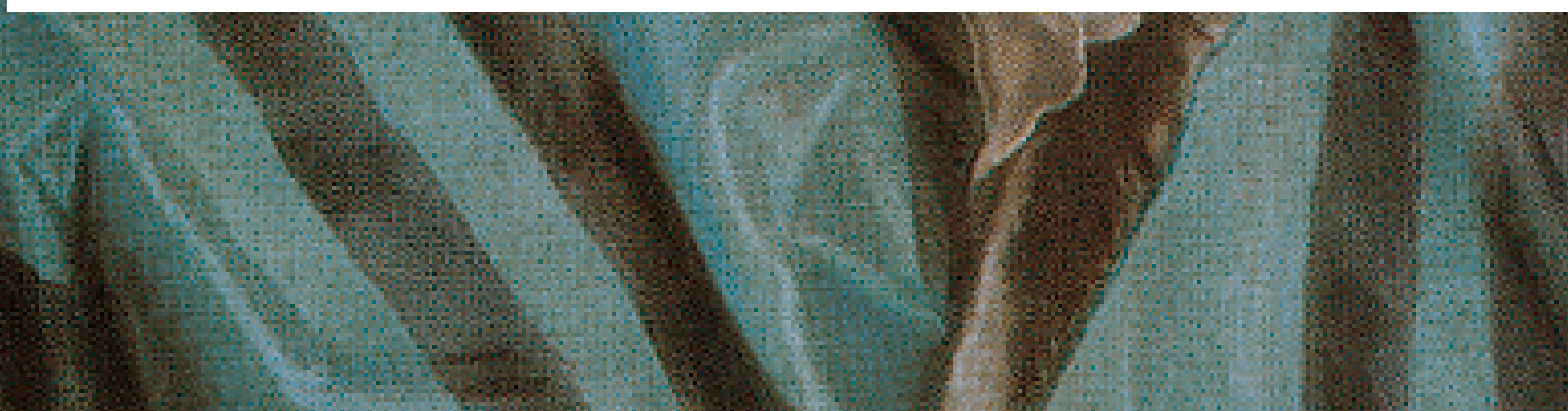
Teoria dos Números 1

Notas de aula transcritas por Caio Tomás de Paula

Prof. Dr. Hemar Teixeira Godinho



Conteúdo

1 Introdução 1

2 Divisibilidade e o Algoritmo de Euclides 1

3 Máximo Divisor Comum (MDC) 2

4 Algoritmo de Euclides para o MDC 4

5 Equação diofantina linear em duas variáveis 5

6 Indução Matemática 7

7 Números primos 9

8 Fundamental da Aritmética 11

9 Mínimo Múltiplo Comum (MMC) 12

10 Bases numéricas 16

11 Critérios de divisibilidade 16

12 Exercícios Resolvidos 17

13 Números de Fermat 21

14 Primos de Mersenne e Números Perfeitos 22

15 Congruência módulo m 25

16 Equação de Congruência 30

17 Exercícios Resolvidos 47

18 Propriedades de polinômios módulo m 52

19 Raízes Primitivas 56

20 Resíduos Quadráticos 70

21 Observação Geral 77

1 Introdução

Esse documento é uma coletânea, em PDF, das notas de aulas ministradas pelo professor Hemar Godinho (UnB), durante o curso de Teoria dos Números 1, ministrado no semestre letivo de 2020/1.

2 Divisibilidade e o Algoritmo de Euclides

No decorrer desse documento, denotaremos:

- os números naturais por $\mathbb{N} = \{1, 2, \dots\}$;
- os números inteiros por $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;
- os números racionais por $\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}$;
- os números primos por $\mathbb{P}$.

Definição. Sejam $a, b \in \mathbb{Z}$. Dizemos que a *divide* b se existe $c \in \mathbb{Z}$ tal que $b = ac$ e escrevemos $a|b$. Do contrário, $a \nmid b$ (a não divide b).

Exemplo. $5|10$, pois $10 = 5 \cdot 2$, mas $3 \nmid 10$, pois $\nexists c \in \mathbb{Z}$ tal que $10 = 3c$.

Definição. Se $a|b$, dizemos que b é um *múltiplo* de a.

Lema 2.1. Sejam $a, b, c \in \mathbb{Z}$. Se $a|b$ e $b|c$, então $a|c$.

Demonstração. Se $a|b$, então $b = ak_1, k_1 \in \mathbb{Z}$. Além disso, se $b|c$, então $c = bk_2, k_2 \in \mathbb{Z}$. Portanto, $c = a(k_1k_2) = ak_3,\ k_3 = k_1k_2 \in \mathbb{Z}$. Logo, $a|c$. □

Lema 2.2. Sejam $a, b, c \in \mathbb{Z}$. Se $a|b$ e $a|c$, então $a|\lambda b + \mu c$, para quaisquer $\lambda, \mu \in \mathbb{Z}$.

Demonstração. Por hipótese, sabemos que $b = ak_1$ e $c = ak_2$. Daí, quaisquer que sejam $\lambda, \mu \in \mathbb{Z}$, sabemos que $\lambda b + \mu c = \lambda ak_1 + \mu ak_2 = a(\lambda k_1 + \mu k_2) = ak_3$. Logo, $a|\lambda b + \mu c$. □

Exemplo. $5|10$ e $5|15 \Rightarrow 5|2 \cdot 10 - 15$.

Princípio da Boa Ordenação (PBO): todo conjunto de inteiros limitado inferiormente tem um menor elemento.

Teorema 2.3 (Teorema de Euclides)**.** Sejam $a, b \in \mathbb{N}$ quaisquer. Então, existe um único par $q, r \in \mathbb{Z}$ tal que

$$a = bq + r, \qquad 0 \leq r < b$$

Demonstração. (Existência) Se $a < b$, tome $q = 0$ e $r = a < b$. Se $a = b$, tome $q = 1$ e $r = 0$.

Suponha, então, $a > b$ e considere

$$M = \{a - bx \mid x \in \mathbb{Z}\}.$$

Observe que

$$M = \{\ldots, a - 2b, a - b, a, a + b, a + 2b, \ldots\}.$$

Seja

$$M_+ = \{m \in M \mid m \geq 0\} \subseteq \mathbb{N} \cup \{0\}$$

Pelo PBO, existe $r \in M_+$ tal que $r \leq m, \forall m \in M_+$. Como $r \in M_+ \subset M$, existe $q \in \mathbb{Z}$ tal que $a - bq = r$, ou seja, $a = bq + r, r \geq 0$. Falta mostrar que $r < b$. Suponha $r \geq b$. Então, $r - b \geq 0$, i.e., $a - b(q + 1) \geq 0$. Logo, $r^* = r - b \in M_+$ e $r^* < r$, o que é absurdo pois r é o menor elemento de M_+. Portanto, $0 \leq r < b$.

(Unicidade) Suponha que $a = bq^* + r^*$, com $q^*, r^* \in \mathbb{Z}$ e $0 \leq r^* < b$. Se $r = r^*$, temos

$$a = bq + r = bq^* + r^* \Rightarrow b(q - q^*) = r - r^* = 0 \Rightarrow q = q^*$$

Suponha $r \neq r^*$ e, sem perda de generalidade, tome $r < r^*$. Temos $0 \leq r < r^* < b$. Segue que $0 \leq r^* - r < b$ e, como $b(q - q^*) = r^* - r$, temos $0 \leq b(q - q^*) < b$. Mas $b \in \mathbb{N}$ e $q - q^* \in \mathbb{Z}_+$. Logo, temos que é absurdo pois $r < r^*$.

Portanto, $q, r \in \mathbb{Z}$ são únicos. □

3 Máximo Divisor Comum (MDC)

Definição. Sejam $a, b \in \mathbb{Z}$. Dizemos que $d \in \mathbb{N}$ é o *máximo divisor comum* entre a e b se:

1. $d|a$ e $d|b$
2. se $d^*|a$ e $d^*|b$, então $d^* \leq d$

Denotamos $d = \text{mdc}(a, b)$.

Exemplo. Vamos calcular o $\text{mdc}(18, 14)$. Os divisores positivos de 18 e 14 são:

$$18 : 1, 2, 3, 6, 9, 18$$

$$14 : 1, 2, 7, 14$$

Logo, $\text{mdc}(18, 14) = 2$.

Lema 3.1. Sejam $a, b \in \mathbb{Z}^*$, e seja $d = \text{mdc}(a, b)$. Então,

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

Demonstração. Como $d|a$ e $d|b$, temos $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}^*$. Seja $d^* = \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right)$. Logo, $\frac{a}{d} = \lambda_1 d^*$ e $\frac{b}{d} = \lambda_2 d^*$, ou seja, $a = \lambda_1 d d^*$ e $b = \lambda_2 d d^*$, $\lambda_1, \lambda_2 \in \mathbb{Z}$. Portanto, $dd^*|a$ e $dd^*|b$. Como $d = \text{mdc}(a, b)$ e $d^* \in \mathbb{N}$, segue que $dd^* \leq d \Rightarrow d^* = 1$. □

Definição. Se $\text{mdc}(a, b) = 1$, dizemos que a e b são *coprimos* ou *primos entre si*.

Observação 3.1. Sejam $a, b \in \mathbb{Z}^*$. Note que $\text{mdc}(a, b) = \text{mdc}(-a, b) = \text{mdc}(a, -b) = \text{mdc}(-a, -b)$.

Lema 3.2. Sejam $a, b \in \mathbb{Z}^*$ e $d = \text{mdc}(a, b)$. Então, existem inteiros r, s tais que $d = ra + sb$.

Demonstração. Pela Observação (3.1), podemos tomar $a, b \in \mathbb{N}$. Seja

$$M = \{ax + by \mid x, y \in \mathbb{Z}\} = \{\ldots, -2a - 2b, -2a - b, -a - 2b, -a - b, -a, -b, 0, a, b, \ldots\}.$$

Seja

$$P = \{m \in M \mid m \geq 1\} \subseteq \mathbb{N}$$

. Pelo PBO, P tem um menor elemento d^* e, como $P \subset M$, segue que $d^* = ra + sb$ para algum par $r, s \in \mathbb{Z}$. Vamos mostrar que $d^*|a$ e $d^*|b$. Pelo Algoritmo de Euclides, segue que $a = d^*q + r, 0 \leq r < d^*$. Daí, $r = a - d^*q = a - q(ra + sb) = a(1 - qr) + b(-qs)$, ou seja, $r \in M$ e $r \geq 0$. Se $r = 0$, $d^*|a$. Se $r \geq 1$, então $r \in P$ e $r < d^*$, o que é absurdo pois d^* é o menor elemento de P. Portanto, $r = 0$ e $d^*|a$.

Também pelo Algoritmo de Euclides, temos $b = q_0 d^* + r_0, 0 \leq r_0 < d^*$. Analogamente ao que foi feito acima, concluímos que $d^*|b$. Falta mostrar que $d^* = d$. Como $d^*|a$ e $d^*|b$, temos, por definição, $d^* \leq d$. Por outro lado, como $d|a$ e $d|b$, segue do Lema (2.2) que $d|ra + sb = d^*$, ou seja, $d \leq d^*$. Como $d, d^* \in \mathbb{N}$, segue que $d = d^*$. □

Vale observar que, além de demonstrar que $\text{mdc}(a, b)$ pode ser escrito como combinação linear de a e b, mostramos que o mdc é, na verdade, a *menor* dessas combinações.

Corolário 3.2.1. Seja $d = \text{mdc}(a, b)$. Se $d_0|a$ e $d_0|b$, então $d_0|d$.

Demonstração. Pelo Lema (3.2), $\exists r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Como $d_0|a$ e $d_0|b$, segue do Lema (2.2) que $d_0|ra + sb$, i.e., $d_0|d$. □

Lema 3.3. Se $a|bc$ e $\text{mdc}(a, b) = 1$, então $a|c$.

Demonstração. Sabemos que existem $r, s \in \mathbb{Z}$ tais que $1 = ra+sb$ (Lema (3.2)). Também sabemos que $bc = at, t \in \mathbb{Z}$. Daí,

$$c = c \cdot 1 = c(ra + sb) = acr + bcs = acr + ast = (cr + st)a \quad \therefore \quad a|c$$

□

Lema 3.4. Sejam $a, b \in \mathbb{N}$ e tome $a = bq + r, 0 \leq r < b$. Então, $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Demonstração. Sejam $d = \text{mdc}(a, b)$ e $d^* = \text{mdc}(b, r)$. Pelo Lema (2.2), segue que $d|r$, pois $r = a - bq$ e $d|a$ e $d|b$. Logo, como $d|b$ e $d|r$, segue do Corolário que $d|d^*$.

Por outro lado, sabemos que $d^*|b$ e $d^*|r$. Pelo Lema (2.2), $d^*|bq + r = a$ e, pelo Corolário, $d^*|d$. Como $d, d^* \in \mathbb{N}$, segue que $d = d^*$. □

4 Algoritmo de Euclides para o MDC

Sejam $a, b \in \mathbb{N}$. Pelo Algoritmo de Euclides, temos

$$\begin{aligned}
a &= bq + r, && 0 \leq r < b \\
b &= rq_1 + r_1, && 0 \leq r_1 < r < b \\
r &= r_1q_2 + r_2, && 0 \leq r_2 < r_1 < r < b \\
r_1 &= r_2q_3 + r_3, && 0 \leq r_3 < r_2 < r_1 < r < b \\
&\vdots
\end{aligned}$$

Como há b inteiros entre 0 e b, esse algoritmo tem, no máximo, b passos, i.e., para algum $n > b$ teremos

$$\begin{aligned}
&\vdots \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2} < \cdots < b \\
r_{n-2} &= r_{n-1}q_n + r_n, \quad r_n = 0
\end{aligned}$$

Logo, $r_{n-1}|r_{n-2}$, ou seja, $\text{mdc}(r_{n-1}, r_{n-2}) = r_{n-1}$, pois $r_{n-1} < r_{n-2}$. Pelo Lema (3.4), segue que

$$\text{mdc}(a, b) = \text{mdc}(b, r) = \text{mdc}(r, r_1) = \cdots = \text{mdc}(r_{n-2}, r_{n-1}) = r_{n-1},$$

ou seja, $\text{mdc}(a, b) = r_{n-1}$.

Exemplo. Calcule $\text{mdc}(153, 27)$. Temos

$$\begin{aligned}
153 &= 27 \cdot 5 + 18 \\
27 &= 18 \cdot 1 + 9 \\
18 &= 9 \cdot 2,
\end{aligned}$$

logo $\text{mdc}(153, 27) = 9$.

Exemplo. Calcule $\text{mdc}(190, 136)$ e determine $r, s \in \mathbb{Z}$ tais que $\text{mdc}(190, 136) = 190r + 136s$. Temos

$$\begin{aligned} 190 &= 136 \cdot 1 + 54 \\ 136 &= 54 \cdot 2 + 28 \\ 54 &= 28 \cdot 1 + 26 \\ 28 &= 26 \cdot 1 + 2 \\ 26 &= 2 \cdot 13, \end{aligned}$$

logo $\text{mdc}(190, 136) = 2$. Reescrevendo os restos, temos

$$\begin{aligned} 54 &= 190 - 136 \\ 28 &= 136 - 2 \cdot 54 = 136 - 2(190 - 136) = 3 \cdot 136 - 2 \cdot 190 \\ 26 &= 54 - 28 = (190 - 136) - (3 \cdot 136 - 2 \cdot 190) = -4 \cdot 136 + 3 \cdot 190 \\ 2 &= 28 - 26 = (3 \cdot 136 - 2 \cdot 190) - (-4 \cdot 136 + 3 \cdot 190) = 190 \cdot (-5) + 136 \cdot (7) \end{aligned}$$

5 Equação diofantina linear em duas variáveis

Sejam $a, b, c \in \mathbb{Z}$ e considere a equação

$$ax + by = c.$$

Queremos determinar todas as soluções inteiras dessa equação.

Lema 5.1. A equação $ax + by = c$ tem solução inteira se, e somente se, $\text{mdc}(a, b)|c$.

Demonstração. Suponha que $x_0, y_0 \in \mathbb{Z}$ é solução de $ax + by = c$, ou seja, $ax_0 + by_0 = c$. Seja $d = \text{mdc}(a, b)$. Então, como $d|a$ e $d|b$, pelo Lema (2.2), $d|c$. Reciprocamente, suponha que $d|c$. Então, $c = \lambda d, \lambda \in \mathbb{Z}$. Pelo Lema (3.2), existem $r, s \in \mathbb{Z}$ tais que $d = ar + bs$, logo $c = \lambda d = a(\lambda r) + b(\lambda s)$, ou seja, tomando $x_0 = \lambda r$ e $y_0 = \lambda s$ temos que x_0, y_0 é solução de $ax + by = c$. □

Lema 5.2. Suponha que $x_0, y_0 \in \mathbb{Z}$ seja solução de $ax + by = c$. Então

$$x_t = x_0 + \frac{b}{d}t \quad \text{e} \quad y_t = y_0 - \frac{a}{d}t, \quad d = \text{mdc}(a, b)$$

é também solução de $ax + by = c$, $\forall t \in \mathbb{Z}$. Além disso, todas as soluções de $ax + by = c$ são obtidas dessa forma (i.e., se $x^*, y^* \in \mathbb{Z}$ é solução de $ax + by = c$, então existe $t \in \mathbb{Z}$ tal que $x^* = x_t$ e $y^* = y_t$).

Demonstração. Primeiro, vamos mostrar que $\forall t \in \mathbb{Z}$, x_t, y_t é solução de $ax + by = c$. Note que

$$\begin{aligned} ax_t + by_t &= ax_0 + by_0 + \frac{ab}{d}t - \frac{ba}{d}t \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

Portanto, x_y, y_t é solução.

Suponha, agora, que x^*, y^* é solução de $ax + by = c$. Então,

$$ax^* + by^* = c = ax_0 + by_0 \Rightarrow a(x^* - x_0) = b(y_0 - y^*).$$

Como $d|a$ e $d|b$, segue que

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

Pelos Lemas (3.1) e (3.3), temos

$$\begin{aligned} \frac{a}{d}\Big|(y_0 - y^*) \quad \text{e } \frac{b}{d}\Big|(x^* - x_0), \quad \text{pois mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \\ \Rightarrow y_0 - y^* = t\frac{a}{d} \quad \text{e } x^* - x_0 = k\frac{b}{d}, \quad t, k \in \mathbb{Z}. \end{aligned}$$

Agora,

$$\begin{aligned} & c = ax^* + by^* = a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}t\right) \\ \Leftrightarrow\ & c = ax^* + by^* = ax_0 + by_0 + \frac{ab}{d}(k - t) \\ \Leftrightarrow\ & c = c + \frac{ab}{d}(k - t) \\ \Leftrightarrow\ & \frac{ab}{d}(k - t) = 0 \underset{a,b\in\mathbb{N}}{\Rightarrow} k = t. \end{aligned}$$

Portanto, $x^* = x_0 + \frac{b}{d}t$ e $y^* = y_0 - \frac{a}{d}t$. □

Corolário 5.2.1. Sejam $a, b \in \mathbb{Z}$. Se $\text{mdc}(a, b) = 1$, então $ax + by = c$ tem infinitas soluções inteiras, independentemente do valor de c.

Demonstração. Do Lema (5.1), segue que essa equação sempre tem solução pois $\text{mdc}(a, b) = 1$ e $1|c$, para todo $c \in \mathbb{Z}$. Pelo Lema (5.2), segue que há infinitas soluções. □

Exemplo. Encontre todas as soluções de $3x + 5y = 14$.

Como $\text{mdc}(3, 5) = 1$ e $1|14$, existem infinitas soluções. Note que $1 = 3 \cdot 2 - 1 \cdot 5$, logo $14 = 3(2 \cdot 14) + 5(-1 \cdot 14)$. Portanto, $(x_0, y_0) = (28, -14)$ é solução, e as demais são

$$\begin{cases} x_t = 28 + 5t \\ y_t = -14 - 3t \end{cases}, t \in \mathbb{Z}.$$

Observação 5.1. O exemplo acima ilustra que basta conhecer $r, s \in \mathbb{Z}$ tais que $\text{mdc}(a,b) = ra+sb$ para encontrar uma solução para $ax+by=c$. Se $d = \text{mdc}(a,b)$ e $d|c$, escreva $c = \lambda d = \lambda(ra+sb) = a(\lambda r) + b(\lambda s)$, ou seja,

$$x_0 = \lambda r \quad \text{e } y_0 = \lambda s$$

é solução. É possível obter, do Algoritmo de Euclides para o cálculo do MDC, os valores de r e s. Observe o exemplo a seguir.

Exemplo. Encontre todas as soluções de

$$190x + 136y = 14$$

Num exemplo anterior, descobrimos que $\text{mdc}(190, 136) = 2$. Como $2|14$, há infinitas soluções. Também vimos que

$$2 = 190 \cdot (-5) + 136 \cdot 7,$$

logo

$$14 = 190 \cdot (-35) + 136 \cdot (49),$$

e temos

$$x_0 = -35, \;\; y_0 = 49.$$

Portanto, as soluções são

$$\begin{cases} x_t = -35 + 68t \\ y_t = 49 - 95t \end{cases}, t \in \mathbb{Z}.$$

6 Indução Matemática

Seja $p(n)$ uma proposição lógica que dependa de $n \in \mathcal{N} \subseteq \mathbb{N} \cup \{0\}$.

Exemplo. $p(n)$ = "A soma dos primeiros n números naturais consecutivos é igual a $\frac{n(n+1)}{2}$".

Em linguagem matemática,

$$p(n) = \text{“}1 + 2 + \cdots + n = \frac{n(n+1)}{2}\text{”}$$

Essa é uma proposição lógica que depende de n.

Teorema 6.1 (Indução Matemática)**.** Seja $\mathcal{N} \subseteq \mathbb{N} \cup \{0\}$ e escreva $\mathcal{N} = \{n_0, n_1, \dots\}$ com $n_0 < n_1 < \dots$.

Seja $p(n)$ uma proposição lógica que dependa de $n \in \mathbb{N}$. Se

$$\begin{cases} p(n_0) \text{ é verdadeira} \\ p(n_k) \Longrightarrow p(n_{k+1}) \forall n_k \in \mathcal{N} \end{cases}$$

então $p(n)$ é verdadeira $\forall n \in \mathcal{N}$.

Demonstração. Seja $\mathcal{F} = \{n \in \mathcal{N} \mid p(n) \text{ é falsa}\}$. Queremos mostrar que, sob as hipóteses do teorema, $\mathcal{F} = \varnothing$, i.e., $p(n)$ é verdadeira $\forall n \in \mathcal{N}$. Como $\mathcal{F} \subset \mathcal{N} \subseteq \mathbb{N} \cup \{0\}$, pelo PBO existe $n_r \in \mathcal{F}$ tal que $n_r \leq m, \forall m \in \mathcal{F}$.

Pela primeira hipótese do teorema, $n_r > n_0$ (pois $p(n)$ é verdadeira) e, portanto, $p(n_0), \ldots, p(n_{r-1})$ são verdadeiras.

Pela segunda hipótese, temos $p(n_r)$ verdadeira, o que é absurdo pois $n_r \in \mathcal{F}$. Logo, $\mathcal{F} = \varnothing$. □

Exemplo. Mostre que, $\forall n \in \mathbb{N}$, $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Vamos aplicar indução. Primeiro, note que para $n = 1$, temos $1 = 1$ e $p(1)$ é verdadeira. Suponha que, para $m \in \mathbb{N}$, $p(m)$ é verdadeira, ou seja

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

Daí, segue que

$$\begin{aligned} 1 + 2 + \cdots + m + m + 1 &= \frac{m(m+1)}{2} + m + 1 \\ &= \frac{(m+1)(m+2)}{2} \end{aligned}$$

e $p(m+1)$ é verdadeira. Logo, segue por indução que $p(n)$ é sempre verdadeira.

Observação 6.1. No caso da indução matemática, chamamos a primeira hipótese do teorema de *caso particular* e a afirmação "se $p(n_k)$ é verdadeira" de *hipótese de indução.*

Exemplo. Mostre que, $\forall n \in \mathbb{N}$, temos

$$1 + x + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

Para o caso particular $n = 1$, temos $1 + x = \dfrac{x^2 - 1}{x - 1} = x + 1$.

Suponha, por hipótese de indução, que

$$1 + x + \cdots + x^k = \frac{x^{k+1} - 1}{x - 1}.$$

Considere

$$\begin{aligned} 1 + x + \cdots + x^k + x^{k+1} &= \frac{x^{k+1} - 1}{x - 1} + x^{k+1} \\ &= \frac{x^{k+1} - 1 + x^{k+2} - x^{k+1}}{x - 1} \\ &= \frac{x^{k+2} - 1}{x - 1}. \end{aligned}$$

Logo, $p(k+1)$ também é verdadeira e, por indução, $p(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Exemplo. Mostre que, $\forall n \in \mathbb{N}$, $n^3 + (n+1)^3 + (n+2)^3$ é sempre divisível por 9.

Para o caso particular $n = 1$, temos $1^3 + 2^3 + 3^3 = 36$ e $9|36$.

Suponha, por hipótese de indução, que $9|m^3 + (m+1)^3 + (m+2)^3$. Considere

$$\begin{aligned}(m+1)^3 + (m+2)^3 + (m+3)^3 &= (m+1)^3 + (m+2)^3 + (m^3 + 9m^2 + 27m + 27) \\ &= \left(m^3 + (m+1)^3 + (m+2)^3\right) + 9m^2 + 27m + 27 \\ &= 9M + 9(m^2 + 2m + 3),\end{aligned}$$

que claramente é divisível por 9. Logo, $p(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Exemplo. Mostre que, $\forall n \in \mathbb{N}$,

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

Para o caso particular $n = 1$, temos $1^3 = 1^2$. Suponha, por hipótese de indução, que

$$1^3 + 2^3 + \cdots + k^3 = (1 + 2 + \cdots + k)^2$$

e considere

$$\begin{aligned}1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= (1 + 2 + \cdots + k)^2 + (k+1)^3 \\ &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\ &= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\ &= \frac{(k+1)^2(k^2 + 4k + 4)}{4} \\ &= \left(\frac{(k+1)(k+2)}{2}\right)^2 \\ &= (1 + 2 + \cdots + k + k + 1)^2.\end{aligned}$$

Logo, segue por indução que a proposição vale $\forall n \in \mathbb{N}$.

7 Números primos

Definição. Seja $p \in \mathbb{N}, p \neq 1$. O número p é chamado de *primo* se os únicos divisores positivos de p são 1 e p.

Exemplo. $2, 3, 5, 7, 11, 13, 17, 19, 23$ são primos.

Lema 7.1. Seja p um primo e $a \in \mathbb{Z}$. Se $p \nmid a$, então $\text{mdc}(a, p) = 1$.

Demonstração. Seja $d = \text{mdc}(a, p)$. Logo, $d|p$ e $d|a$. Como p é primo, $d = 1$ ou $d = p$. Se $d = p$, então $p|a$, absurdo. Portanto, $d = 1$. □

Lema 7.2. Sejam p primo e $a, b \in \mathbb{Z}$. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. Suponha que $p \nmid a$. Pelo Lema (7.1), $\text{mdc}(a,p) = 1$. Como $p|ab$, pelo Lema (3.3) temos que $p|b$. □

Lema 7.3. Sejam p, q_1, q_2 primos. Se $p|q_1q_2$, então ou $p = q_1$ ou $p = q_2$.

Demonstração. Pelo Lema (7.2), $p|q_1$ ou $p|q_2$. Suponha, sem perda de generalidade, que $p|q_1$. Como p é primo, $p \neq 1$ e, como q_1 é primo, devemos ter $p = q_1$. □

Lema 7.4. Sejam $p, q_1, \ldots, q_r$ primos. Se $p|q_1q_2\cdots q_r$, então existe $j \in \{1, 2, \ldots, r\}$ tal que $p = q_j$.

Demonstração. Vamos proceder por indução em r. Como caso particular, temos $r = 1$: se $p|q_1$, então $p = q_1$. Suponha, por hipótese de indução, que se $p|q_1q_2\cdots q_k$, então $p|q_j$ para algum $j \in \{1, 2, \ldots, k\}$. Considere

$$\underbrace{q_1\cdots q_k}_{a} \cdot \underbrace{q_{k+1}}_{b} = ab.$$

Pelo Lema (7.2), sabemos que $p|a$ ou $p|b$, i.e., $p|q_1\cdots q_k$ ou $p|q_{k+1}$. Se $p|q_{k+1}$, então $p = q_{k+1}$, pois p e q_{k+1} são primos. Se $p|q_1\cdots q_k$, segue da hipótese de indução que $p|q_j$ para algum $j \in \{1, 2, \ldots, k\}$.

Logo, segue por indução que o lema é verdadeiro. □

Definição. Seja $m \in \mathbb{N}, m \neq 1$. Se m não é primo, m é chamado de *composto*.

Lema 7.5. Sejam p, q primos distintos. Se $p|a$ e $q|a$, então $pq|a$.

Demonstração. Como $p|a$, $a = pM, M \in \mathbb{Z}$. Como $q|a$, segue que $q|pM$. Pelo Lema (7.2), $q|p$ ou $q|M$. Se $q|p$, então $q = p$, absurdo. Portanto, $q|M$, i.e., $M = qR, R \in \mathbb{Z}$. Logo, $a = pqR$, ou seja, $pq|a$. □

O resultado principal dessa seção é o Teorema Fundamental da Aritmética, mas antes de apresentá-lo precisamos de uma outra versão do Teorema de Indução Matemática.

Teorema 7.6 (Indução Matemática – 2ª forma)**.** Seja $\mathcal{N} \subseteq \mathbb{N} \cup \{0\}$ e escreva $\mathcal{N} = \{n_0, n_1, n_2, \ldots\}$ com $n_0 < n_1 < n_2 < \cdots$. Seja $p(n)$ uma proposição lógica que dependa de $n \in \mathcal{N}$. Se

$$\begin{cases} p(n_0) \text{ é verdadeira} \\ p(n_j) \text{ é verdadeira para todo } j < k \text{ então } p(n_k) \text{ é verdadeira} \end{cases}$$

então $p(n)$ é verdadeira $\forall n \in \mathcal{N}$.

Demonstração. A mesma do Teorema de Indução Matemática. □

8 Fundamental da Aritmética

Teorema 8.1 (Teorema Fundamental da Aritmética)**.** Todo número natural maior que 1 pode ser escrito de maneira única (a menos de ordem) como um produto de primos.

Demonstração. (Existência) Vamos proceder por indução sobre n. Para o caso particular $n = 2$, podemos escrever $2 = 2$.

Suponha, por hipótese de indução, que todo $r \in \mathbb{N}, 1 < r < m, m \in \mathbb{N}$, pode ser escrito como produto de primos. Se m é primo, m é produto de um primo.

Suponha m composto e $m = uv, 1 < u, v < m$. Pela hipótese de indução, temos

$$u = p_1 p_2 \cdots p_r \quad \text{e} \quad v = q_1 q_2 \cdots q_s, \text{ logo}$$

$$m = uv = p_1 \cdots p_r q_1 \cdots q_s$$

também é um produto de primos.

(Unicidade) Seja $n \in \mathbb{N}, n > 1$ e suponha que

$$n = p_1 \cdots p_r = q_1 \cdots q_s, r \leq s.$$

Logo, $p_1 | q_1 \cdots q_s$, ou seja, $\exists j \in \{1, 2, \ldots, s\}$ tal que $p_1 = q_j$, pelo Lema (7.4). Reordenando os índices dos q_i's, assuma $p_1 = q_1$. Então,

$$p_1 p_2 \cdots p_r = p_1 q_2 \cdots q_s \Rightarrow p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Continuando esse processo, teremos, eventualmente,

$$p_r = q_r q_{r+1} \cdots q_s, \text{ pois } r \leq s.$$

Como p_r é primo, segue que $r = s$ e $p_r = q_r$. □

Lema 8.2. Sejam $p_1, \ldots, p_r$ primos distintos. Se $p_1^m | p_1^{t_1} \cdots p_r^{t_r}$, com $m, t_1, \ldots, t_r \in \mathbb{N} \cup \{0\}$, então $m \leq t_1$.

Demonstração. Suponha $m > t_1$ e escreva $m = t_1 + s, s \geq 1$. Daí, por hipótese,

$$\lambda p_1^m = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r} \Longrightarrow \lambda p_1^{t_1} p_1^s = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r} \Longrightarrow \lambda p_1^s = p_2^{t_2} \cdots p_r^{t_r}.$$

Contudo, isso contraria o TFA, pois do lado direito temos um número escrito como produto de primos $p_2, p_3, \ldots, p_r$ e, do lado esquerdo, escrito como outro produto de primos, com o fator p_1^s. Isso é absurdo, pois a fatoração é única, logo $m \leq t_1$. □

Lema 8.3. Seja $n = p_1^{r_1} \cdots p_s^{r_s}$, com $p_1, p_2, \ldots, p_r$ primos distintos. Então, $d | n$ se, e somente se, $d = p_1^{l_1} \cdots p_s^{l_s}$, com $0 \leq l_i \leq r_i, i = 1, 2, \ldots, s$.

Demonstração. Se $d|n$, então $\lambda d = p_1^{r_1}\cdots p_s^{r_s}$. Seja q primo tal que $q|d$. Como $d|n$, segue do Lema (2.1) que $q|n$. Pelo Lema (7.4), temos $q \in \{p_1, \ldots, p_s\}$. Assim, devemos ter

$$d = p_1^{l_1}\cdots p_s^{l_s}.$$

Agora, nem todos os primos podem estar na fatoração de n, e podemos ter $l_i = 0$ para algum i; por outro lado, o Lema (8.2) nos diz que $l_i \leq r_i$. Desse modo, $0 \leq l_i \leq r_i, \forall i$.

Reciprocamente, suponha que $d = p_1^{l_1}\cdots p_s^{l_s}$, com $0 \leq l_i \leq r_i, i = 1, 2, \ldots, s$. Como $l_i \leq r_i$, podemos escrever $r_i = l_i + k_i, k_i \in \mathbb{N} \cup \{0\}$. Daí, temos

$$\begin{aligned} n = p_1^{r_1}\cdots p_s^{r_s} &= \left(p_1^{l_1}\cdots p_s^{l_s}\right)\left(p_1^{k_1}\cdots p_s^{k_s}\right) \\ &= d\lambda, \lambda \in \mathbb{Z}. \end{aligned}$$

Logo, $d|n$. □

Lema 8.4. Seja $a \in \mathbb{N}, a \geq 2$ e escreva $a = p_1^{r_1}\cdots p_s^{r_s}$ com $p_1, \ldots, p_s$ primos distintos. O número de divisores positivos de a é $\prod_{i=1}^{s}(r_i + 1)$.

Demonstração. O Lema (8.3) nos diz que d é um divisor positivo de a se, e só se, $d = p_1^{l_1}\cdots p_s^{l_s}$, com $0 \leq l_i \leq r_i$ e $i \leq s$. Portanto, para contar os divisores positivos de a pode ser feita uma correspondência

$$p_1^{l_1}\cdots p_s^{l_s} \leftrightarrow (l_1, \ldots, l_s),$$

ou seja, contar a quantidade de s-uplas. Como $0 \leq l_i \leq r_i$, o total é $\prod_{i=1}^{s}(r_i + 1)$. □

Exemplo. Seja $a = 2\cdot 3\cdot 5^2$. Logo, o número de divisores positivos de a é $(1+1)(1+1)(2+1) = 12$. A saber: $2^0\cdot 3^0\cdot 5^0, 2^1\cdot 3^0\cdot 5^0, 2^0\cdot 3^1\cdot 5^0, 2^0\cdot 3^0\cdot 5^1, 2^1\cdot 3^1\cdot 5^0, 2^1\cdot 3^0\cdot 5^1, 2^0\cdot 3^1\cdot 5^1, 2^0\cdot 3^0\cdot 5^2, 2^1\cdot 3^0\cdot 5^2, 2^0\cdot 3^1\cdot 5^2, 2^1\cdot 3^1\cdot 5^2, 2^1\cdot 3^1\cdot 5^1$.

9 Mínimo Múltiplo Comum (MMC)

Definição. Sejam $a, b \in \mathbb{Z}$ e seja $m \in \mathbb{N}$. Dizemos que m é o *mínimo múltiplo comum* de a e b se

1. $a|m$ e $b|m$
2. se $a|m^*$ e $b|m^*$, então $m \leq m^*$

Denotamos $m = \text{mmc}(a, b)$.

Exemplo. Determine $\text{mmc}(12, 20)$. Note que os múltiplos positivos são

$$12 : 12, 24, 36, 48, 60, 72, 84, \ldots$$

$$20 : 20, 40, 60, 80, \ldots$$

logo $\text{mmc}(12, 20) = 60$.

Lema 9.1. Sejam $a, b \in \mathbb{Z}$ e escreva $a = p_1^{r_1} \cdots p_s^{r_s}$ e $b = p_1^{l_1} \cdots p_s^{l_s}$, com $r_j, l_j \geq 0$ para $j = 1, 2, \ldots, s$ e $p_1 < p_2 < \cdots < p_s$ primos. Defina, para $1 \leq j \leq s$, $v_j = \min\{r_j, l_j\}$ e $u_j = \max\{r_j, l_j\}$, e escreva $d = p_1^{v_1} \cdots p_s^{v_s}$, $m = p_1^{u_1} \cdots p_s^{u_s}$. Então, $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$.

Demonstração. Pelo Lema (8.3), sabemos que $d|a$ e $d|b$, e se $d^*|a$ e $d^*|b$ então $d^* = p_1^{t_1} \cdots p_s^{t_s}$ com $t_j \leq r_j$ e $t_j \leq l_j$, logo $t_j \leq \min\{r_j, t_j\}$, ou seja, $d^*|d$. Logo, $d = \text{mdc}(a, b)$.

Também do Lema (8.3), $a|m$ e $b|m$. Seja m^* um múltiplo comum de a e b, i.e., $a|m^*$ e $b|m^*$. Assim,

$$m^* = a\lambda = p_1^{r_1} \cdots p_s^{r_s} \cdot \lambda \quad \text{e} \quad m^* = b\delta = p_1^{l_1} \cdots p_s^{l_s} \cdot \delta.$$

Em particular, $p_j^{u_j} | m^*$ com $j = 1, 2, \ldots, s$, logo $m|m^*$. Portanto, $m = \text{mmc}(a, b)$. □

Corolário 9.1.1. Seja $m = \text{mmc}(a, b)$. Se $a|m^*$ e $b|m^*$, então $m|m^*$.

Demonstração. Segue da demonstração do Lema (9.1). □

Exemplo. Sejam $a = 200 = 2^3 \cdot 5^2$ e $b = 945 = 3^3 \cdot 5 \cdot 7$. Pelo Lema (9.1), $\text{mdc}(a, b) = 2^0 \cdot 3^0 \cdot 5 \cdot 7^0 = 5$ e $\text{mmc}(a, b) = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7 = 37800$.

Lema 9.2. Sejam $a, b \in \mathbb{N}$. Então $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = ab$.

Demonstração. Escreva $a = \prod_{i=1}^{s} p_i^{r_i}$ e $b = \prod_{i=1}^{s} p_i^{l_i}$, com $p_1 < p_2 < \cdots < p_s$ primos. Pelo Lema (9.1), temos $\text{mdc}(a, b) = \prod_{i=1}^{s} p_i^{\min\{r_i, l_i\}}$ e $\text{mmc}(a, b) = \prod_{i=1}^{s} p_i^{\max\{r_i, l_i\}}$. Observe que $\min\{r_i, l_i\} + \max\{r_i, l_i\} = r_i + l_i$. Logo, $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = \prod_{i=1}^{s} p_i^{l_i + r_i} = ab$. □

Teorema 9.3. O conjunto $\mathbb{P}$ dos números primos é infinito.

Demonstração. Suponha $\mathbb{P}$ finito e escreva

$$\mathbb{P} = \{p_1, p_2, \ldots, p_k\}.$$

Seja $m = p_1 p_2 \cdots p_k + 1$, logo $m \in \mathbb{N}$. Pelo TFA, temos

$$m = q_1 q_2 \cdots q_s, q_i \in \mathbb{P} \text{ para } i = 1, 2, \ldots, s.$$

Após renumeração de índices, assuma $q_1 = p_1$. Logo,

$$m = p_1 q_2 \cdots q_s = p_1 p_2 \cdots p_k + 1 \Rightarrow p_1 q_2 \cdots q_s - p_1 p_2 \cdots p_s = 1 \Rightarrow p_1 (q_2 \cdots q_s - p_2 \cdots p_k) = 1 \Rightarrow p_1 | 1,$$

o que é absurdo pois p_1 é primo. Portanto, $\mathbb{P}$ é infinito. □

Observação 9.1. Seja $k \in \mathbb{N}, k \geq 2$. Como $k! = 1 \cdot 2 \cdots (k-1) \cdot k$, temos que $n|k!$ para todo $1 \leq n \leq k$. Observe que a lista abaixo

$$k! + 1, k! + 2, \ldots, k! + k$$

é uma lista de k naturais consecutivos e, como $k! + j$ é divisível por j se $2 \leq j \leq k$ e $k! + j > j$, compostos. Logo, sempre podemos encontrar intervalos de $\mathbb{N}$, arbitrariamente grandes, que não contêm primos.

Lema 9.4. Todo $n \in \mathbb{N}$ composto tem um fator primo menor ou igual a $\sqrt{n}$.

Demonstração. Como n é composto, $n = p_1 \cdots p_r$ com $p_1 \leq \cdots \leq p_r$ primos e $r \geq 2$. Nesse caso, temos

$$n = p_1 \left(p_2 \cdots p_r\right) \geq p_1^2 \text{ pois } p_1 \leq \cdots \leq p_r,$$

logo $\sqrt{n} \geq p_1$, como queríamos. □

Há resultados muito bonitos sobre primos, cujas demonstrações estão além desse curso. Contudo, vale mencioná-los.

- Euler (1737): seja $\mathbb{P}$ o conjunto dos primos. Então, $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverge;
- Dirichlet (1837): sejam $a, b \in \mathbb{N}$ com $\text{mdc}(a, b) = 1$. Existem infinitos números primos da forma $an + b$, i.e., há infinitos primos na P.A.

$$a + b, 2a + b, 3a + b, \ldots$$

- Teorema dos Números Primos (Hadamard – de la Vallée Poussin — 1896): seja $x \in \mathbb{R}, x > 1$ qualquer e defina $\pi(x)$ como a quantidade de primos menores que x. Daí,

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Observação 9.2. Embora o Teorema de Dirichlet seja difícil de demonstrar, vamos, a seguir, apresentar um caso onde conseguimos provar que existem infinitos primos nessa P.A.

Pelo Algoritmo de Euclides, todo $m \in \mathbb{Z}$ pode ser escrito como $m = qk + r, 0 \leq r < k, k \in \mathbb{N}$ fixo. Logo, podemos dividir $\mathbb{Z}$ em k subconjuntos disjuntos de acordo com o resto na divisão por k:

$$\begin{aligned}
M_0 &= \{kq \mid q \in \mathbb{Z}\} = \{\ldots, -3k, -2k, -k, 0, k, 2k, 3k, \ldots\}, \\
M_1 &= \{kq + 1 \mid q \in \mathbb{Z}\} = \{\ldots, -3k + 1, -2k + 1, -k + 1, 1, k + 1, 2k + 1, 3k + 1, \ldots\}, \\
&\vdots \\
M_{k-1} &= \{kq + (k-1) \mid q \in \mathbb{Z}\} = \{\ldots, -2k + (k-1), -k + (k-1), +(k-1), k + (k-1), \ldots\}.
\end{aligned}$$

Portanto,

$$\mathbb{Z} = \dot{\bigcup_{i=0}^{k-1}} M_i.$$

Exemplo. Se $k = 6$, temos

$$\begin{aligned}
M_0 &= \{6q \mid q \in \mathbb{Z}\} = \{\dots, -18, -12, -6, 0, 6, 12, 18, \dots\}, \\
M_1 &= \{6q + 1 \mid q \in \mathbb{Z}\} = \{\dots, -17, -11, -5, 1, 7, 13, 19, \dots\}, \\
&\vdots \\
M_5 &= \{6q + 5 \mid q \in \mathbb{Z}\} = \{\dots, -13, -7, -1, 5, 11, 17, 23, \dots\}.
\end{aligned}$$

Desse modo,

$$\begin{aligned}
247 = 6 \cdot 41 + 1 &\Longrightarrow 247 \in M_1, \\
5428 = 6 \cdot 904 + 4 &\Longrightarrow 5428 \in M_4, \\
92333 = 6 \cdot 15388 + 5 &\Longrightarrow 92333 \in M_5.
\end{aligned}$$

Lema 9.5. Sejam $k \in \mathbb{N}$ e $a, b \in M_1 = \{kq + 1 \mid q \in \mathbb{Z}\}$. Logo, $ab \in M_1$.

Demonstração. Temos $a = kq_0 + 1$ e $b = kq_1 + 1$. Daí,

$$\begin{aligned}
ab &= k^2 q_0 q_1 + k(q_0 + q_1) + 1 \\
&= k(kq_0 q_1 + q_0 + q_1) + 1 \\
&= \underbrace{km}_{\in M_1} + 1, m \in \mathbb{Z}.
\end{aligned}$$

□

Lema 9.6. Existem infinitos primos da forma $4k + 3, k \in \mathbb{N} \cup \{0\}$.

Demonstração. Vamos dividir $\mathbb{Z} = \dot{\bigcup_{i=0}^{3}} M_i$, de acordo com os restos da divisão por 4. Como M_0 e M_2 têm apenas números pares, não há primos neles. Logo, há infinitos primos em $M_1 \cup M_3$.

Suponha que $M_3^{(p)}$ é finito, i.e., a quantidade de primos da forma $4k + 3$ é finita. Suponha

$$M_3^{(p)} = \{p_1, p_2, \dots, p_r\}, \quad 3 = p_1 < p_2 < \cdots < p_r,$$

defina

$$(*) \qquad m = 4 \cdot p_2 p_3 \cdots p_r + 3 \in M_3,$$

e note que $p_1 = 3$ está excluído. Pelo TFA,

$$m = q_1 q_2 \cdots q_s, q_1 \leq q_2 \leq \cdots \leq q_s \text{ primos.}$$

De (*), segue que $3 \nmid m$, logo $q_1 \neq 3$, e como $p_j \nmid 4 \cdot p_2 p_3 \cdots p_r + 3$, temos $q_1, q_2, \ldots, q_s \in M_3$, logo $q_1, q_2, \ldots, q_s \in M_1$. Pelo Lema (9.5), $m = q_1 q_2 \cdots q_s \in M_1$, logo

$$4 \cdot p_2 p_3 \cdots p_r + 3 = m = 4k + 1$$

o que é absurdo! Logo, $M_3^{(p)}$ é infinito. □

10 Bases numéricas

Em geral, escrevemos todo os números na base 10, i.e., $\forall n \in \mathbb{Z}$, escrevemos

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0,$$

com $a_j \in \{0, 1, 2, \ldots, 9\}, 1 \leq j \leq k$.

Exemplo. $12346 = 1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 6$.

Usando as mesmas ideias, podemos escrever n em qualquer base por meio de divisões sucessivas.

Exemplo. $12346 = 5 \cdot 7^4 + 0 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7 + 5$, logo $(12346)_{10} = (50665)_7$.

A base numérica usada em computadores é a base 2 (binária).

Exemplo. $12346 = 2^{13} + 2^{12} + 0 \cdot 2^{11} + \cdots + 0 \cdot 2^6 + 2^5 + 2^4 + 2^3 + 0 \cdot 2^2 + 2^1 + 1$, logo $12346 = (11000000111010)_2$.

11 Critérios de divisibilidade

A seguir apresentaremos alguns critérios de divisibilidade de $n \in \mathbb{N}$. Primeiramente, vamos escrever n como

$$n = \sum_{i=0}^{k} a_i 10^i, a_i \in \{0, 1, \ldots, 9\}.$$

Lema 11.1. $9|n \Leftrightarrow 9 \Big| \sum_{j=0}^{k} a_j$.

Demonstração. Note que

$$10^k = \underbrace{999\ldots9}_{k \text{ vezes}} + 1 = 9 \cdot \underbrace{111\ldots1}_{k \text{ vezes}} + 1,$$

logo

$$\begin{aligned} n &= a_k(9 \cdot \underbrace{111\ldots1}_{k} + 1) + \cdots + a_2(9 \cdot 11 + 1) + a_1(9 + 1) + a_0 \\ &= 9(a_k \cdot \underbrace{111\ldots1}_{k} + \cdots + a_2 \cdot 11 + a_1) + (a_k + \cdots + a_1 + a_0) \\ &= 9M + \sum_{j=0}^{k} a_j. \end{aligned}$$

Portanto, $9|n \Leftrightarrow 9\Big|\sum_{j=0}^{k} a_j$. □

Exemplo. $9|109521$ pois $9|1+9+5+2+1=18$.

Corolário 11.1.1. $3|n \Leftrightarrow 3\Big|\sum_{j=0}^{k} a_j$.

Corolário 11.1.2. $6|n \Leftrightarrow n$ é par e $3\Big|\sum_{j=0}^{k} a_j$.

Demonstração. Das hipóteses, $2|n$ e $3|n$ implica que $6|n$. □

Lema 11.2. $5|n \Leftrightarrow a_0 = 0$ ou 5.

Demonstração. Como

$$\begin{aligned} n &= 10(a_k 10^{k-1} + \cdots + a_2 10 + a_1) + a_0 \\ &= 10M + a_0. \end{aligned}$$

Logo, $5|n \Leftrightarrow 5|a_0 \Leftrightarrow a_0 = 0$ ou $a_0 = 5$. □

Lema 11.3. $4|n \Leftrightarrow 4|a_1 10 + a_0$.

Demonstração. Como

$$\begin{aligned} n &= 10^2(a_k 10^{k-2} + \cdots + a_2) + a_1 10 + a_0 \\ &= 10^2 M + 10a_1 + a_0 \end{aligned}$$

e, como $4|10^2$, temos que

$$4|n \Leftrightarrow 4|10a_1 + a_0.$$

□

12 Exercícios Resolvidos

Exercício 1. Mostre que se $x, y \in \mathbb{N}$ são ímpares, então $x^2 + y^2$ não pode ser um quadrado.

Solução. Escreva $x = 2t+1$ e $y = 2l+1, t, l \in \mathbb{Z}$. Daí,

$$x^2 + y^2 = 4t^2 + 4t + 1 + 4l^2 + 4l + 1 = 4M + 2 \text{ (par)}.$$

Se $x^2 + y^2 = n^2$, então n^2 é par e, consequentemente, n é par. Mas então $4|n^2$, o que é absurdo por $4 \nmid 4M + 2$.

Exercício 2. Mostre que $a|bc \Leftrightarrow \dfrac{a}{d}\Big|c$, com $d = \text{mdc}(a, b)$.

Solução. Tome $a = d\lambda$ e $b = d\mu$. Suponha que $a|bc$. Desse modo, $bc = at$, logo

$$d\mu c = d\lambda t \Rightarrow \mu c = \lambda t \Rightarrow \lambda|\mu c.$$

Pelo Lema (3.1), $\text{mdc}(\lambda, \mu) = 1$, logo, pelo Lema (3.3), temos que $\lambda|c$, i.e., $\dfrac{a}{d}\Big|c$.

Reciprocamente, suponha que $\lambda|c$. Então, $c = \lambda r$. Note que $bc = d\mu\lambda r = (d\lambda)\mu r = a\mu r$, i.e., $a|bc$.

Exercício 3. Mostre que se $n \in \mathbb{N}, n > 4$ inteiro composto, então $n|(n-1)!$.

Solução. Vamos considerar casos. Primeiro, suponha $n = p^r, r \geq 2$. Nesse caso,

$$(p^r - 1)! = 1 \cdot 2 \cdots p(p+1) \cdots 2p \cdots p^{r-1} \cdots (p^r - 2)(p^r - 1).$$

Logo, como $r \geq 2$, temos

$$(p^r - 1)! = p^r M \Rightarrow p^r|(p^r - 1)!.$$

Agora, suponha $n = p_1^{r_1} \cdots p_s^{r_s}$, com $s \geq 2$. Nesse caso,

$$p_j^{r_j} < n, \forall j = 1, 2, \ldots, s$$

logo todas as potências $p_j^{r_j}$ aparecerão em $(n-1)!$, ou seja, $p_j^{r_j}|(n-1)!, \forall j = 1, 2, \ldots, s$. Note que $\text{mdc}(p_i^{r_i}, p_j^{r_j}) = 1$ sempre que $i \neq j$. Desse modo, generalizando o Lema (7.5), temos

$$p_1^{r_1} \cdots p_s^{r_s}|(n-1)!.$$

Exercício 4. Mostre que existem infinitos primos da forma $6k + 5, k \in \mathbb{N} \cup \{0\}$.

Solução. Pela Observação (9.2), temos $\mathbb{Z} = M_0 \dot{\bigcup} M_1 \dot{\bigcup} M_2 \dot{\bigcup} M_3 \dot{\bigcup} M_4 \dot{\bigcup} M_5$ com $M_j = \{6k + j \mid k \in \mathbb{Z}\}$ e $j = 0, 1, 2, 3, 4, 5$.

Observe que M_0 e M_4 não têm primos (pois contêm números pares diferentes de 2 apenas); M_3 tem apenas o primo 3 (pois conterá múltiplos de 3) e M_2 tem apenas o primo 2 (pois conterá pares).

Portanto, há infinitos primos em $M_1 \bigcup M_5$. Suponha que há uma quantidade finita de primos em M_5, digamos $p_0, p_1, \ldots, p_k$, com $p_0 < p_1 < \cdots < p_k$. Nesse caso, $p_0 = 5, p_1 = 11, p_2 = 17$ e assim por diante.

Escreva

$$m = 6p_1 \cdot p_2 \cdots p_k + 5, \text{ excluindo } p_0 = 5.$$

Pelo TFA,

$$m = q_1 q_2 \cdots q_s, \text{ com } q_j \text{ primo}, j = 1, 2, \ldots, s.$$

Observe que

$$m \in M_5, \text{ logo } 2 \nmid m \text{ e } 3 \nmid m.$$

Vamos considerar casos. Primeiro, considere $q_1 = 5$.

Nesse caso, $5|m$, ou seja, $5|6p_1 \cdots p_k + 5$ e $5|6p_1 \cdots p_k$, o que obriga $p_j = 5$ para algum j. Absurdo.

Considere $q_1 = p_j$ para algum $j \in \{1, 2, \ldots, k\}$. Como $q_1|6p_1 \cdots p_k + 5$ e $q_1|6p_1 \cdots p_k$, então $q_1|5$. Como q_1 é primo, $q_1 = 5 = p_j$. Absurdo.

Logo, $q_j \notin M_5, \forall j = 1, 2, \ldots, s$, de modo que $q_1, q_2, \ldots, q_s \in M_1$. Pelo Lema (9.5), $m = q_1 q_2 \cdots q_s \in M_1$, o que é absurdo pois $m \in M_5$ e $M_i \bigcap M_j = \varnothing$ sempre que $i \neq j$. Logo, há infinitos primos em M_5.

Exercício 5. Mostre que todo primo da forma $3k + 1$ é também da forma $6t + 1, k, t \in \mathbb{Z}$.

Solução. Seja $p = 3k + 1$ primo. Se k é ímpar, então $k = 2l + 1$, logo $p = 3(2l + 1) + 1 = 6l + 4$, i.e., $p = 2$, absurdo! Logo, k é par, $k = 2l$, e temos $p = 6l + 1$.

Exercício 6. Encontre $n \in \mathbb{N}$ tal que $n/2$ é quadrado, $n/3$ é cubo e $n/5$ é quinta potência.

Solução. Devemos ter $n = 2^a \cdot 3^b \cdot 5^c \cdot N$. Assuma $n = 2^a \cdot 3^b \cdot 5^c$. Temos que

$$a - 1, b, c \text{ são pares;}$$

$$a, b - 1, c \text{ são múltiplos de 3;}$$

$$a, b, c - 1 \text{ são múltiplos de 5.}$$

Escolha $a = 15, b = 10$ e $c = 6$. Note que $n = 2^{15} \cdot 3^{10} \cdot 5^6$ satisfaz os requisitos.

Exercício 7. Para que valores $n \in \mathbb{Z}$ temos $\dfrac{2n - 1}{n + 7} \in \mathbb{Z}$?

Solução. Queremos $2n - 1 = \lambda(n + 7), \lambda \in \mathbb{Z}$. Note que

$$2n - 1 = 2(n + 7) - 15, \text{ logo}$$

$$n + 7|2n - 1 \Leftrightarrow n + 7|15.$$

Os divisores inteiros de 15 são $\pm 1, \pm 3, \pm 5, \pm 15$. Daí, $n + 7 = -6, -8, -4, -10, -2, -12, 8, -22$, ou seja, $n \in \{-22, -12, -10, -8, -6, -4, -2, 8\}$.

Exercício 8. Mostre que toda lista de k inteiros consecutivos contém um elemento divisível por k.

Solução. Seja a lista $n, n + 1, \ldots, n + k - 1$. Pelo Algoritmo de Euclides, $n = qk + r$, com $r \in \{0, 1, \ldots, k - 1\}$. Se $r = 0$, $k|n$ e terminamos. Suponha $1 \leq r \leq k - 1$. Logo, existe $t \in \{1, 2, \ldots, k - 1\}$ tal que $r + t = k$. Portanto, $n + t = k$.

Exercício 9. Mostre que o produto de k inteiros consecutivos é divisível por $k!$.

Solução. Escreva o produto como

$$n(n+1)\cdots(n+k-1), \text{ com } n \in \mathbb{Z}.$$

Se esse produto é 0, temos $k!|0$. Assuma, sem perda de generalidade, que o produto é não nulo e todos os termos são naturais. Escreva

$$\Gamma = m(m-1)(m-2)\cdots(m-k+1).$$

Note que $\binom{m}{k} = \dfrac{m!}{k!(m-k)!} = \dfrac{\Gamma}{k!} \in \mathbb{Z}_+^*$, logo $k!|\Gamma$.

Exercício 10. Seja $n \in \mathbb{N}, n \geq 2$ e $Q_n = n! + 1$. Mostre que todo divisor primo de Q_n é maior que n, e conclua que existem infinitos primos.

Solução. Pelo TFA, $Q_n = p_1 \cdots p_r, p_1 \leq \cdots \leq p_r$ primos. Suponha $p_1 \leq n$. Logo, $p_1|n!$, ou seja, $p_1|Q_n - n! = 1$, absurdo! Logo, $p_j > n, \forall 1 \leq j \leq r$.

Vamos mostrar que $\text{mdc}(Q_n, Q_m) = 1, \forall m, n \in \mathbb{N}, m \neq n$.

Suponha, sem perda de generalidade, $2 \leq m < n$. Note que $\forall r \in \mathbb{N}$, $m! + 1 < m \cdot m! < (m+1) \cdot m! = (m+1)!$, logo $Q_m < (m+1)! = Q_{m+1} - 1$. Logo, $Q_m < n!$ sempre que $m < n$, e então

$$Q_m|n! \Rightarrow \text{ se } p|Q_m \text{ então } p \nmid Q_m,$$

ou seja, os primos divisores de Q_n não dividem nenhum dos Q_m's anteriores, logo $|\mathbb{P}| = \infty$.

Exercício 11. Mostre que três ímpares consecutivos somente serão primos se forem $3, 5, 7$.

Solução. Seja $n \in \mathbb{N}, n \geq 3$, e considere $n, n+2, n+4$ ímpares. Note que $n+2, n+3, n+4$ são três números consecutivos, i.e., um deles é divisível por 3. Como $n+2$ e $n+4$ são primos maiores que 5, devemos ter $3|n+3$. Logo, $n+3 = 3\lambda$, i.e., $3|n$. Como n é primo, temos $n = 3$.

Exercício 12. Suponha que $\text{mdc}(a, p^2) = p$ e $\text{mdc}(b, p^3) = p^2$. Calcule $\text{mdc}(ab, p^4)$ e $\text{mdc}(a + b, p^4)$.

Solução. Por hipótese, $a = p\lambda$ e $b = p^2\mu$, com $\text{mdc}(p, \lambda\mu) = 1$. Logo, $ab = p^3\lambda\mu$ e $a+b = p(\lambda + p\mu)$. Se $p|\lambda + p\mu$, então $p|\lambda$, absurdo! Logo, $\text{mdc}(ab, p^4) = p^3$ e $\text{mdc}(a + b, p^4) = p$.

Exercício 13. Mostre que $\text{mdc}(n! + 1, (n+1)! + 1) = 1, \forall n \in \mathbb{N}$.

Solução. Seja $d = \text{mdc}(n!+1, (n+1)!+1)$ e escreva $(n+1)!+1 = n \cdot n! + n! + 1$. Como $d|(n+1)!+1$ e $d|n! + 1$, então $d|n \cdot n!$.

Por outro lado, $\text{mdc}(n!, n! + 1) = 1$. Pelo Lema (3.3), $d|n$, o que implica $d|n!$, um absurdo se $d \neq 1$.

Exercício 14. Determine todos os primos p tais que $17p+1$ é quadrado.

Solução. Temos $17p+1 = n^2 \Leftrightarrow 17p = (n-1)(n+1)$. Como $n+1 = (n-1)+2$, então $d = \text{mdc}(n+1, n-1)|2$, logo $d = 1$ ou $d = 2$. Como $p \neq 2$, $d = 1$. Do TFA, segue que $17 = n-1$ e $p = n+1$ ou $17 = n+1$ e $p = n-1$, o que implica $n = 18$ e $p = 19$ ou $n = 16$ e $p = 15$. Logo, $p = 19$.

Exercício 15. Mostre que n^4+4 é sempre composto, $\forall n \geq 2$.

Solução. Para fatorar n^4+4, podemos fazê-lo como

$$n^4+4 = (n+a)(n^3+b_1n^2+b_2n+b_3) \text{ ou } n^4+4 = (n^2+an+b)(n^2+cn+d).$$

No primeiro caso, temos $(-a)^4+4 = 0$, absurdo. No segundo caso, encontramos

$$n^4+4 = \underbrace{(n^2-2n+2)}_{\geq 1}\underbrace{(n^2+2n+2)}_{\geq 1}, \text{ pois } n \geq 2.$$

Logo, n^4+4 é sempre composto.

Exercício 16. Seja $n \in \mathbb{N}$ e $n = a_k10^k + \cdots + a_110 + a_0$ com $a_1, \ldots, a_k \in \{0, 1, \ldots, 9\}$. Mostre que $11|n \Leftrightarrow 11\left|\sum_{j \text{ ímpar}} a_j - \sum_{j \text{ par}} a_j\right.$.

Solução. Note que

$$10^{2n} = \underbrace{9090\ldots90}_{2(n-1)}9 \cdot 11 + 1 \text{ e } 10^{2n+1} = \underbrace{9090\ldots90}_{2(n-1)}9 \cdot 11 - 1.$$

Assim, temos

$$n = 11R + \sum_{j \text{ par}} a_j - \sum_{j \text{ ímpar}} a_j, \text{ pois } 10^l = \begin{cases} 11M+1, l \text{ par} \\ 11N-1, l \text{ ímpar.} \end{cases}$$

Logo, $11|n \Leftrightarrow 11\left|\sum_{j \text{ par}} a_j - \sum_{j \text{ ímpar}} a_j\right.$.

13 Números de Fermat

Lema 13.1. Sejam $a, b \in \mathbb{N}$ com $a \geq 2$. Se a^n+1 é primo, então a é par e $n = 2^k, k \in \mathbb{N}$.

Demonstração. Como $a \geq 2$, então $a^n+1 \geq 3$ e como a^n+1 é par para a ímpar, devemos ter a par para que a^n+1 seja primo. Suponha $n = rs$ com $r \geq 3$ ímpar. Como

$$x^r+1 = (x+1)(x^{r-1}-x^{r-2}+\cdots+1),$$

temos que $x+1|x^r+1$. Fazendo $x = a^s$, obtemos que $a^s+1|a^n+1$, i.e., a^n+1 é composto.

Portanto, se $a^n+1 \in \mathbb{P}$, então a é par e n não tem fator ímpar, ou seja, $n = 2^k, k \in \mathbb{N}$. □

Definição. Seja $n \in \mathbb{N} \cup \{0\}$. Os números da forma $F_n = 2^{2^n} + 1$ são chamados *números de Fermat*.

Note que $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Fermat conjecturou que todos F_n são primos e de fato $F_0, \ldots, F_4$ o são. Contudo, ainda não encontrou-se nenhum primo F_n com $n \geq 5$.

Lema 13.2. $\prod_{i=0}^{n} F_i = F_{n+1} - 1$.

Demonstração. Vamos proceder por indução em n. Como caso particular, temos $F_0 = F_1 - 2$.

Suponha, por hipótese de indução, que

$$\prod_{i=0}^{k} F_i = F_{k+1} - 2,$$

e considere

$$\begin{aligned}\prod_{i=0}^{k+1} F_i &= (F_{k+1} - 2)F_{k+1} \\ &= \left(2^{2^{k+1}} - 1\right)\left(2^{2^{k+1}} + 1\right) \\ &= 2^{2^{k+2}} - 1 \\ &= F_{k+2} - 2.\end{aligned}$$

O lema segue por indução. □

Lema 13.3. $\text{mdc}(F_i, F_j) = 1$ sempre que $i \neq j$.

Demonstração. Suponha, sem perda de generalidade, $i < j$ e seja $d = \text{mdc}(F_i, F_j)$. Por definição, F_n é sempre ímpar, logo d é ímpar. Pelo Lema (13.2), $2 = F_j - F_0 \cdots F_i \cdots F_{j-1}$. Como $d|F_i$ e $d|F_j$, então $d|2$. Logo, $d = 1$. □

Teorema 13.4. $|\mathbb{P}| = \infty$.

Demonstração. Tome $i, j \in \mathbb{N}, i \neq j$. Pelo TFA, $F_i = q_1 q_2 \cdots q_s$ e $F_j = p_1 p_2 \cdots p_r$. Pelo Lema (13.3), $\text{mdc}(F_i, F_j) = 1$, logo $q_t \neq p_l$ para todo $1 \leq t \leq s$ e $1 \leq l \leq r$. Como há infinitos números de Fermat distintos, $|\mathbb{P}| = \infty$. □

14 Primos de Mersenne e Números Perfeitos

Lema 14.1. Sejam $a, n \in \mathbb{N}, a \geq 2$. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.

Demonstração. Já vimos que

$$(*) \qquad x^t - 1 = (x - 1)(x^{t-1} + \cdots + x + 1),$$

ou seja, $x-1|x^t-1$. Tomando $x=a$ e $t=n$, temos que $a-1|a^n-1$, i.e., a^n-1 é composto se $a>2$.

Suponha n composto e escreva $n=rs$ com $1<r\leq s<n$. Tomando $t=r$ e $x=a^s$ em (*), temos que $a^s-1|a^n-1$, logo a^n-1 é composto. Portanto, é necessário ter $a=2$ e n primo para que a^n-1 seja primo (mas não é suficiente!). □

Definição. Seja p primo e defina $M_p=2^p-1$. Os número M_p são chamados de *primos de Mersenne*.

Mersenne conjecturou, em 1644, que M_p era primo para $p\leq 257$ se, e só se,

$$p\in\{2,3,5,7,13,17,19,31,67,127,257\}.$$

À época, já se sabia que $2^{11}-1$ não é primo (Regis – 1636); $2^{17}-1$ e $2^{19}-1$ são primos (Cataldi – 1603); $2^{23}-1$ e $2^{17}-1$ não são primos (Fermat – 1640).

Euler mostrou, em 1738, que $2^{29}-1$ não é primo, mas $2^{31}-1$ é. Lucas mostrou, em 1876, que $2^{127}-1$ é primo e Perrouchine mostrou, em 1883, que $2^{61}-1$ é primo. Em 1900, Powers mostrou que $2^{89}-1$ e $2^{107}-1$ são primos.

Hoje, sabemos que a lista correta de M_p primos com $p\leq 257$ é

$$\{2,3,5,7,13,17,19,31,61,89,107,127\}.$$

O maior primo M_p conhecido (2018) é $M_{82589933}$.

Definição (Função $\sigma(n)$)**.** Seja $n\in\mathbb{N}$ e defina a função $\sigma(n)$ como a soma dos divisores positivos de n, i.e.,

$$\sigma(n)=\sum_{d|n} d, d\in\mathbb{N}.$$

Exemplo. $\sigma(1)=1,\sigma(2)=3,\sigma(3)=4,\sigma(4)=7,\sigma(5)=6,\sigma(6)=12$.

Lema 14.2. Seja $n\in\mathbb{N}$. Então $n\in\mathbb{P}\Leftrightarrow\sigma(n)=n+1$.

Demonstração. Suponha n primo. Então, os únicos divisores positivos de n são 1 e n, logo $\sigma(n)=n+1$. Reciprocamente, suponha $\sigma(n)=n+1$. Como $\sigma(n)>n+1$ para todo n composto, segue que n é primo. □

Lema 14.3. Sejam $m,n\in\mathbb{N}$. Se $\text{mdc}(m,n)=1$, então $\sigma(mn)=\sigma(m)\sigma(n)$.

Demonstração. Como $\text{mdc}(m,n)=1$, segue que todo divisor de mn é da forma rs, com r divisor de m e s divisor de n (TFA). Sejam $r_1,\ldots,r_t$ os divisores positivos de m e $s_1,\ldots,s_l$ os divisores

positivos de n. Daí, os divisores positivos de mn são $r_1s_1, \ldots, r_1s_l, \ldots, r_ts_1, \ldots, r_ts_l$. Portanto,

$$\begin{aligned}\sigma(mn) &= r_1s_1 + \cdots + r_1s_l + \cdots + r_ts_1 + \cdots + r_ts_l \\ &= r_1\sigma(n) + \cdots + r_t\sigma(n) \\ &= \sigma(m)\sigma(n).\end{aligned}$$

□

Definição. Um número $n \in \mathbb{N}$ é *perfeito* se $\sigma(n) = 2n$.

Exemplo. 6, 28, 496, 8128 são perfeitos.

Teorema 14.4. Se M_p é primo, então $n = 2^{p-1}M_p$ é perfeito. Além disso, se n é perfeito par então $\exists p \in \mathbb{P}$ tal que $n = 2^{p-1}M_p$ e M_p é primo.

Demonstração. Suponha M_p primo e escreva $n = 2^{p-1}M_p$. Como M_p é sempre ímpar, segue do Lema (14.3) que $\sigma(n) = \sigma(2^{p-1})\sigma(M_p)$. Note que

$$\sigma(2^{p-1}) = 1 + 2 + 2^2 + \cdots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1.$$

Como M_p é primo, temos $\sigma(M_p) = M_p + 1 = 2^p$. Daí,

$$\sigma(n) = \sigma(2^{p-1})\sigma(M_p) = (2^p - 1)2^p = 2 \cdot 2^{p-1}M_p = 2n,$$

logo n é perfeito.

Reciprocamente, suponha n perfeito par e escreva $n = 2^{k-1}m$, m ímpar. Assim,

$$\sigma(n) = 2n = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Como $2n = 2^km$ e $\text{mdc}(2^k, 2^{k-1}) = 1$, segue que $2^k - 1 | m$ (Lema (3.3)). Escrevendo $m = (2^k - 1)m_0$, temos

$$\sigma(n) = 2^km = 2^k(2^k - 1)m_0 = (2^k - 1)\sigma(m) \Leftrightarrow \sigma(m) = 2^km_0.$$

Note que

$$\sigma(m) = 2^km_0 \geq m + m_0 = (2^k - 1)m_0 + m_0 = 2^km_0,$$

pois m e m_0 dividem m. Logo, $\sigma(m) = m + m_0$, i.e., m só tem dois divisores positivos, sendo primo; logo, $m_0 = 1$ e, daí, $m = 2^k - 1$ é primo e k é primo (Lema (14.1)). Portanto, $m = M_k$ e $n = 2^{k-1}M_k$, k primo. □

Observação 14.1. Todos os números perfeitos conhecidos são pares, e sabe-se que se n é perfeito ímpar, então $n > 10^{500}$.

15 Congruência módulo m

Definição. Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}, m \geq 2$. Dizemos que a é *congruente a* b *módulo* m se $m|a-b$. Denotamos esse fato por $a \equiv b \bmod m$.

Exemplo. $19 \equiv 4 \bmod 5$, pois $5|19-4$; $121 \equiv 0 \bmod 4$, pois $11|121-0$; $1001 \equiv 2 \bmod 9$, pois $9|1001-2$.

Lema 15.1. Seja $m \in \mathbb{N}, m \geq 2$. Então,

(i) $a \equiv a \bmod m, \forall a \in \mathbb{Z}$;

(ii) $a \equiv b \bmod m \Rightarrow b \equiv a \bmod m, \forall a, b \in \mathbb{Z}$;

(iii) $a \equiv b \bmod m$ e $b \equiv c \bmod m \Rightarrow a \equiv c \bmod m, \forall a, b, c \in \mathbb{Z}$.

Demonstração. Como $m|a-a, a \equiv a \bmod m$.

Se $a \equiv b \bmod m$, então $m|a-b$, i.e., $a-b = mt \Leftrightarrow b-a = m(-t) \Leftrightarrow b \equiv a \bmod m$.

Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a-b = mt_1$ e $b-c = mt_2$. Logo, $a-c = m(t_1+t_2)$, i.e., $a \equiv c \bmod m$. □

Lema 15.2. Sejam $a, b, c, d, m \in \mathbb{Z}, m \geq 2$. Suponha $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Então

(i) $a + c \equiv b + d \bmod m$;

(ii) $ac \equiv bd \bmod m$.

Demonstração. Por hipótese, $a - b = mt$ e $c - d = mk$. Daí, $(a+c) - (b+d) = m(t+k)$, i.e., $m|(a+c)-(b+d)$ e $a + c \equiv b + d \bmod m$.

Além disso, $ac - bc = mtc$ e $cb - bd = mkb$, logo $ac - bd = m(tc + kb)$, i.e., $ac \equiv bd \bmod m$. □

Lema 15.3. Se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m, \forall n \in \mathbb{N}$.

Demonstração. (Indução sobre n) Segue do Lema (15.2) que, tomando $c = a$ e $d = b$, temos $a^2 \equiv b^2 \bmod m$. Suponha, por hipótese de indução, $a^{k-1} \equiv b^{k-1} \bmod m$. Considerando $c = a^{k-1}$ e $d = b^{k-1}$, segue do Lema (15.2) que $a^k \equiv b^k \bmod m$, e o resultado segue por indução. □

Exemplo. Temos $119 \equiv 20 \bmod 11$ e $91 \equiv 14 \bmod 11$, logo $210 \equiv 34 \bmod 11$, $10829 \equiv 280 \bmod 11$ e $753571 \equiv 2744 \bmod 11$.

Definição. Sejam $a, m \in \mathbb{Z}, m \geq 2$. Defina $\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \bmod m\}$. O conjunto $\overline{a}$ é a *classe de congruência de* a *módulo* m.

Com essa notação, podemos reescrever o Lema (15.1) como

Lema 15.4. Sejam $a, b, c, d, m \in \mathbb{Z}, m \geq 2$. Então

(i) $a \in \overline{a}$;

(ii) $a \in \overline{b} \Rightarrow b \in \overline{a}$;

(iii) $a \in \overline{b}$ e $b \in \overline{c} \Rightarrow a \in \overline{c}$.

Demonstração. Como $a \equiv a \bmod m$ (Lema (15.1)), $a \in \overline{a}$.

Se $a \in \overline{b}$, $a \equiv b \bmod m$, por definição. Do Lema (15.1), $b \equiv a \bmod m$, i.e., $b \in \overline{a}$.

Se $a \in \overline{b}$ e $b \in \overline{c}$, então $a \equiv b \bmod m$ e $b \equiv c \bmod m$. Do Lema (15.1), $a \equiv c \bmod m$, i.e., $a \in \overline{c}$. □

Lema 15.5. Sejam $a, b, m \in \mathbb{Z}, m \geq 2$. Então

(i) $a \in \overline{b} \Rightarrow \overline{a} = \overline{b}$;

(ii) $a \notin \overline{b} \Rightarrow \overline{a} \cap \overline{b} = \varnothing$.

Demonstração. Por definição, $a \in \overline{b}$ implica $a \equiv b \bmod m$. Do Lema (15.4)(iii),

$$c \in \overline{a} \Leftrightarrow a \equiv c \bmod m \Leftrightarrow b \equiv c \bmod m \Leftrightarrow c \in \overline{b},$$

logo $\overline{a} = \overline{b}$.

Suponha $a \notin \overline{b}$ e $c \in \overline{a} \cap \overline{b}$. Então, $c \equiv a \bmod m$ e $c \equiv b \bmod m$, logo $a \equiv b \bmod m$ (Lema (15.1)(iii)), i.e., $a \in \overline{b}$, absurdo. □

Lema 15.6. Sejam $a, m \in \mathbb{Z}, m \geq 2$, e escreva $a = mq + r, 0 \leq r < m$. Então, $a \equiv r \bmod m$, i.e., $a \in \overline{r}$.

Demonstração. Como $a - r = mq$, então $a \equiv r \bmod m$. □

Lema 15.7. Seja $m \in \mathbb{N}, m \geq 2$. Então

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{m-1},$$

com $\overline{c}$ a classe de congruência de c módulo m.

Demonstração. Da Observação (9.2), vimos que $\mathbb{Z} = \dot{\bigcup_{i=0}^{m-1}} M_i$, com $M_r = \{mq + r \mid q \in \mathbb{Z}\}$ e $0 \leq r \leq m-1$. Observe que $b \in M_r \Leftrightarrow b = mq + r \Leftrightarrow b \equiv r \bmod m \Leftrightarrow b \in \overline{r}$, ou seja, $M_r = \overline{r}$. Com isso, temos o resultado desejado. □

Exemplo. Para $m = 8$, temos

$$\overline{0} = \{8q \mid q \in \mathbb{Z}\} = \{\dots, -16, -8, 0, 8, 16, \dots\},$$
$$\overline{1} = \{8q + 1 \mid q \in \mathbb{Z}\} = \{\dots, -15, -7, 1, 9, 17, \dots\}.$$

Segue do Lema (15.5) que, por exemplo

$$\overline{0} = \overline{-24} = \overline{-8} = \overline{16} = \overline{32},$$
$$\overline{1} = \overline{-31} = \overline{-7} = \overline{17} = \overline{25}.$$

Lema 15.8. Sejam $a, b, c, m \in \mathbb{Z}, m \geq 2$. Se $ac \equiv bc \bmod m$ e $\text{mdc}(m, c) = 1$, então $a \equiv b \bmod m$.

Demonstração. Por hipótese, $ac - bc = c(a - b) = m\lambda$. Como $m|c(a - b)$ e $\text{mdc}(m, c) = 1$, então pelo Lema (3.3) $m|a - b$. Logo, $a \equiv b \bmod m$. □

Observação 15.1. $2 \cdot 3 \equiv 2 \cdot 0 \bmod 6$, mas $3 \not\equiv 0 \bmod 6$.

Lema 15.9. Seja $m \in \mathbb{N}, m \geq 2$. Se $a, b \in \overline{d}$, então $a \equiv b \bmod m$, com $\overline{d}$ a classe de congruência de d módulo m.

Demonstração. Por hipótese, $a \equiv d \bmod m$ e $b \equiv d \bmod m$. Segue do Lema (15.1) que $s \equiv b \bmod m$. □

Definição. Sejam $a_1, a_2, \dots, a_r, m \in \mathbb{Z}, m \geq 2$. Dizemos que $\{a_1, a_2, \dots, a_r\}$ é um *sistema completo de resíduos (SCR) módulo* m se

(1) $a_i \not\equiv a_j \bmod m$ se $i \neq j$;

(2) $\forall b \in \mathbb{Z}$, $\exists i \in \{1, 2, \dots, r\}$ tal que $b \equiv a_i \bmod m$.

Lema 15.10. Seja $m \in \mathbb{N}, m \geq 2$. Então $\{0, 1, 2, \dots, m - 1\}$ é SCR módulo m.

Demonstração. Sejam $i, j \in \{0, 1, 2, \dots, m - 1\}$, $i \neq j$. Sem perda de generalidade, suponha $0 \leq i < j \leq m - 1$, de modo que $0 < j - i < m - 1$. Nesse caso, $m \nmid j - i$, i.e., $i \not\equiv j \bmod m$. Isso verifica a condição (1).

Seja $b \in \mathbb{Z}$ qualquer e escreva $b = mq + r$, $0 \leq r \leq m - 1$. Como $b \equiv r \bmod m$, a condição (2) é satisfeita. □

Observação 15.2. Uma demonstração alternativa desse lema segue do Lema (15.7), onde vimos que $\mathbb{Z} = \overline{0} \dot\cup \overline{1} \dot\cup \cdots \dot\cup \overline{(m-1)}$.

Lema 15.11. Seja $m \in \mathbb{N}, m \geq 2$. Sejam $a_1 \in \overline{0}, a_2 \in \overline{1}, \dots, a_m \in \overline{(m-1)}$. Então, $\{a_1, a_2, \dots, a_m\}$ é SCR módulo m.

Demonstração. Sejam a_i, a_j com $i \neq j$. Por hipótese, $a_i \equiv i-1 \not\equiv j-1 \equiv a_j \bmod m$, pois $i-1, j-1 \in \{0,1,\ldots,m-1\}$ e $i \neq j$. Tome $b \in \mathbb{Z}$ qualquer e escreva $b = mq + r$. Então, $b \equiv r \bmod m, r \in \{0,1,\ldots,m-1\}$, i.e., $b \in \overline{r}$. Como $a_{r+1} \equiv r \bmod m$, então $a_{r+1} \in \overline{r}$ e $b \equiv a_{r+1} \bmod m$ pelo Lema (15.9). □

Lema 15.12. Sejam $a_1, a_2, \ldots, a_r, m \in \mathbb{Z}, m \geq 2$. Se $\{a_1, a_2, \ldots, a_r\}$ é SCR módulo m, então

(i) $r = m$;

(ii) após renumeração de índices, $a_1 \in \overline{0}, a_2 \in \overline{1}, \ldots, a_m \in \overline{(m-1)}$.

Demonstração. Pelo Lema (15.7), temos $\mathbb{Z} = \overline{0} \dot\cup \overline{1} \dot\cup \cdots \dot\cup \overline{(m-1)}$. Se $r > m$, então pelo Princípio da Casa dos Pombos, existem $i, j \in \{1,2,\ldots,r\}$ e $n \in \{0,1,\ldots,m-1\}$ tais que $a_i, a_j \in \overline{n} \Leftrightarrow a_i \equiv a_j \bmod n$ pelo Lema (15.9). Absurdo, pois $\{a_1, \ldots, a_r\}$ é SCR módulo m.

Se $r < m$, existe $n \in \{0,1,\ldots,m-1\}$ tal que $\{a_1, a_2, \ldots, a_r\} \cap \overline{n} = \varnothing$, ou seja, $n \not\equiv a_j \bmod m, \forall j \in \{1,2,\ldots,r\}$, o que também é impossível pois é SCR. Logo, $r = m$.

Como os a_j's são dois a dois incongruentes módulo m, não podemos ter dois deles na mesma clase de congruência módulo m, ou seja, após reordenação de índices, necessariamente teremos

$$a_1 \in \overline{0}, a_2 \in \overline{1}, \ldots, a_m \in \overline{(m-1)}.$$

□

Corolário 15.12.1. Com as mesmas hipóteses do lema anterior, temos $\dot\bigcup_{i=1}^{m} \overline{a_i}$.

Demonstração. Segue do Lema (15.5) que $\overline{a_1} = \overline{0}, \overline{a_2} = \overline{1}, \ldots, \overline{a_m} = \overline{m-1}$. □

Lema 15.13. Sejam $b_1, b_2, \ldots, b_m \in \mathbb{Z}$ dois a dois incongruentes módulo m. Então $\{b_1, \ldots, b_m\}$ é SCR módulo m.

Demonstração. Como os b_i's são incongruentes dois a dois, e há m deles, devemos ter $b_1 \in \overline{0}, b_2 \in \overline{1}, \ldots, b_m \in \overline{(m-1)}$ após reordenação de índices. O resultado segue, então, do Lema (15.11). □

Lema 15.14. Seja $\{r_1, \ldots, r_m\}$ SCR módulo m e $b \in \mathbb{Z}$ com $\text{mdc}(m, b) = 1$. Então $\{br_1, \ldots, br_m\}$ é SCR módulo m.

Demonstração. Sejam $i, j \in \{1,2,\ldots,m\}, i \neq j$. Se $br_i \equiv br_j \bmod m$, então $r_i \equiv r_j \bmod m$ pelo Lema (15.8). Como $\{r_1, \ldots, r_m\}$ é SCR módulo m, temos então que $br_i \not\equiv br_j \bmod m$. Pelo Lema (15.13), $\{br_1, \ldots, br_m\}$ é SCR módulo m. □

Exemplo. Seja $m = 4$. Temos $\mathbb{Z} = \overline{14} \cup \overline{41} \cup \overline{387} \cup \overline{1260}$ porque $1260 \equiv 0 \bmod 4$, $41 \equiv 1 \bmod 4$, $14 \equiv 2 \bmod 4$ e $387 \equiv 3 \bmod 4$.

Lema 15.15 (Lema de Euler)**.** Sejam $p \in \mathbb{P}$ e $a \in \mathbb{Z}$, com $\text{mdc}(a,p) = 1$. Então

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

Demonstração. Como $\text{mdc}(a,p) = 1$, os Lemas (15.10) e (15.14) garantem que $\{0, a\cdot 1, \ldots, a(p-1)\}$ é SCR módulo p. Como $\{0,1,\ldots,p-1\}$ é SCR módulo p, temos que $\forall i \in \{1,2,\ldots,p-1\}$, $\exists! j \in \{1,2,\ldots,p-1\}$ tal que $a\cdot i \equiv j \bmod p$. Logo, pelo Lema (15.2),

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

ou seja

$$a^{p-1}\cdot(p-1)! \equiv (p-1)! \bmod p.$$

Como $\text{mdc}((p-1)!, p) = 1$, segue do Lema (15.8) que

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

□

Exemplo. Determine o resto da divisão de 429^{346} por 7. Note que $429 = 7\cdot 61 + 2$, i.e., $429 \equiv 2 \bmod 7$. Assim, $429^{346} \equiv 2^{346} \bmod 7$. Pelo Lema de Euler, $2^6 \equiv 1 \bmod 7$ e, como $346 = 6\cdot 57 + 4$, temos $2^{346} \equiv (2^6)^{57}\cdot 2^4 \equiv 16 \equiv 2 \bmod 7$. Logo, o resto é 2.

Teorema 15.16 (Pequeno Teorema de Fermat)**.** Sejam $p \in \mathbb{P}$ e $a \in \mathbb{Z}$. Então

$$a^p \equiv a \bmod p.$$

Demonstração. Se $a \equiv 0 \bmod p$, então $a^p \equiv 0 \equiv a \bmod p$. Suponha, então, $a \not\equiv 0 \bmod p$, i.e., $\text{mdc}(a,p) = 1$. Do Lema de Euler, $a^{p-1} \equiv 1 \bmod p$ e, consequentemente, $a^p \equiv a \bmod p$. □

Lema 15.17. Sejam $p, q \in \mathbb{P}, p \neq q$. Então

$$p^{q-1} + q^{p-1} \equiv 1 \bmod pq.$$

Demonstração. Pelo Lema de Euler, temos

$$p^{q-1} + q^{p-1} \equiv 0 + 1 \equiv 1 \bmod p,$$
$$p^{q-1} + q^{p-1} \equiv 1 + 0 \equiv 1 \bmod q.$$

Logo, tanto p quanto q dividem $p^{q-1} + q^{p-1} - 1$. Como $\text{mdc}(p,q) = 1$, segue que pq também divide, i.e., $p^{q-1} + q^{p-1} \equiv 1 \bmod p$. □

16 Equação de Congruência

Sejam a, b inteiros e $m \in \mathbb{N}, m \geq 2$. Considere a equação

$$ax \equiv b \bmod m.$$

Observe que se $ax_1 \equiv b \bmod m$, $x_1 \in \mathbb{Z}$, então $\exists x_0 \in \{0, 1, \ldots, m-1\}$ tal que $ax_1 \equiv ax_0 \equiv b \bmod m$. Portanto, podemos nos concentrar em encontrar soluções em $\{0, 1, \ldots, m-1\}$. O seguinte lema torna isso evidente.

Lema 16.1. Se $x_0 \in \mathbb{Z}$ é solução de

$$ax \equiv b \bmod m,$$

então todo $x^* \in \overline{x_0}$ também é.

Demonstração. Segue do Lema (15.2), já que $b \equiv ax_0 \equiv ax^* \bmod m$. □

Observação 16.1. O Lema (16.1) nos mostra que se existe uma solução, então existem infinitas soluções que são duas a duas congruentes. Portanto, para evitar discrepâncias, vamos considerar somente soluções incongruentes.

Lema 16.2. A equação de congruência

$$ax \equiv b \bmod m$$

tem solução se, e só se, $\text{mdc}(a, m) | b$. Se existir solução, então há exatamente $d = \text{mdc}(a, m)$ soluções incongruentes.

Demonstração. Seja x_0 solução. Então $\exists y_0 \in \mathbb{Z}$ tal que

$$ax_0 = b + my_0 \Leftrightarrow ax_0 - by_0 = b.$$

Pelos Lemas (5.1) e (5.2), essa equação tem solução se, e só se, $d | b$. Isso mostra a primeira parte do lema, e também nos dá as soluções dessa equação diofantina:

$$x_t = x_0 + \frac{m}{d}t \quad \text{e} \quad y_t = y_0 - \frac{a}{d}t.$$

Observe que $\forall t \in \mathbb{Z}$

$$ax_t = ax_0 + m\frac{at}{d} \text{ e } d|a, \text{ logo } ax_t \equiv ax_0 \equiv b \bmod m.$$

Além disso, $x_0, x_1, \ldots, x_{d-1}$ são incongruentes dois a dois, pois suponha que $i, j \in \{0, 1, \ldots, d-1\}, j \geq i$. Se $x_i \equiv x_j \bmod m$, então $m | x_j - x_i$, i.e., $m \Big| \frac{m}{d}(j-i)$, logo existe λ tal que $\frac{m}{d}(j-i) = m\lambda$, ou seja $j - i = d\lambda$, pois $m \geq 2$. Mas $0 \leq j - i \leq d - 1$, logo $j = i$.

Seja x_t outra solução qualquer, com $t \geq d$. Escreva $t = dq + r, 0 \leq r \leq d-1$. Logo

$$x_t = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(dq + r) = x_0 + \frac{m}{d}r + mq = x_r + mq,$$

ou seja

$$x_t \equiv x_r \bmod m, \text{ com } r \in \{0, 1, \ldots, d-1\}.$$

□

Corolário 16.2.1. Se a equação

$$ax \equiv b \bmod m$$

tem solução x_0, então as $d = \text{mdc}(a, m)$ soluções incongruentes são

$$x_0, x_1 = x_0 + \frac{m}{d}, \ldots, x_{d-1} = x_0 + \frac{m}{d}(d-1).$$

Exemplo. Encontre todas as soluções de $6x \equiv 3 \bmod 21$. Note que $\text{mdc}(6, 21) = 3|3$, logo pelo Lema (16.2) essa congruência tem exatamente 3 soluções incongruentes. Para encontrar uma delas, usamos o algoritmo de Euclides para a divisão

$$21 = 6 \cdot 3 + 3 \Rightarrow 3 = 21 \cdot 3 + 6 \cdot (-3),$$

logo $x_0 = -3$ é solução, e as demais são

$$x_1 = -3 + \frac{21}{3} = 4,$$
$$x_2 = -3 + \frac{21}{3} \cdot 2 = 11.$$

As soluções são $-3, 4, 11$.

Observe que poderíamos ter escolhido qualquer trio x_0^*, x_1^*, x_2^* com $x_0^* \in \overline{-3}, x_1^* \in \overline{4}$ e $x_2^* \in \overline{11}$. Então, vamos adotar como padrão apresentar soluções dentro de $\{0, 1, \ldots, m-1\}$ que já vimos ser SCR módulo m.

No caso acima, $m = 21$. Assim, vamos escolher

$$x_0 = -3 \equiv 18 \bmod 21.$$

Portanto, as soluções incongruentes são $4, 11$ e 18.

Observação 16.2. Sejam $a, m \in \mathbb{Z}, m \geq 2$ e assuma que $\text{mdc}(a, m) = 1$. Pelo Lema (16.2), a equação

$$ax \equiv 1 \bmod m$$

tem exatamente uma solução.

Definição. Sejam $a, m \in \mathbb{Z}, m \geq 2$ e $\text{mdc}(a, m) = 1$. A única solução x_0 de $ax \equiv 1 \bmod m$ é chamada de *inverso de a módulo m*, $x_0 = a^{-1}$.

Exemplo. Seja $m = 9$. No conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ os coprimos com 9 são $1, 2, 4, 5, 7$ e 8.

Assim, para $a \in \{1, 2, 4, 5, 7, 8\}$ queremos encontrar a^{-1}, i.e., a única solução de $ax \equiv 1 \bmod 9$. Temos

$$1 \cdot 1 \equiv 1 \bmod 9 \Rightarrow 1^{-1} = 1,$$

$$2 \cdot 5 \equiv 1 \bmod 9 \Rightarrow 2^{-1} = 5,$$

$$5 \cdot 2 \equiv 1 \bmod 9 \Rightarrow 5^{-1} = 2,$$

$$4 \cdot 7 \equiv 1 \bmod 9 \Rightarrow 4^{-1} = 7 \text{ e } 7^{-1} = 4,$$

$$8 \cdot 8 \equiv 1 \bmod 9 \Rightarrow 8^{-1} = 8.$$

Observação 16.3. Como vimos acima, alguns números podem ser inversos de si mesmos módulo m. Vamos determinar quais são eles quando m é primo. Note que isso equivale a determinar as soluções de

$$x^2 \equiv 1 \bmod m.$$

Lema 16.3. Seja $p \in \mathbb{P}$. As únicas soluções de

$$x^2 \equiv 1 \bmod p$$

são $x = 1$ e $x = p - 1$.

Demonstração. É bom lembrar que "únicas" sempre significa soluções incongruentes e como padrão estamos determinando soluções em $\{0, 1, \ldots, p-1\}$, que é SCR módulo p. Como devemos ter $\text{mdc}(x, p) = 1$, excluímos $x = 0$. Agora,

$$x^2 \equiv 1 \bmod p \Leftrightarrow p | x^2 - 1 \Leftrightarrow p | (x-1)(x+1) \Leftrightarrow x = -1 \text{ ou } x = 1, \text{ com } x \in \{1, 2, \ldots, p-1\}.$$

Como $-1 \equiv p - 1 \bmod p$, as soluções são 1 e $p - 1$. □

Exemplo. Seja $p = 11$. Vamos determinar todos os inversos de $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, um SCR módulo 11. Pelo Lema (16.3), temos $1^{-1} = 1$ e $10^{-1} = 10$. Agora

$$2 \cdot 6 \equiv 1 \bmod 11 \Rightarrow 2^{-1} = 6 \text{ e } 6^{-1} = 2,$$

$$3 \cdot 4 \equiv 1 \bmod 11 \Rightarrow 3^{-1} = 4 \text{ e } 4^{-1} = 3,$$

$$5 \cdot 9 \equiv 1 \bmod 11 \Rightarrow 5^{-1} = 9 \text{ e } 9^{-1} = 5,$$

$$7 \cdot 8 \equiv 1 \bmod 11 \Rightarrow 7^{-1} = 8 \text{ e } 8^{-1} = 7.$$

Exemplo. Qual o inverso de 335 módulo 11? Note que $\text{mdc}(335, 11) = 1$, então existe 335^{-1}. Agora, $335 \equiv 5 \bmod 11$ e, pelo exemplo anterior, $335^{-1} \equiv 5^{-1} \equiv 9$.

Teorema 16.4 (Wilson)**.** Seja $p \in \mathbb{P}$. Então, $(p-1)! \equiv -1 \bmod p$.

Demonstração. Temos $(p-1)! = 1 \cdots 2 \cdot 3 \cdots (p-2) \cdot (p-1)$. Pelo Lema (16.3), só temos $1^{-1} = 1$ e $(p-1)^{-1} = p-1$, logo $\forall a \in \{2, 3, \ldots, p-2\}, \exists! b \in \{2, 3, \ldots, p-2\}$ tal que $ab \equiv 1 \bmod p$, i.e., $a^{-1} = b$ e $a \neq b$. Portanto, podemos escrever

$$(p-1)! = 1 \cdot (p-1) \cdot 2 \cdot 2^{-1} \cdots (p-2)^{-1}(p-2) \equiv p-1 \equiv -1 \bmod p.$$

□

Exemplo. Para $p = 11$, temos a lista de inversos, logo

$$(p-1)! = 10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 1 \cdot 10 \cdot 2 \cdot 6 \cdot 3 \cdot 4 \cdot 5 \cdot 9 \cdot 7 \cdot 8 \equiv 10 \bmod 11.$$

Definição. Seja $m \in \mathbb{N}$. Defina $\phi(m)$ como *o número de elementos em* $\{1, 2, \ldots, m-1\}$ *que são coprimos com* m.

Exemplo. Seja $m = 12$. Então, $\phi(m) = 4$, pois $1, 5, 7$ e 11 são os únicos números coprimos com 12 em $\{1, 2, \ldots, 11\}$.

Lema 16.5. Seja $p \in \mathbb{N}$. Então, $p \in \mathbb{P} \Leftrightarrow \phi(p) = p - 1$.

Demonstração. Se $p \in \mathbb{P}$, então $\phi(p) = p-1$. Reciprocamente, se $\phi(p) = p-1$ então $\forall a, 1 < a \leq p-1$, $a \nmid p$. Logo, $p \in \mathbb{P}$. □

Lema 16.6. Seja $p \in \mathbb{P}$. Então toda lista com p inteiros consecutivos terá $p-1$ coprimos com p.

Demonstração. Seja $a \in \mathbb{Z}$ e escreva a lista

$$a, a+1, \ldots, a+(p-1).$$

Por Euclides, $a = pq + r, r \in \{0, 1, \ldots, p-1\}$ (se $a < 0$, tome $|a|$). Observe que $\exists! i_0 \in \{0, 1, \ldots, p-1\}$ tal que $r + i_0 = p$, i.e., $a + i_0 \equiv r + i_0 \equiv 0 \bmod p$, e segue que $\forall j \in \{0, 1, \ldots, p-1\}$, $j \neq i_0$, temos

$$a + j \equiv r + j \not\equiv 0 \bmod p \Leftrightarrow \text{mdc}(a + j, p) = 1 \text{ para } j \neq i_0,$$

ou seja, todos os elementos com exceção de $r + i_0$ são coprimos com p, totalizando $p-1$ elementos.

□

Exemplo. Considere a sequência $103, 104, 105, 106, 107, 108, 109$. Como $7 | 105$, temos $\text{mdc}(7, 103) = \cdots = \text{mdc}(7, 109) = 1$.

Lema 16.7. Seja $p \in \mathbb{P}$ e $m \in \mathbb{N}$. Então

$$\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1) = p^m\left(1 - \frac{1}{p}\right).$$

Demonstração. A sequência de inteiros entre 1 e p^m pode ser dividida em p^{m-1} subsequências de p elementos consecutivos.

$$\underbrace{1, 2, \ldots, p}_{p \text{ elementos}}, \overbrace{p+1, p+2, \ldots, 2p}^{p \text{ elementos}}, \ldots, \underbrace{p^{m-1}+1, p^{m-1}+2, \ldots, p^{m-1}+p}_{p \text{ elementos}}, \overbrace{p^m - p + 1, p^m - p + 2, \ldots, p^m}^{p \text{ elementos}}$$

Pelo Lema (16.6), em cada uma das subsequências existe um único elemento divisível por p. Logo, entre 1 e p^m há exatamente p^{m-1} elementos divisíveis por p e os demais são coprimos com p, resultando em $\phi(p^m) = p^m - p^{m-1}$. □

Exemplo. Seja $p = 3$. Vamos calcular $\phi(3^3)$. Escreva

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27.$$

Logo, $\phi(27) = 27 - 9 = 18$.

Definição. O conjunto $\{r_1, r_2, \ldots, r_t\}$ é um *sistema reduzido de resíduos módulo* m (SRR) se:

(i) $\text{mdc}(r_i, m) = 1$, para $1 \leq i \leq t$;

(ii) $r_i \not\equiv r_j \bmod m$ se $i \neq j$;

(iii) $\forall a \in \mathbb{Z}$, com $\text{mdc}(a, m) = 1$, existe r_i tal que

$$a \equiv r_i \bmod m.$$

Definição. Seja $m \in \mathbb{N}$ e defina $E(m) = \{l \in \mathbb{N} \mid 1 \leq l \leq m-1, \text{mdc}(m, l) = 1\}$.

Observação 16.4. Segue das definições que $\phi(m) = |E(m)|$.

Exemplo. $E(15) = \{1, 2, 4, 7, 8, 11, 13, 14\} \Rightarrow \phi(15) = |E(15)| = 8$.

Lema 16.8. Sejam $a, m \in \mathbb{Z}, m \geq 2$ e $\text{mdc}(a, m) = 1$. Então, se $b \in \overline{a}, \text{mdc}(b, m) = 1$.

Demonstração. Seja $d = \text{mdc}(b, m)$. Como $b \in \overline{a}$, temos $b = a + mt$. Como $d|b$ e $d|m$, segue que $d|a$. Logo, $d|\text{mdc}(a, m)$, i.e., $d = 1$. □

Lema 16.9. Seja $m \in \mathbb{N}, m \geq 2$. Então $E(m)$ é SRR módulo m.

Demonstração. Como $E(m) \subset \{0, 1, \ldots, m-1\}$ (e esse último conjunto é SCR módulo m), segue que os elementos de $E(m)$ são incongruentes dois a dois módulo m (Lema (15.10)). Por definição, os elementos de $E(m)$ são coprimos com m. Então, seja $a \in \mathbb{Z}$, com $\text{mdc}(a, m) = 1$. Segue do Lema (15.10) que $\exists r \in \{0, 1, \ldots, m-1\}$ tal que $a \equiv r \bmod m$. Do Lema (16.8), temos $\text{mdc}(r, m) = 1$, logo $r \in E(m)$. □

Lema 16.10. Seja $m \in \mathbb{N}, m \geq 2$, e $E(m) = \{r_1, r_2, \ldots, r_{\phi(m)}\}$. Se $\{a_1, a_2, \ldots, a_s\}$ é SRR módulo m, então

(i) $s = \phi(m)$;

(ii) após reordenação de índices,

$$a_1 \in \overline{r_1}, a_2 \in \overline{r_2}, \ldots, a_{\phi(m)} \in \overline{r}_{\phi(m)}.$$

Demonstração. A demonstração é análoga à do Lema (15.12), pois se $b \in \mathbb{Z}$ e $\text{mdc}(b, m) = 1$, então $b \in \overline{r}_1 \cup \cdots \cup \overline{r}_{\phi(m)}$. □

Lema 16.11. Sejam $r_1, r_2, \ldots, r_{\phi(m)} \in \mathbb{Z}$ distintos, com $\text{mdc}(r_j, m) = 1$. Se $r_i \not\equiv r_j \bmod m$ para $i \neq j$, então $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ é SRR módulo m.

Demonstração. Segue a demonstração do Lema (15.13), utilizando o Lema (16.10). □

Lema 16.12. Seja $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ um SRR módulo m e seja $a \in \mathbb{Z}$, com $\text{mdc}(a, m) = 1$. Então $\{ar_1, \ldots, ar_{\phi(m)}\}$ é SRR módulo m.

Demonstração. Segue a demonstração do Lema (15.14), usando o Lema (16.11). □

Lema 16.13 (Euler)**.** Seja $m \in \mathbb{N}, m \geq 2$, e $a \in \mathbb{Z}, \text{mdc}(a, m) = 1$. Então,

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

Demonstração. Seja $a \in \mathbb{Z}, \text{mdc}(a, m) = 1$, e seja $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ um SRR módulo m. Pelo Lema (16.12), $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ também é. Logo, $\forall i \in \{1, 2, \ldots, \phi(m)\}, \exists! j \in \{1, 2, \ldots, \phi(m)\}$ tal que $ar_i \equiv r_j \bmod m$. Portanto

$$\begin{aligned} ar_1 \cdot ar_2 \cdots ar_{\phi(m)} &\equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \bmod m \\ \Leftrightarrow a^{\phi(m)} r_1 \cdot r_2 \cdots r_{\phi(m)} &\equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \bmod m. \end{aligned}$$

Como $\text{mdc}(r_i, m) = 1$, segue que $\text{mdc}(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$ e, do Lema (15.8), $a^{\phi(m)} \equiv 1 \bmod m$. □

Lema 16.14. Sejam $m, n \in \mathbb{N}, \text{mdc}(m, n) = 1$. Então, $\phi(mn) = \phi(m)\phi(n)$.

Demonstração. A ideia da demonstração é construir um conjunto com $\phi(m)\phi(n)$ elementos que seja SRR módulo mn, de modo que o Lema (16.10) garanta que $\phi(mn) = \phi(m)\phi(n)$.

Sejam $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ e $\{s_1, s_2, \ldots, s_{\phi(n)}\}$ dois SRR's módulo m e n, respectivamente. Defina

$$\mathcal{B} = \{nr_j + ms_i \mid 1 \leq j \leq \phi(m), 1 \leq i \leq \phi(n)\},$$

e seja $\alpha_{ij} = nr_i + ms_j$.

Afirmação 1: $\text{mdc}(\alpha_{ij}, mn) = 1$

Sejam $d_m = \text{mdc}(\alpha_{ij}, m)$ e $d_n = \text{mdc}(\alpha_{ij}, n)$. Temos que $d_m | \alpha_{ij} - s_j$, logo $d_m | nr_i$. Como $\text{mdc}(m, n) = 1$, segue que $d_m | r_i$, logo $d_m | \text{mdc}(r_i, m)$. Mas os r_i's são SRR módulo m, logo $\text{mdc}(r_i, m) = 1$ e $d_m = 1$. Analogamente, temos $d_n = 1$. Logo, como $\text{mdc}(m, n) = 1$, segue que $\text{mdc}(\alpha_{ij}, mn) = 1$.

Afirmação 2: $\alpha_{ij} \not\equiv \alpha_{uv} \bmod mn$ se $i \neq u$ ou $j \neq v$

Temos

$$\alpha_{ij} \equiv \alpha_{uv} \bmod mn \Leftrightarrow nr_i + ms_j \equiv nr_u + ms_v \bmod mn \Leftrightarrow n(r_i - r_u) \equiv m(s_v - s_j) \bmod mn.$$

Em particular, $n(r_i - r_u) \equiv 0 \bmod m$ e $m(s_v - s_j) \equiv 0 \bmod n$. Como $\text{mdc}(m, n) = 1$, temos

$$r_i - r_u \equiv 0 \bmod m \text{ e } s_v - s_j \equiv 0 \bmod n,$$

logo $i = u$ e $v = j$, pois os r_i's e s_j's formam SRR's módulo m e n, respectivamente.

Afirmação 3: $\forall a \in \mathbb{Z}, \text{mdc}(a, mn) = 1$, então $a \equiv \alpha_{ij} \bmod mn$, para algum par i, j.

Seja $a \in \mathbb{Z}$, $\text{mdc}(a, mn) = 1$. Como $\text{mdc}(m, n) = 1$, existem $x_0, y_0 \in \mathbb{Z}$ tais que $x_0 m + y_0 n = 1$. Logo, $xm + yn = a$, com $x = ax_0$ e $y = ay_0$. Como $\text{mdc}(a, m) = 1 = \text{mdc}(a, n)$, então necessariamente $\text{mdc}(x, n) = 1 = \text{mdc}(y, m)$. Logo, existem r_i e s_j tais que

$$\begin{gathered} x \equiv s_j \bmod n \text{ e } y \equiv r_i \bmod m \\ \Rightarrow mx \equiv ms_j \bmod mn \text{ e } ny \equiv nr_i \bmod mn, \end{gathered}$$

ou seja,

$$a = xm + yn \equiv ms_j + nr_i \equiv \alpha_{ij} \bmod mn.$$

Portanto, $\mathcal{B}$ é SRR módulo mn, possuindo então $\phi(mn)$ elementos. Mas por construção $|\mathcal{B}| = \phi(m)\phi(n)$, logo $\phi(mn) = \phi(m)\phi(n)$. □

Teorema 16.15. Seja $n \in \mathbb{N}$. Então

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Demonstração. Escreva $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Pelo Lema (16.14), temos

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{\alpha_i}).$$

Pelo Lema (16.7),

$$\begin{aligned}\phi(n) &= \prod_{i=0}^{r} p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)\\ &= \left(\prod_{i=1}^{r} p_i^{\alpha_i}\right)\left(\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\right)\\ &= n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).\end{aligned}$$

□

Exemplo. $\phi(1200) = \phi(2^4\cdot 3\cdot 5^2) = \phi(2^4)\phi(3)\phi(5^2) = 2^3(2-1)2\cdot 5(5-1) = 320.$

Lema 16.16. Sejam $n \in \mathbb{N}$ e $D(n) = \left\{d \in \mathbb{N} \;\middle|\; d|n\right\}$. Então,

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

Demonstração. Sejam $S_n = \{1,2,\ldots,n\}$ e $T_d = \{a \in S_n \mid \text{mdc}(a,n) = d\}$, para todo $d \in D(n)$. Observe que se $d_1, d_2 \in D(n)$ e $d_1 \neq d_2$, então $T_{d_1} \cap T_{d_2} = \varnothing$ (porque nenhum número pode ter dois mdc's distintos com um dado número). Escreva $D(n) = \{d_1, d_2, \ldots, d_r\}$, $1 < d_1 < \cdots < d_r = n$. Assim, S_n é dado pela união disjunta dos T_{d_i}, logo

$$n = |S_n| = |T_{d_1}| + \cdots + |T_{d_r}|.$$

Observe que

$$T_d \subseteq \left\{d, 2d, \ldots, \left(\frac{n}{d}\right)d\right\}.$$

Por outro lado,

$$\lambda d \in T_d \Leftrightarrow \text{mdc}(\lambda d, n) = d \Leftrightarrow \text{mdc}\left(\lambda, \frac{n}{d}\right) = 1,$$

logo

$$T_d = \left\{\lambda d \mid 1 \leq \lambda \leq \frac{n}{d} \text{ e } \text{mdc}\left(\lambda, \frac{n}{d}\right) = 1\right\},$$

e portanto

$$|T_d| = \phi\left(\frac{n}{d}\right) \Rightarrow n = |S_n| = \sum_{d\in D(n)} \phi\left(\frac{n}{d}\right) = \sum_{d\in D(n)} \phi\left(d\right)$$

pois $\dfrac{n}{d}$ apenas reordena $D(n)$. □

Exemplo. Seja $n = 20$. Daí, $S_{20} = \{1, 2, \ldots, 20\}$, $D(20) = \{1, 2, 4, 5, 10, 20\}$ e o conjunto dos $\frac{n}{d}$'s é $\{20, 10, 5, 4, 2, 1\}$. Temos

$$\begin{aligned}
T_1 &= \{1, 3, 7, 9, 11, 13, 17, 19\} \Rightarrow |T_1| = 8 = \phi(20),\\
T_2 &= \{2, 6, 14, 18\} \Rightarrow |T_2| = 4 = \phi(20/2) = \phi(10),\\
T_4 &= \{4, 8, 12, 16\} \Rightarrow |T_4| = 4 = \phi(5),\\
T_5 &= \{5, 15\} \Rightarrow |T_5| = 2 = \phi(4),\\
T_{10} &= \{10\} \Rightarrow |T_{10}| = 1 = \phi(2),\\
T_{20} &= \{20\} \Rightarrow |T_{20}| = 1 = \phi(1).
\end{aligned}$$

Agora, $\phi(1) + \phi(2) + \phi(4) + \phi(5) + \phi(10) + \phi(20) = 1 + 1 + 2 + 4 + 4 + 8 = 20$.

Lema 16.17. Sejam $m, n \in \mathbb{N}$ e $d = \text{mdc}(m, n)$. Então

$$\phi(mn) = \frac{d\phi(m)\phi(n)}{\phi(d)}.$$

Demonstração. Escreva

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s} \text{ e } n = p_1^{\delta_1} \cdots p_r^{\delta_r} Q_1^{\gamma_1} \cdots Q_t^{\gamma_t}$$

com $p_1, \ldots, p_r, q_1, \ldots, q_s, Q_1, \ldots, Q_t$ primos distintos. Logo,

$$d = \text{mdc}(m, n) = p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r}, \text{ com } \varepsilon_j = \min\{\alpha_j, \delta_j\}, 1 \leq j \leq r.$$

Pelo teorema sobre a função ϕ de Euler, temos que

$$\phi(d) = d \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \Leftrightarrow \frac{\phi(d)}{d} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Pelo mesmo teorema, também temos

$$\phi(mn) = mn \cdot \left[\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)\right] \cdot \left[\prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right)\right] \cdot \left[\prod_{k=1}^{t} \left(1 - \frac{1}{Q_k}\right)\right].$$

Por outro lado,

$$\begin{aligned}
\phi(m)\phi(n) &= mn \cdot \left[\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)\right]^2 \cdot \left[\prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right)\right] \cdot \left[\prod_{k=1}^{t} \left(1 - \frac{1}{Q_k}\right)\right]\\
&= \frac{\phi(d)}{d}\phi(mn)\\
&\Leftrightarrow \phi(mn) = \frac{d\phi(m)\phi(n)}{\phi(d)}.
\end{aligned}$$

□

Exemplo. Sejam $m = 15$ e $n = 25$. Logo, $\text{mdc}(m, n) = 5$. Portanto, $\phi(mn) = \phi(15 \cdot 25) = \frac{5\phi(15)\phi(25)}{\phi(5)} = \frac{5 \cdot 8 \cdot 20}{4} = 200$.

Exemplo. Determine todos os valores de $n \in \mathbb{N}$ tais que $\phi(n)|n$.

Temos que $\phi(1) = 1, \phi(2) = 1$, logo $\phi(1)|1$ e $\phi(2)|2$. Assuma $n \geq 3$. Escreva $n = 2^a p_1^{b_1} \cdots p_r^{b_r}$, com $p_1, \ldots, p_r$ primos ímpares distintos.

Caso 1: $a = 0$ Nesse caso, o teorema sobre a função ϕ nos diz que

$$\phi(n) = p_1^{b_1-1} \cdots p_r^{b_r-1}(p_1 - 1) \cdots (p_r - 1)$$

logo

$$\frac{n}{\phi(n)} = \frac{p_1 \cdots p_r}{(p_1 - 1) \cdots (p_r - 1)}.$$

Como os p_i's são ímpares, então 2 não divide o numerador; por outro lado, o denominador é par, logo $\phi(n) \nmid n$.

Caso 2: $a \geq 1$ Nesse caso, $\phi(n) = 2^{a-1} p_1^{b_1-1} \cdots p_r^{b_r-1}(p_1 - 1) \cdots (p_r - 1)$, logo

$$\frac{n}{\phi(n)} = \frac{2p_1 \cdots p_r}{(p_1 - 1) \cdots (p_r - 1)}.$$

Se $r \geq 2$, i.e., há pelo menos dois primos distintos, então $4|(p_1 - 1) \cdots (p_r - 1)$ mas $4 \nmid 2p_1 \cdots p_r$, logo $\phi(n) \nmid n$.

Se $r = 1$, então temos $\dfrac{n}{\phi(n)} = \dfrac{2p_1}{p_1 - 1}$. Se $\phi(n)|n$, então $p_1 - 1|2p_1$. Como $\text{mdc}(p_1 - 1, p_1) = 1$, segue que $p_1 - 1|2$, i.e., $p_1 = 3$. Portanto,

$$\phi(n)|n \Leftrightarrow n \in \left\{1, 2^a, 2^a \cdot 3^b\right\}, \text{ com } a, b \in \mathbb{N}.$$

Definição. Sejam $a_1, \ldots, a_r \in \mathbb{Z}$. Diremos que $d \in \mathbb{N}$ é o $\text{mdc}(a_1, \ldots, a_r)$ se

(i) $d|a_1, \ldots, d|a_r$;

(ii) se $d^*|a_1, \ldots, d^*|a_r$, então $d^* \leq d$.

Lema 16.18. Se chamarmos $d = \text{mdc}(a_1, a_2, \ldots, a_r)$, então existem $x_1, x_2, \ldots, x_r \in \mathbb{Z}$ tais que

$$d = x_1 a_1 + \cdots x_r a_r.$$

Demonstração. A demonstração é essencialmente a mesma do Lema (3.2). Escreva

$$S = \{a_1 y_1 + \cdots + a_r y_r \mid y_1, \ldots, y_r \in \mathbb{Z}\}$$

e defina

$$S_+ = \{s \in S \mid s \in \mathbb{N}\}.$$

Pelo PBO, existe d_0 o menor elemento de S_+. Logo, $d_0 = x_1a_1 + \cdots x_ra_r$.

Seja $a_j \in \{a_1, \ldots, a_r\}$ qualquer e escreva $a_j = d_0q + r$, com $0 \leq r < d_0$. Se $r = 0$, $d_0|a_j$. Se $r > 0$, escreva

$$r = a_j - d_0q = a_j - (x_1a_1 + \cdots x_ra_r)q \in S$$

e, como $r > 0$, então $r \in S_+$. Mas isso é absurdo, pois implica $r < d_0$, contrariando o PBO. Logo, d_0 é divisor comum de $a_1, \ldots, a_r$. Observe que se d^* é divisor comum de $a_1, \ldots, a_r$, então $d^*|x_1a_1 + \cdots x_ra_r$, i.e., $d^*|d_0$. Portanto, $d_0 = \text{mdc}(a_1, \ldots, a_r)$. □

Corolário 16.18.1. Se d^* é divisor comum de $a_1, \ldots, a_r$, então d^* divide $\text{mdc}(a_1, \ldots, a_r)$.

Definição. Sejam $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. Dizemos que $M \in \mathbb{N}$ é o $\text{mmc}(a_1, \ldots, a_r)$ se

(i) $a_1|M, \ldots, a_r|M$;

(ii) se $a_1|M^*, \ldots, a_r|M^*$, então $M \leq M^*$.

Lema 16.19. Sejam $a_1, a_2, \ldots, a_r \in \mathbb{N}$ e escreva

$$a_j = p_1^{\alpha_1(j)}p_2^{\alpha_2(j)}\cdots p_n^{\alpha_n(j)}, \text{ com } \alpha_i(j) \in \mathbb{N} \cup \{0\}, 1 \leq i \leq n \text{ e } 1 \leq j \leq r.$$

Então

$$\text{mdc}(a_1, \ldots, a_r) = p_1^{\varepsilon_1}p_2^{\varepsilon_2}\cdots p_n^{\varepsilon_n}$$

e

$$\text{mmc}(a_1, \ldots, a_r) = p_1^{\delta_1}p_2^{\delta_2}\cdots p_n^{\delta_n}$$

com

$$\varepsilon_j = \min\{\alpha_j(1), \alpha_j(2), \ldots, \alpha_j(r)\} \text{ e } \delta_j = \max\{\alpha_j(1), \alpha_j(2), \ldots, \alpha_j(r)\}, \text{ com } 1 \leq j \leq r.$$

Demonstração. Pelo Lema (8.3), sabemos que $d = p_1^{\varepsilon_1}\cdots p_n^{\varepsilon_n}|a_j, 1 \leq j \leq r$. Se $d^*|a_j, 1 \leq j \leq r$, então $d^* = p_1^{t_1(j)}\cdots p_n^{t_n(j)}$, com $t_i(j) \leq \alpha_i(j)$ para todo $1 \leq i \leq n$ e $1 \leq j \leq r$. Logo, $t_i(j) \leq \varepsilon_j$ para todo j, e portanto, $d^*|d$. Por definição, segue que $d = \text{mdc}(a_1, \ldots, a_r)$.

Também do Lema (8.3), temos que $a_j|m = p_1^{\delta_1}\cdots p_n^{\delta_n}, 1 \leq j \leq r$. Seja m^* um múltiplo comum de $a_1, \ldots, a_r$, i.e., $a_j|m^*$ para todo $1 \leq j \leq r$. Logo,

$$m^* = \lambda_ja_j = \lambda_jp_1^{\alpha_1(j)}p_2^{\alpha_2(j)}\cdots p_n^{\alpha_n(j)}, 1 \leq j \leq r.$$

Em particular, como todos os a_j's dividem m^*, então $p_i^{\delta_i}|m^*$ para todo $1 \leq i \leq n$. Logo, $m|m^*$ e, por definição, $m = \text{mmc}(a_1, \ldots, a_r)$. □

Observação 16.5. Segue desse lema que podemos calcular tanto o mdc quanto o mmc de forma indutiva, i.e.,

$$\text{mdc}(a_1, a_2, \ldots, a_r) = \text{mdc}(a_1, \text{mdc}(a_2, \ldots, a_r))$$

e

$$\text{mmc}(a_1, a_2, \ldots, a_r) = \text{mmc}(a_1, \text{mmc}(a_2, \ldots, a_r)).$$

Exemplo. $\text{mdc}(20, 30, 35, 40) = \text{mdc}(20, \text{mdc}(30, 35, 40)) = \text{mdc}(20, \text{mdc}(30, \text{mdc}(35, 40))) = \text{mdc}(20, \text{mdc}(30, 5)) = \text{mdc}(20, 5) = 5$.

Teorema 16.20 (Resto Chinês)**.** Sejam $m_1, m_2, \ldots, m_r \in \mathbb{N}$ com $\text{mdc}(m_i, m_j) = 1, \forall i, j$ com $1 \leq i \leq j \leq r$. Sejam $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ tais que $\text{mdc}(a_i, m_i) = 1$, com $1 \leq i \leq r$ e sejam $b_1, \ldots, b_r \in \mathbb{Z}$ quaisquer. Então o sistema

$$\begin{cases} a_1 x & \equiv b_1 \bmod m_1 \\ a_2 x & \equiv b_2 \bmod m_2 \\ & \vdots \\ a_r x & \equiv b_r \bmod m_r \end{cases}$$

tem solução única módulo $m_1 \cdot m_2 \cdots m_r$.

Demonstração. Essa demonstração tem duas partes: a prova da existência e a prova da unicidade módulo $m_1 \cdot m_2 \cdots m_r$.

(i) Unicidade: suponha x_0 e x_1 soluções do sistema. Em particular, temos que

$$a_i x_0 \equiv b_i \equiv a_i x_1 \bmod m_i, 1 \leq i \leq r.$$

Como $\text{mdc}(a_i, m_i) = 1$, segue que

$$x_0 \equiv x_1 \bmod m_i, \forall i, 1 \leq i \leq r.$$

Como $\text{mdc}(m_i, m_j) = 1$ se $i \neq j$, segue que

$$x_0 \equiv x_1 \bmod m_1 \cdot m_2 \cdots m_r.$$

(ii) Existência: como $\text{mdc}(a_i, m_i) = 1$, cada equação tem exatamente uma solução, pelo Lema (16.2). Sejam $x_1, x_2, \ldots, x_r$ as soluções individuais de cada equação. Defina, para $1 \leq i \leq r$,

$$n_i = \frac{m_1 \cdot m_2 \cdots m_r}{m_i} \Rightarrow \text{mdc}(n_i, m_i) = 1 \text{ e } \text{mdc}(n_i, m_j) = m_j, i \neq j.$$

Pelo Lema (16.2), cada uma das equações

$$n_i z \equiv 1 \bmod m_i, 1 \leq i \leq r$$

admite solução única. Sejam $z_1, \ldots, z_r$ as soluções únicas e individuais de cada equação. Agora, defina

$$x_0 = x_1 n_1 z_1 + \cdots + x_r n_r z_r.$$

Observe que, para todo $1 \leq i \leq r$, tem-se

$$\begin{aligned} a_i x_0 &\equiv a_i x_1 n_1 z_1 + \cdots + a_i x_i n_i z_i + \cdots + a_i x_r n_r z_r \\ &\equiv a_i x_i n_i z_i \\ &\equiv a_i x_i \\ &\equiv b_i \bmod m_i, \end{aligned}$$

pois $m_i | n_j$ se $i \neq j$ e $n_i z_i \equiv 1 \bmod m_i$, ou seja, x_0 é solução do sistema. □

Observação 16.6. Esta demonstração nos dá um algoritmo de como encontrar a solução do sistema. Vamos ilustrar esse processo com um exemplo.

Exemplo. Encontre soluções para o seguinte sistema:

$$\begin{cases} 3x \equiv 2 \bmod 7 \\ 5x \equiv 3 \bmod 9 \\ 8x \equiv 7 \bmod 11 \end{cases}.$$

Temos que $\text{mdc}(7,9) = \text{mdc}(7,11) = \text{mdc}(9,11) = 1$ e $\text{mdc}(3,7) = \text{mdc}(5,9) = \text{mdc}(8,11) = 1$. Pelo Teorema do Resto Chinês, esse sistema tem solução única módulo $693 (= 7 \cdot 9 \cdot 11)$.

(a) Soluções das equações individuais: como os números são pequenos, podemos obter as soluções diretamente:

$$x_1 = 3, x_2 = 6, x_3 = 5.$$

(b) Valores dos n_i's:

$$n_1 = \frac{7 \cdot 9 \cdot 11}{7} = 99, n_2 = 77, n_3 = 63.$$

(c) Soluções das equações $n_i z \equiv 1 \bmod m_i$:

$$99z \equiv 1 \bmod 7 \Rightarrow z \equiv 1 \bmod 7 \Rightarrow z_1 = 1,$$

$$77z \equiv 1 \bmod 9 \Rightarrow 5z \equiv 1 \bmod 9 \Rightarrow z_2 = 2,$$

$$63z \equiv 1 \bmod 11 \Rightarrow 8z \equiv 1 \bmod 11 \Rightarrow z_3 = 7.$$

(d) Solução do sistema:

$$x_0 = 3 \cdot 99 \cdot 1 + 6 \cdot 77 \cdot 2 + 5 \cdot 63 \cdot 7 = 3426$$

e

$$3426 \equiv 654 \bmod 693 \Rightarrow x_0 = 654.$$

Vamos concluir testando essa solução

$$3 \cdot 654 \equiv 3 \cdot 3 \equiv 2 \bmod 7,$$

$$5 \cdot 654 \equiv 5 \cdot 6 \equiv 3 \bmod 9,$$

$$8 \cdot 654 \equiv 8 \cdot 5 \equiv 7 \bmod 11.$$

Exemplo. Encontre um natural que deixa restos $3, 2$ e 5 nas divisões por $5, 8$ e 11, respectivamente.

Encontrar esse número é equivalente a determinar uma solução para o sistema

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 8 \\ x \equiv 5 \bmod 11 \end{cases}.$$

Nesse caso, já temos as soluções individuais de cada equação:

$$x_1 = 3, x_2 = 2, x_3 = 5.$$

Agora,

$$n_1 = 88, n_2 = 55 \text{ e } n_3 = 40$$

e as equações

$$88z \equiv 1 \bmod 5 \Rightarrow 3z \equiv 1 \bmod 5 \Rightarrow z_1 = 2,$$

$$55z \equiv 1 \bmod 8 \Rightarrow 7z \equiv 1 \bmod 8 \Rightarrow z_2 = 7,$$

$$40z \equiv 1 \bmod 11 \Rightarrow 7z \equiv 1 \bmod 11 \Rightarrow z_3 = 8,$$

de modo que a solução do sistema é

$$x_0 = 3 \cdot 88 \cdot 2 + 2 \cdot 55 \cdot 7 + 5 \cdot 40 \cdot 8 = 528 + 770 + 1600 = 2898.$$

Como $5 \cdot 8 \cdot 11 = 440$, procuramos

$$x_0 \equiv 2898 \equiv 258 \bmod 440.$$

Testando

$$\begin{cases} 258 \equiv 3 \bmod 5 \\ 258 \equiv 2 \bmod 8 \\ 258 \equiv 5 \bmod 11 \end{cases}.$$

A seguir veremos uma aplicação interessante do Teorema do Resto Chinês.

Teorema 16.21. Seja $m \in \mathbb{N}$ e escreva $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. A congruência

$$f(x) = a_x x^n + \cdots + a_1 x + a_0 \equiv 0 \bmod m$$

tem solução se, e somente se, o sistema

$$\begin{cases} f(x) & \equiv 0 \bmod p_1^{\alpha_1} \\ & \vdots \\ f(x) & \equiv 0 \bmod p_r^{\alpha_r} \end{cases}$$

tem solução.

Demonstração. A demonstração é uma generalização do Lema (7.5). Se $f(a) \equiv 0 \bmod m$, então $m | f(a)$, ou seja, $p_i^{\alpha_i} | f(a)$ para todo $1 \leq i \leq r$. Em particular,

$$f(a) \equiv 0 \bmod p_i^{\alpha_i}, \forall i, 1 \leq i \leq r.$$

Por outro lado, se $f(a) \equiv 0 \bmod p_i^{\alpha_i}$ para todo $1 \leq i \leq r$, então $p_1^{\alpha_1} | f(a), p_2^{\alpha_2} | f(a), \ldots, p_r^{\alpha_r} | f(a)$. Mas $\text{mdc}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ se $i \neq j$. Logo

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} | f(a) \Rightarrow m | f(a) \Rightarrow f(a) \equiv 0 \bmod m.$$

□

Para encontrar uma solução para o sistema acima, podemos usar o Teorema do Resto Chinês da seguinte forma.

Sejam $\beta_1, \ldots, \beta_r \in \mathbb{Z}$ tais que $f(\beta_i) \equiv 0 \bmod p_i^{\alpha_i}, 1 \leq i \leq r$. Pelo Teorema do Resto Chinês, determinamos $k_0 \in \mathbb{N}$ tal que

$$\begin{cases} x_0 & \equiv \beta_1 \bmod p_1^{\alpha_1} \\ & \vdots \\ x_0 & \equiv \beta_r \bmod p_r^{\alpha_r} \end{cases}.$$

Segue dos Lemas (15.2) e (15.3) que

$$f(x_0) \equiv f(\beta_i) \equiv 0 \bmod p_i^{\alpha_i}$$

portanto, pelo Teorema acima,

$$f(x_0) \equiv 0 \bmod m.$$

Exemplo. Verifique se a congruência abaixo tem solução:

$$f(x) = x^3 - 4x^2 + 5x - 6 \equiv 0 \bmod 63.$$

Inicialmente, escreva $63 = 7 \cdot 3^2$ e observe que $f(4) \equiv 0 \bmod 7$ e $f(3) \equiv 0 \bmod 9$. Pelo Teorema do Resto Chinês,

$$\begin{cases} x \equiv 4 \bmod 7 \\ x \equiv 3 \bmod 9 \end{cases} \quad \text{tem solução.}$$

Escreva $x_1 = 4, x_2 = 3, n_1 = 9, n_2 = 7$. Como

$$9z \equiv 1 \bmod 7 \Rightarrow z_1 = 4,$$
$$7z \equiv 1 \bmod 9 \Rightarrow z_2 = 4,$$

temos que

$$x_0 = 4 \cdot 9 \cdot 4 + 3 \cdot 7 \cdot 4 = 228 \equiv 39 \bmod 63.$$

Portanto,

$$f(39) \equiv 0 \bmod 63.$$

Vamos apresentar um método para encontrar soluções módulo p^{m+1} a partir de soluções módulo p.

Seja $f(x) = a_n x_n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, com coeficientes inteiros. Agora,

$$(b + tp^r)^k = b^k + kb^{k-1} \cdot tp^r + \binom{k}{2} b^{k-2} \cdot (tp^r)^2 + \cdots + \binom{k}{k-1} b(tp^r)^{k-1} + (tp^r)^k,$$

logo

$$(b + tp^r)^k \equiv b^k + kb^{k-1} \cdot tp^r \bmod p^{r+1}.$$

Portanto, como

$$f(b + tp^r) = a_n(b + tp^r)^n + a_{n-1}(b + tp^r)^{n-1} + \cdots + a_1(b + tp^r) + a_0$$

temos que

$$\begin{aligned} f(b + tp^r) &\equiv \left(a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0\right) + \left(na_n b^{n-1} + (n-1)a_{n-1}b^{n-2} + \cdots + a_1\right) tp^r \\ &\equiv f(b) + f'(b) \cdot tp^r \bmod p^{r+1} \end{aligned}$$

com

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \text{ (a derivada!)}$$

Lema 16.22 (Hensel)**.** Seja $f(x)$ um polinômio com coeficientes inteiros e suponha que existe $b \in \mathbb{Z}$ tal que $f(b) \equiv 0 \bmod p^r$ e $f'(b) \not\equiv 0 \bmod p$. Então existe um único $t \in \mathbb{Z}$ (módulo p) tal que

$$f(b + tp^r) \equiv 0 \bmod p^{r+1}.$$

Demonstração. Escreva $f(b) = B \cdot p^r$ e $f'(b) = A$. Sabemos que

$$f(b + tp^r) \equiv B \cdot p^r + A \cdot tp^r \bmod p^{r+1}.$$

Assim, encontrar $t \in \mathbb{Z}$ tal que

$$Bp^r + Ap^r t \equiv 0 \bmod p^{r+1}$$

é equivalente a determinar uma solução para

$$B + At \equiv 0 \bmod p,$$

ou seja, uma solução para $At \equiv -B \bmod p$. Pelo Lema (16.2), essa congruência tem solução pois por hipótese $\mathrm{mdc}(A, p^r) = 1$, e a solução é única módulo p. □

Exemplo. Resolva a equação

$$x^2 + x + 47 \equiv 0 \bmod 7^3.$$

Escreva $f(x) = x^2 + x + 47$ e observe que $f(1) = f(5) \equiv 0 \bmod 7$. Note que $f'(x) = 2x + 1$ e $f'(1) \not\equiv 0 \bmod 7$ e $f'(5) \not\equiv 0 \bmod 7$. Assim, podemos aplicar o Lema de Hensel em qualquer uma das soluções. Vamos aplicar na solução 5, então $f(5) = 77 = 7 \cdot 11$ e $f'(5) = 11$.

Vamos determinar t tal que $f(5 + 7t) \equiv 0 \bmod 7^2$. Isso é equivalente a encontrar uma solução para

$$11 + 11t \equiv 0 \bmod 7 \Rightarrow t = -1.$$

Escolha $a_1 = 5 + 7(-1) = -2$ e observe que

$$f(-2) = 49 \equiv 0 \bmod 7^2 \text{ e } f'(-2) = -3 \not\equiv 0 \bmod 7.$$

Podemos aplicar novamente o Lema de Hensel e buscar t tal que $f(-2 + t \cdot 7^2) \equiv 0 \bmod 7^3$. Isso é equivalente a resolver

$$1 - 3t \equiv 0 \bmod 7 \Rightarrow t = 5.$$

Tome $a_2 = -2 + 5 \cdot 7^2 = 243$. Agora,

$$f(243) = 59339 = 7^3 \cdot 173 \Rightarrow f(243) \equiv 0 \bmod 7^3.$$

Observação 16.7. Analisando o exemplo acima, note que com $a = 5$ temos $f(a) \equiv 0 \bmod 7$. Depois, determinamos $t_0 = -1$ tal que

$$a_1 = a + t_0 \cdot 7 = 5 + (-1) \cdot 7$$

e $f(a_1) \equiv 0 \bmod 7^2$. Em seguida, determinamos $t_1 = 5$ tal que

$$a_2 = a_1 + t_1 \cdot 7^2 = -2 + 5 \cdot 7^2 = 243$$

e $f(a_2) \equiv 0 \bmod 7^3$.

Agora, $a_2 = a_1 + t_1 \cdot 7^2 = a + t_0 \cdot 7 + t_1 \cdot 7^2$. Como $f'(x)$ é também um polinômio com coeficientes inteiros e $(a + tp)^k \equiv a^k \bmod p$, segue que se $f'(a) \not\equiv 0 \bmod p$ então $f'(a + t_0 \cdot p) \not\equiv 0 \bmod p^2$ e em geral

$$f'(a + t_0 \cdot p + \cdots + t_r \cdot p^{r+1}) \equiv f'(a) \equiv 0 \bmod p.$$

Logo, se $f(a) \equiv 0 \bmod p^r$ e $f'(a) \not\equiv 0 \bmod p$, sempre teremos solução para $f(x) \equiv 0 \bmod p^{r+m} \forall m \in \mathbb{N}$ e a solução terá a forma

$$a_{m-1} = a + t_0 \cdot p + \cdots + t_{m-2} \cdot p^{m-1}$$

pois $f'(a_{m-2}) \equiv f'(a_{m-3}) \equiv \cdots \equiv f'(a_1) \equiv f'(a) \not\equiv 0 \bmod p$. Com isso, provamos o teorema:

Teorema 16.23 (Hensel)**.** Seja $f(x)$ um polinômio com coeficientes inteiros. Se existe $a \in \mathbb{Z}$ tal que $f(a) \equiv 0 \bmod p$ e $f'(a) \not\equiv 0 \bmod p$, p primo, então para todo $m \in \mathbb{N}$

$$f(x) \equiv 0 \bmod p^m$$

tem solução.

17 Exercícios Resolvidos

Exercício 17. Mostre que se $a, b \in \mathbb{Z}$ são tais que $\text{mdc}(ab, 91) = 1$, então $91 | a^{12} - b^{12}$.

Solução. Como $91 = 7 \cdot 13$, basta mostrarmos que 7 e 13 dividem essa diferença. Como $\text{mdc}(ab, 91) = 1$, então $\text{mdc}(a, 7) = \text{mdc}(b, 7) = 1 = \text{mdc}(a, 13) = \text{mdc}(b, 13)$. Por Euler, segue que

$$a^6 \equiv 1 \bmod 7 \Rightarrow a^{12} \equiv 1 \bmod 7,$$

$$b^6 \equiv 1 \bmod 7 \Rightarrow b^{12} \equiv 1 \bmod 7,$$

$$a^{12} \equiv 1 \bmod 13 \text{ e } b^{12} \equiv 1 \bmod 13,$$

e o resultado segue.

Exercício 18. Mostre que $\forall n \in \mathbb{Z}$ temos que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} \in \mathbb{Z}$.

Solução. Queremos mostrar que $\frac{3n^5 + 5n^3 + 7n}{15} \in \mathbb{Z}$, i.e., que 15 divide o numerador. Para isso, basta notar que

$$3n^5 + 5n^3 + 7n \equiv 2n + n \equiv 0 \bmod 3,$$
$$3n^5 + 7n^3 + 7n \equiv 3n + 2n \equiv 0 \bmod 5,$$

pois, pelo Pequeno Teorema de Fermat, temos

$$n^3 \equiv n \bmod 3,$$
$$n^5 \equiv n \bmod 5,$$

e o resultado segue.

Exercício 19. Determine os três últimos dígitos da representação decimal de a^{400}, com $\text{mdc}(a, 10) = 1$.

Solução. Escreva

$$a^{400} = a_k 10^k + \cdots a_1 10 + a_0, \text{ com } a_0, \ldots, a_k \in \{0, 1, \ldots, 9\}.$$

Por Euler, segue que

$$a^{\phi(10^3)} = a^{400} \equiv 1 \bmod 10^3.$$

Logo,

$$a^{400} \equiv a_2 10^2 + a_1 10 + a_0 \equiv 1 \bmod 10^3 \iff a_2 10^2 + a_1 10 + a_0 - 1 = 10\lambda,$$

de onde segue que $a_2 = 0 = a_1$ e $a_0 = 1$, pois $a_0, a_1, a_2 \in \{0, 1, \ldots, 9\}$.

Exercício 20. Determine o último dígito da representação decimal de 2^{400}.

Solução. Nesse caso, $\text{mdc}(2, 10) \neq 1$, mas note que

$$2^{400} = a_k 10^k + \cdots + a_1 10 + a_0$$

e, como $\phi(5) = 4$, temos

$$2^{400} \equiv (2^4)^{100} \equiv a_0 \equiv 1 \bmod 5.$$

Como 2^{400} é par e $0 \leq a_0 \leq 9$, segue que $a_0 = 6$.

Exercício 21. Encontre um SRR módulo 9 composto apenas de primos.

Solução. Como $\phi(9) = 6$, sabemos que todo SRR módulo 9 tem 6 elementos. Também sabemos que

$$E(9) = \{1, 2, 4, 5, 7, 8\}$$

é SRR módulo 9. Do Lema (16.10), se $\{r_1, \ldots, r_6\}$ é SRR módulo 9, então após reordenação de índices temos

$$r_1 \in \overline{1}, r_2 \in \overline{2}, r_3 \in \overline{4}, r_4 \in \overline{5}, r_5 \in \overline{7}, r_6 \in \overline{8}.$$

Queremos então encontrar um primo em cada classe. Note que

$$\begin{aligned} 19 &= 2 \cdot 9 + 1 \in \overline{1}, \\ 11 &= 1 \cdot 9 + 2 \in \overline{2}, \\ 13 &= 1 \cdot 9 + 4 \in \overline{4}, \\ 5 &= 0 \cdot 9 + 5 \in \overline{5}, \\ 7 &= 0 \cdot 9 + 7 \in \overline{7}, \\ 17 &= 1 \cdot 9 + 8 \in \overline{8}. \end{aligned}$$

Logo $\{5, 7, 11, 13, 17, 19\}$ é SRR módulo 9 com apenas primos.

Exercício 22. Mostre que $n^{9^9} + 4 \not\equiv 0 \bmod 37, \forall n \in \mathbb{N}$.

Solução. Por Euler, temos

$$n^{\phi(37)} = n^{36} \equiv 1 \bmod 37 \text{ se } \operatorname{mdc}(n, 37) = 1.$$

Note que se $n \equiv 0 \bmod 37$, então $n^{9^9} + 4 \equiv 4 \not\equiv 0 \bmod 37$. Logo, podemos assumir $\operatorname{mdc}(n, 37) = 1$.

Se $n^{9^9} + 4 \equiv 0 \bmod 37$, então

$$n^{9^9} \equiv -4 \bmod 37 \Leftrightarrow \left(n^{9^9}\right)^4 \equiv 256 \equiv 34 \bmod 37.$$

Por outro lado, temos

$$\left(n^{9^9}\right)^4 = \left(n^{36}\right)^{9^8}$$

e por Euler

$$\left(n^{36}\right)^{9^8} \equiv 1 \not\equiv 34 \bmod 37.$$

Exercício 23. Encontre todos os valores de $n \in \mathbb{N}$ tais que $3 \nmid \phi(n)$.

Solução. Escreva

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \Longrightarrow \phi(n) = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1).$$

Então, se $3 \nmid \phi(n)$, devemos ter que

$$3 \nmid p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1} \text{ e } 3 \nmid (p_1 - 1) \cdots (p_r - 1),$$

ou seja 9 não pode dividir $\phi(n)$ e $p_j \equiv 2 \bmod 3, \forall j = 1, 2, \ldots, r$.

Exercício 24. Mostre que existem infinitos $n \in \mathbb{N}$ tais que $10 | \phi(n)$.

Solução. Note que $\phi(11) = 10$, logo todo n da forma

$$n = 11^a p_1^{r_1} \cdots p_s^{r_s}$$

é tal que $10 | \phi(n)$.

Exercício 25. Seja p primo ímpar. Mostre que

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv \begin{cases} -1 \bmod p, \text{ se } p \equiv 1 \bmod 4 \\ 1 \bmod p, \text{ se } p \equiv 3 \bmod 4 \end{cases}.$$

Solução. Note que

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1).$$

Agora,

$$\begin{aligned} p - 1 &\equiv -1 \bmod p, \\ p - 2 &\equiv -2 \bmod p, \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \bmod p, \end{aligned}$$

de modo que

$$(p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \cdot (-1)^{\frac{p-1}{2}} \equiv -1 \bmod p$$

por Wilson. Como o expoente de -1 é par se $p \equiv 1 \bmod 4$ e ímpar se $p \equiv 3 \bmod 4$, o resultado segue.

Vamos apresentar um exemplo da aplicação do Teorema de Hensel.

Exemplo. Encontre uma solução para $x^4 + x^3 + 8 \equiv 0 \bmod 21025$.

Solução. Note que $21025 = 5^2 \cdot 29^2$ e sejam $f(x) = x^4 + x^3 + 8$ e $f'(x) = 4x^3 + 3x^2$. Seguindo a demonstração do Lema de Hensel, buscamos $b \in \mathbb{Z}$ tal que $f(b) \equiv 0 \bmod p$ e $f'(b) \not\equiv 0 \bmod p$. Por tentativa, obtemos

$$f(1) = 10 = 2 \cdot 5 \equiv 0 \bmod 5, f'(1) = 7 \not\equiv 0 \bmod 5,$$
$$f(3) = 116 = 4 \cdot 29 \equiv 0 \bmod 29, f'(3) = 135 \not\equiv 0 \bmod 29.$$

Queremos $t \in \mathbb{Z}$ tal que $f(b + tp) \equiv f(b) + f'(b) \cdot t \cdot p \equiv 0 \bmod p^2$.

(i) para $p = 5$, temos

$$f(1) = 2 \cdot 5, f'(1) = 7 \Rightarrow b_1 = 1 + 5t,$$

de modo que

$$f(b_1) \equiv 2 \cdot 5 + 7 \cdot t \cdot 5 \equiv 0 \bmod 5^2 \Leftrightarrow 2 + 7t \equiv 0 \bmod 7 \Leftrightarrow t = 4 \therefore b_1 = 21.$$

(ii) para $p = 29$, temos

$$f(3) = 4 \cdot 29, f'(3) = 135 \Rightarrow b_1 = 3 + 29t,$$

de modo que

$$f(b_1) \equiv 4 \cdot 29 + 135 \cdot t \cdot 29 \equiv 0 \bmod 29^2 \Leftrightarrow 4 + 135t \equiv 0 \bmod 29 \Leftrightarrow 19t \equiv -4 \bmod 29.$$

Por Euclides, temos

$$29 = 19 \cdot 1 + 10,$$
$$19 = 10 \cdot 1 + 9,$$
$$10 = 9 \cdot 1 + 1,$$

de modo que

$$1 = (2) \cdot 29 + (-3) \cdot 19 \Leftrightarrow -4 = (-8) \cdot 29 + (12) \cdot 19$$

e, portanto,

$$t = 12 \therefore b_1 = 351.$$

Até agora, temos $f(21) \equiv 0 \bmod 25$ e $f(351) \equiv 0 \bmod 29^2$. Para obter a solução para a congruência do problema, utilizamos o Teorema do Resto Chinês.

$$\begin{cases} x \equiv 21 \bmod 25 \\ x \equiv 351 \bmod 841 \end{cases}.$$

1. Soluções particulares:

$$x_1 = 21, x_2 = 351.$$

2. Valores dos n_i's:

$$n_1 = 841, n_2 = 25.$$

3. Valores dos z_i's:

   (a)

$$841z \equiv 1 \bmod 25 \Rightarrow 16z \equiv 1 \bmod 25.$$

   Por Euclides,

$$1 = 25 \cdot (-7) + 16 \cdot (11) \Rightarrow z_1 = 11.$$

   (b)

$$25z \equiv 1 \bmod 841.$$

   Por Euclides, temos

$$1 = 841 \cdot (11) + 25 \cdot (-370) \Rightarrow z_2 = -370.$$

4. Solução do sistema:

$$x_0 = 21 \cdot 841 \cdot 11 + 351 \cdot 25 \cdot (-370) = -3052479.$$

   Tomando x_0 módulo $25 \cdot 29^2 = 21025$, obtemos

$$x_0 = 17171 \bmod 21025$$

   logo,

$$f(17171) \equiv 0 \bmod 21025.$$

18 Propriedades de polinômios módulo m

Vamos denotar por $\mathbb{Z}[x]$ o conjunto de todos os polinômios com coeficientes inteiros. Sejam $m \in \mathbb{N}, m \geq 2$ e $f(x) \in \mathbb{Z}[x]$. Escreva, com $n \geq k$,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_k x^k + \cdots + a_1 x + a_0.$$

Dizemos que *o grau de* $f(x)$ *módulo* m é igual a k se $a_n \equiv a_{n-1} \equiv \cdots \equiv a_{k+1} \equiv 0 \bmod m$ e $a_k \not\equiv 0 \bmod m$. Além disso, se $g(x) \in \mathbb{Z}[x], g(x) = b_t x^t + \cdots + b_1 x + b_0$, diremos que

$$f(x) \equiv g(x) \bmod m$$

se o grau de $g(x)$ módulo m for igual a k e $a_j \equiv b_j \bmod m, 0 \leq j \leq k$.

Exemplo. Considere os polinômios

$$f(x) = 7x^5 + 21x^4 + 3x^3 + 5x^2 - x + 11, \quad g(x) = 24x^3 + 5x^2 + 20x + 4.$$

Note que $f(x) \equiv g(x) \bmod 7$, pois

$$7 \equiv 21 \equiv 0 \bmod 7, 3 \equiv 24 \bmod 7, 5 \equiv 5 \bmod 7, -1 \equiv 20 \bmod 7, 11 \equiv 4 \bmod 7.$$

O grau de $f(x)$ e $g(x)$ módulo 7 e 3.

Lema 18.1. Sejam $f(x), g(x), h(x) \in \mathbb{Z}[x]$ e $p \in \mathbb{P}$. Suponha que $f(x) \equiv g(x) \cdot h(x) \bmod p$ e seja $b \in \mathbb{Z}$. Se $f(b) \equiv 0 \bmod p$, então $g(b) \equiv 0 \bmod p$ ou $h(b) \equiv 0 \bmod p$.

Demonstração. Segue do Lema (7.2). □

Lema 18.2. Seja $b \in \mathbb{Z}$. Então, $x^t - b^t = (x-b)(x^{t-1} + x^{t-2}b + \cdots + xb^{t-2} + b^{t-1})$.

Demonstração. Basta efetuar o produto e verificar a igualdade. □

Lema 18.3. Se $d|t$, então $x^t - 1 = (x^d - 1)(x^{t-d} + x^{t-2d} + \cdots + x^d + 1)$.

Demonstração. Escreva $t = dn$. Do Lema (18.2), temos

$$y^n - 1 = (y-1)(y^{n-1} + \cdots + 1).$$

Tomando $y = x^d$, o resultado segue. □

Lema 18.4. Sejam $f(x) \in \mathbb{Z}[x]$ e $b \in \mathbb{Z}$. Escreva

$$f(x) = a_k x^k + \cdots + a_0.$$

Então,

$$f(x) - f(b) = (x-b)(a_k x^{k-1} + B_{k-2}x^{k-2} + \cdots + B_1 x + B_0),$$

com $B_{k-2}, \ldots, B_1, B_0 \in \mathbb{Z}$.

Demonstração. Note que

$$\begin{aligned} f(x) - f(b) &= \sum_{j=1}^{k} a_j (x^j - b^j) \\ &= \sum_{j=1}^{k} a_j (x-b)(x^{j-1} + x^{j-2}b + \cdots + xb^{j-2} + b^{j-1}) \\ &= (x-b) \sum_{j=1}^{k} a_j (x^{j-1} + x^{j-2}b + \cdots + xb^{j-2} + b^{j-1}) \end{aligned}$$

pelo Lema (18.2). Logo, $f(x) - f(b) = (x-b)g(x)$, com $g(x) = a_k x^{k-1} + B_{k-2}x^{k-2} + \cdots + B_0$ e com os B_j's sendo combinações lineares de b com os coeficientes de $f(x)$ e, portanto, são inteiros. □

Lema 18.5. Sejam $p \in \mathbb{P}, b \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]$, com

$$f(x) = a_k x^k + \cdots + a_1 x + a_0 \text{ e } a_k \not\equiv 0 \bmod p.$$

Então,

$$f(b) \equiv 0 \bmod p \Leftrightarrow f(x) \equiv (x-b)g(x) \bmod p$$

e o grau de $g(x)$ módulo p é $k-1$.

Demonstração. Do Lema (18.4), temos

$$f(x) - f(b) \equiv (x-b)g(x) \bmod p,$$

logo

$$f(b) \equiv 0 \bmod p \Leftrightarrow f(x) \equiv (x-b)g(x) \bmod p.$$

Além disso, como o coeficiente de x^{k-1} em $g(x)$ é a_k e $\text{mdc}(a_k, p) = 1$, então o grau de $g(x)$ módulo p é $k-1$. □

Observação 18.1. Pode ocorrer que tenhamos $g(b) \equiv 0 \bmod p$. Nesse caso, teríamos $f(x) \equiv (x-b)^2 \cdot h(x) \bmod p$, e o grau de $h(x)$ módulo p seria $k-2$. Isso motiva a seguinte definição.

Definição. Sejam $p \in \mathbb{P}, b \in \mathbb{Z}$ e $f(x) \in \mathbb{Z}[x]$, com $f(x)$ de grau k módulo p. Diremos que b é *uma raiz de multiplicidade m módulo p de $f(x)$* se

$$f(x) \equiv (x-b)^m \cdot h(x) \bmod p$$

e $h(b) \not\equiv 0 \bmod p$. Além disso, segue do Lema (18.5) que o grau de $h(x)$ módulo p é $k-m$.

Observação 18.2. Seja $b \in \mathbb{Z}$ tal que $f(b) \equiv 0 \bmod p$. Como $F_p = \{0, 1, \ldots, p-1\}$ é SCR módulo p, então existe $a \in F_p$ tal que $a \equiv b \bmod p$. Assim, $f(a) \equiv 0 \bmod p$. Nós queremos contar raízes, então podemos nos restringir a F_p.

Teorema 18.6 (Lagrange)**.** Sejam $p \in \mathbb{P}$ e $f(x) \in \mathbb{Z}[x]$. Suponha que o grau de $f(x)$ módulo p seja igual a k. Então existem no máximo k raízes de $f(x)$ módulo p em F_p, contando a multiplicidade.

Demonstração. (Indução em k) Se $k = 1$, $f(x) \equiv a_1 x + a_0 \bmod p$, e como $\text{mdc}(a_1, p) = 1$ essa congruência tem exatamente uma solução, que é a raiz de $f(x)$ módulo p em F_p. Assuma, por hipótese de indução, que o teorema é válido para todo polinômio de grau menor que k módulo p.

Se $f(x)$ não tem raízes módulo p, terminamos. Suponha então que $b \in F_p$ seja raiz de multiplicidade m de $f(x)$ módulo p. Então,

$$f(x) \equiv (x-b)^m \cdot h(x) \bmod p$$

e o grau de $h(x)$ módulo p é $k-m$. Segue da hipótese de indução que $h(x)$ tem no máximo $k-m$ raízes módulo p em F_p. Logo, do Lema (18.1), temos que $f(x)$ tem no máximo $m+(k-m)=k$ raízes módulo p em F_p. □

Exemplo. Seja $m = 16$. O polinômio $f(x) = x^2$ possui 4 raízes módulo 16 : $0, 4, 8, 12 \in F_{12}$, apesar de ter grau 2 módulo 12.

Lema 18.7. Sejam $p \in \mathbb{P}$ e $d \in \mathbb{N}$. Se $d|p-1$, então o polinômio $x^d - 1$ tem exatamente d raízes módulo p em F_p.

Demonstração. Do Lema (18.3), $x^{p-1}-1 \equiv (x^d-1)\cdot h(x) \bmod p$ e $h(x)$ tem grau $p-1-d$ módulo p. Agora, $x^{p-1}-1$ tem exatamente $p-1$ raízes módulo $p : 1, 2, \ldots, p-1$, pelo Lema de Euler. O Lema (18.1) garante que essas raízes são raízes de $x^d - 1$ ou de $h(x)$.

Por outro lado, o Teorema de Lagrange garante que $x^d - 1$ tem no máximo d raízes módulo p e $h(x)$ tem no máximo $p-1-d$ raízes módulo p. Logo, $x^d - 1$ tem exatamente d raízes módulo p. □

Com essas novas ferramentas em mãos, podemos realizar uma nova demonstração do Teorema de Wilson.

Teorema 18.8 (Wilson - revisitado)**.** Seja $p \in \mathbb{P}$. Então $(p-1)! \equiv -1 \bmod p$.

Demonstração. Vimos que $x^{p-1}-1$ tem $1, 2, \ldots, p-1$ como suas raízes. Aplicando o Lema (18.5) repetidas vezes,

$$f(x) = x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \bmod p.$$

Como $-i \equiv p-i \bmod p \forall i \in \mathbb{N}$, temos

$$f(x) = x^{p-1} - 1 \equiv (x+(p-1))(x+(p-2))\cdots(x+1) \bmod p$$

logo

$$f(0) = -1 \equiv (p-1)! \bmod p.$$

□

19 Raízes Primitivas

Sejam $a, m \in \mathbb{Z}, m \geq 2$ e $\text{mdc}(a, m) = 1$. Defina a *ordem de a módulo m* como o menor $t \in \mathbb{N}$ tal que $a^t \equiv 1 \bmod m$, denotada por $\text{ord}_m(a) = t$.

Observação 19.1. Segue do Lema (15.3) que se $a \equiv b \bmod m$ então $a^t \equiv b^t \bmod m, \forall t \in \mathbb{N}$. Assim, vamos considerar um SRR módulo m no estudo da ordem módulo m. Em geral, vamos considerar, como antes,

$$E(m) = \{a \in \mathbb{N} \mid 1 \leq a \leq m-1, \text{mdc}(a, m) = 1\}.$$

Exemplo. Para $m = 15$, temos $E(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ e $|E(15)| = \phi(15) = 8$. Note que

$$\begin{aligned}
\text{ord}_{15}(1) &= 1,\\
\text{ord}_{15}(2) &= 4,\\
\text{ord}_{15}(4) &= 2,\\
\text{ord}_{15}(7) &= 4,\\
\text{ord}_{15}(8) &= 4,\\
\text{ord}_{15}(11) &= 2,\\
\text{ord}_{15}(13) &= 4,\\
\text{ord}_{15}(14) &= 2.
\end{aligned}$$

Lema 19.1. Sejam $a, m \in \mathbb{Z}, m \geq 2$ e $\text{mdc}(a, m) = 1$. Então

$$a^k \equiv 1 \bmod m \Leftrightarrow \text{ord}_m(a) | k.$$

Demonstração. Se $\text{ord}_m(a) | k$, então $k = \text{ord}_m(a) \cdot t, t \in \mathbb{Z}$ e, daí, $a^k \equiv \left(a^{\text{ord}_m(a)}\right)^t \equiv 1 \bmod m$. Reciprocamente, assuma $a^k \equiv 1 \bmod m$ e escreva $k = q \cdot \text{ord}_m(a) + r, 0 \leq r < \text{ord}_m(a)$. Logo,

$$1 \equiv a^k \equiv \left(a^{\text{ord}_m(a)}\right)^q \cdot a^r \equiv a^r \bmod m.$$

Como $r < \text{ord}_m(a)$, segue que $r = 0$ e $\text{ord}_m(a) | k$. □

Corolário 19.1.1. Para todos $a, m \in \mathbb{Z}, m \geq 2$ e $\text{mdc}(a, m) = 1$, $\text{ord}_m(a) | \phi(m)$.

Demonstração. Pelo Lema de Euler, $a^{\phi(m)} \equiv 1 \bmod m$, logo $\text{ord}_m(a) | \phi(m)$ pelo Lema (19.1). □

Lema 19.2. Sejam $a \in \mathbb{Z}, m, h, k \in \mathbb{N}, m \geq 2$ e $\text{mdc}(a, m) = 1$. Então,

$$a^k \equiv a^h \bmod m \Leftrightarrow k \equiv h \bmod \text{ord}_m(a).$$

Demonstração. Assuma, sem perda de generalidade, $k \geq h$. Suponha $k \equiv h \bmod \text{ord}_m(a)$, i.e., $\text{ord}_m(a)|k-h$. Pelo Lema (19.1), $a^{k-h} \equiv 1 \bmod m$, ou seja, $\lambda \cdot m = a^{k-h} - 1$, de modo que $\lambda a^h m = a^k - a^h$ e $m|a^k - a^h$. Reciprocamente, assuma $a^k \equiv a^h \bmod m$. Assim, $a^k - a^h = a^h(a^{k-h} - 1) = m\lambda$, com $k \geq h$. Como $\text{mdc}(a, m) = 1$, então $\text{mdc}(a^h, m) = 1$. Pelo Lema (3.3), $m|a^{k-h} - 1$, i.e., $a^{k-h} \equiv 1 \bmod m$. Pelo Lema (19.1), $\text{ord}_m(a)|k-h$. □

Lema 19.3. Seja $k = \text{ord}_m(a)$. Então $1, a, a^2, \ldots, a^{k-1}$ são dois a dois incongruentes módulo m.

Demonstração. Vamos supor que existem $t, h \in \mathbb{N}$ tais que $0 \leq t < h < k$, e $a^t \equiv a^h \bmod m$. Pelo Lema (19.2), $k|h-t$, o que é absurdo pois $0 < h - t < k$. □

Definição. Sejam $g, m \in \mathbb{N}, m \geq 2$ e $\text{mdc}(g, m) = 1$. Diremos que g é *raiz primitiva módulo* m se $\text{ord}_m(g) = \phi(m)$.

Exemplo. Para $m = 11$, temos $\phi(11) = 10$. Pelo corolário do Lema (19.1), a ordem de a módulo m é um divisor positivo de $\phi(m)$. Nesse caso, as possíveis ordens são $1, 2, 5, 10$. Vamos considerar $E(11) = \{1, 2, 3, \ldots, 10\}$. Temos

n	1	2	3	4	5	6	7	8	9	10
$\text{ord}_{11}(n)$	1	10	5	5	5	10	10	10	5	2

Exemplo. Para $m = 8$, temos $E(8) = \{1, 3, 5, 7\}$ e $\phi(8) = 4$. Temos também

$$\text{ord}_8(1) = 1, \text{ord}_8(3) = 2, \text{ord}_8(5) = 2, \text{ord}_8(7) = 2.$$

Logo, não há raiz primitiva módulo 8.

Lema 19.4. Seja $g \in \mathbb{N}$ uma raiz primitiva módulo m. Então $\left\{1, g, \ldots, g^{\phi(m)-1}\right\}$ é SRR módulo m.

Demonstração. Como $\text{ord}_m(g) = \phi(m)$, segue do Lema (19.3) que

$$1, g, \ldots, g^{\phi(m)-1}$$

são dois a dois incongruentes módulo m. Do Lema (16.11) segue o resultado, pois $\text{mdc}(g, m) = 1$. □

Exemplo. Para $m = 11$, temos $\phi(11) = 10$ e vimos que 2 é raiz primitiva. Temos:

$$2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5, 2^5 \equiv 10, 2^6 \equiv 9, 2^7 \equiv 7, 2^8 \equiv 3, 2^9 \equiv 6.$$

Logo, $\left\{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\right\}$ é SRR módulo 11.

Exemplo. Observe que 1 é raiz primitiva módulo 2 e 3 é raiz primitiva módulo 4. Vimos que não há raiz primitiva módulo 8. Vamos analisar módulo 16. Temos

$$E(16) = \{1, 3, 5, 7, 9, 11, 13, 15\} \text{ e } \phi(16) = 8.$$

Temos $\text{ord}_{16}(1) = 1$ e $\text{ord}_{16}(15) = 2$ pois $15 \equiv -1 \bmod 16$. Os divisores positivos de 8 são $1, 2, 4, 8$, de modo que temos:

n	1	3	5	7	9	11	13	15
$\text{ord}_{16}(n)$	1	4	4	2	2	4	4	2

Logo, não há raiz primitiva módulo 16.

Lema 19.5. Seja $k \in \mathbb{N}, k \geq 3$ e seja $a \in \mathbb{Z}$ ímpar. Então,

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

Demonstração. (Indução em k) Seja $k = 3$. Pelo exemplo anterior, temos que

$$a^{\phi(8)/2} = a^{4/2} = a^2 \equiv 1 \bmod 8$$

sempre que $\text{mdc}(a, 8) = 1$, i.e., quando a é ímpar. Suponha, por hipótese de indução, que

$$a^{\phi(2^k)/2} \equiv 1 \bmod 2^k.$$

Nossa hipótese é equivalente a

$$a^{2^{k-2}} \equiv 1 \bmod 2^k$$

pois $\phi(2^k) = 2^{k-1}$. Note que

$$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2$$

de modo que, por hipótese de indução,

$$a^{2^{k-2}} = 2^k\lambda + 1 \Leftrightarrow a^{2^{k-1}} = 2^{2k}\lambda^2 + 2^{k+1}\lambda + 1.$$

Portanto,

$$a^{2^{k-1}} - 1 = 2^{k+1}\left(\lambda + 2^{k-1}\lambda^2\right), \text{ pois } k \geq 3.$$

Ou seja, $a^{2^{k-1}} \equiv 1 \bmod 2^{k+1}$. Como $2^{k-1} = \phi(2^{k+1})/2$, o resultado segue por indução. □

Corolário 19.5.1. Não existem raízes primitivas módulo $2^k, k \geq 3$.

Demonstração. Seja $a \in \mathbb{N}$ com $\text{mdc}(a, 2^k) = 1$, i.e., a ímpar. Pelo Lema (19.5), temos

$$a^{\phi(2^k)/2} \equiv 1 \bmod 2^k$$

e, pelo Lema (19.1), temos que $\text{ord}_{2^k}(a) | \phi(2^k)/2$. Em particular, isso implica que $\text{ord}_{2^k}(a) < \phi(2^k)$, de modo que não há raiz primitiva. Dos exemplos que vimos, há raízes primitivas apenas módulo 2 e 2^2, i.e., para $k = 1, 2$. □

Lema 19.6. Sejam $a, m \in \mathbb{Z}, m \geq 2$ e $\text{mdc}(a, m) = 1$. Então, $\forall t \in \mathbb{N}$,

$$\text{ord}_m(a^t) = \frac{\text{ord}_m(a)}{\text{mdc}(t, \text{ord}_m(a))}.$$

Demonstração. Denote $\text{ord}_m(a) = k, \text{ord}_m(a^t) = l$ e $\text{mdc}(t, k) = d$. Veja que

$$\left(a^t\right)^{k/d} = \left(a^k\right)^{t/d} \equiv 1 \bmod m.$$

Daí, do Lema (19.1), $l | k/d$ (note que $k/d, t/d \in \mathbb{N}$). Por outro lado,

$$1 \equiv (a^t)^l \equiv a^{tl} \bmod m,$$

logo $k | tl$ (Lema (19.1)). Isto implica que $k/d | lt/d$. Pelo Lema (3.1), $\text{mdc}(t/d, k/d) = 1$ e, pelo Lema (3.3), $k/d | l$. Logo, $l = k/d$. □

Corolário 19.6.1. $\text{ord}_m(a^t) = \text{ord}_m(a) \Leftrightarrow \text{mdc}(t, \text{ord}_m(a)) = 1$.

Lema 19.7. Se g é raiz primitiva módulo m, então existem $\phi(\phi(m))$ raízes primitivas incongruentes módulo m.

Demonstração. Do Lema (19.4),

$$\left\{1, g, \ldots, g^{\phi(m)-1}\right\}$$

é SRR módulo m. Como $\text{ord}_m(g) = \phi(m)$, do Lema (19.6) temos

$$\text{ord}_m(g^t) = \frac{\phi(m)}{\text{mdc}(t, \phi(m))}.$$

Logo, $\text{ord}_m(g^t) = \phi(m) \Leftrightarrow \text{mdc}(t, \phi(m)) = 1$. Dentro do conjunto

$$\{1, 2, \ldots, \phi(m) - 1\}$$

dos expoentes, há, por definição, $\phi(\phi(m))$ coprimos com $\phi(m)$, como queríamos mostrar. □

Observação 19.2. Seja $\text{mdc}(ab, m) = 1$ e assuma $\text{ord}_m(a) = k$ e $\text{ord}_m(b) = h$. Então

$$(ab)^{kh} = (a^k)^h (b^h)^k \equiv 1 \bmod m.$$

Do Lema (19.1), $\text{ord}_m(ab) | kh$.

Lema 19.8. Sejam $a, b, m \in \mathbb{Z}, m \geq 2$ e $\text{mdc}(ab, m) = 1$. Se $\text{ord}_m(a) = k, \text{ord}_m(b) = h$ e $\text{mdc}(k, h) = 1$, então $\text{ord}_m(ab) = kh$.

Demonstração. Seja $\text{ord}_m(ab) = t$. Da observação acima, $t|kh$. Note que

$$b^{tk} \equiv (a^k)^t b^{tk} \equiv (ab)^{tk} \equiv ((ab)^t)^k \equiv 1 \bmod m,$$

logo $h|tk$ (Lema (19.1)). Como $\text{mdc}(h, k) = 1$, $h|t$. Similarmente,

$$a^{th} \equiv (b^h)^t a^{th} \equiv ((ab)^t)^h \equiv 1 \bmod m,$$

ou seja, $k|th$. Como $\text{mdc}(k, h) = 1$, $k|t$. Logo, novamente como $\text{mdc}(k, h) = 1$, então $hk|t$ e, daí, $t = hk$. □

Exemplo. Seja $m = 13$. Encontre os ordens dos elementos de $E(13) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ e indique as raízes primitivas.

Solução. Temos $\phi(13) = 12$ e os divisores positivos de 12 são $1, 2, 3, 4, 6$ e 12. Essas são as possíveis ordens; além disso, há $\phi(\phi(13)) = \phi(12) = 4$ raízes primitivas (se houver alguma). Temos $\text{ord}_{13}(1) = 1$ e como $12 \equiv -1 \bmod 13$, então $\text{ord}_{13}(12) = 2$. Temos também

$$2^2 \equiv 4; 2^3 \equiv 8; 2^4 \equiv 3; 2^5 \equiv 6; 2^6 \equiv 12; 2^7 \equiv 11; 2^8 \equiv 9; 2^9 \equiv 5; 2^{10} \equiv 10; 2^{11} \equiv 7; 2^{12} \equiv 1 \bmod 13.$$

Também poderíamos ter usado o Lema de Euler para deduzir que $2^{12} \equiv 1 \bmod 13$. Assim, 2 é raiz primitiva módulo 13. Note que bastava determinar que $2^6 \not\equiv 1 \bmod 13$ para garantir que 2 é raiz primitiva, mas fizemos todas as contas para utilizar o Lema (19.6).

$$\begin{aligned}
2^2 \equiv 4 \bmod 13 &\Rightarrow \text{ord}_{13}(4) = \frac{12}{\text{mdc}(2, 12)} = 6,\\
2^3 \equiv 8 \bmod 13 &\Rightarrow \text{ord}_{13}(8) = \frac{12}{\text{mdc}(3, 12)} = 4,\\
2^4 \equiv 3 \bmod 13 &\Rightarrow \text{ord}_{13}(3) = \frac{12}{\text{mdc}(4, 12)} = 3,\\
2^5 \equiv 6 \bmod 13 &\Rightarrow \text{ord}_{13}(6) = 12,\\
2^6 \equiv 12 \bmod 13 &\Rightarrow \text{ord}_{13}(12) = \frac{12}{6} = 2,\\
2^7 \equiv 11 \bmod 13 &\Rightarrow \text{ord}_{13}(11) = 12,\\
2^8 \equiv 9 \bmod 13 &\Rightarrow \text{ord}_{13}(9) = \frac{12}{4} = 3,\\
2^9 \equiv 5 \bmod 13 &\Rightarrow \text{ord}_{13}(5) = \frac{12}{3} = 4,\\
2^{10} \equiv 10 \bmod 13 &\Rightarrow \text{ord}_{13}(10) = \frac{12}{2} = 6,\\
2^{11} \equiv 7 \bmod 13 &\Rightarrow \text{ord}_{13}(7) = 12.
\end{aligned}$$

Note que

$$2^7 \equiv 2^3 \cdot 2^4 \equiv 8 \cdot 3 \equiv 11 \bmod 13 \text{ e } \operatorname{ord}_{13}(8) = 4 \text{ e } \operatorname{ord}_{13}(3) = 3,$$

daí, como $\operatorname{mdc}(4,3) = 1$, temos que $\operatorname{ord}_{13}(11) = 3 \cdot 4 = 12$ pelo Lema (19.8). Por fim, concluímos que $2, 6, 7, 11$ são as raízes primitivas módulo 13.

Lema 19.9. Sejam $a, m \in \mathbb{N}, m \geq 2, \operatorname{mdc}(a,m) = 1$ e $p \in \mathbb{P}$. Se $\operatorname{ord}_m(a) | p^\alpha$ e $\operatorname{ord}_m(a) \nmid p^{\alpha-1}$, então $\operatorname{ord}_m(a) = p^\alpha$.

Demonstração. Como $\operatorname{ord}_m(a) \in \mathbb{N}$ e $\operatorname{ord}_m(a) | p^\alpha$, então $\operatorname{ord}_m(a) = p^r, 1 \leq r \leq \alpha$. Por outro lado, $\operatorname{ord}_m(a) \nmid p^{\alpha-1}$, logo $r \neq \alpha - 1$. Suponha que $r < \alpha - 1$. Então existe $t \in \mathbb{N}$ tal que $\alpha - 1 = r + t$. Logo,

$$a^{p^{\alpha-1}} = a^{p^{r+t}} = \left(a^{p^r}\right)^{p^t} \equiv 1 \bmod m$$

o que é absurdo, pois implica $\operatorname{ord}_m(a) | p^{\alpha-1}$. Portanto, $r = \alpha$ e $\operatorname{ord}_m(a) = p^\alpha$. □

Teorema 19.10. Seja $p \in \mathbb{P}$ ímpar. Então sempre existe uma raiz primitiva módulo p.

Demonstração. Escreva $\phi(p) = p - 1 = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$, com $q_1, \ldots, q_n$ primos distintos e $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. Defina

$$H_i(x) = x^{h_i} - 1,$$

com $h_i = \dfrac{p-1}{q_i}, i = 1, \ldots, n$. Pelo Teorema de Lagrange, a congruência

$$H_i(x) \equiv 0 \bmod m$$

tem no máximo h_i soluções incongruentes módulo p em $\{1, 2, \ldots, p-1\}$. Como $h_i < p - 1$, então existe $a_i \in \{1, 2, \ldots, p-1\}$ tal que

$$H_i(a_i) \not\equiv 0 \bmod p,$$

isto é,

$$a_i^{h_i} \not\equiv 1 \bmod p.$$

Defina

$$\beta_i = \frac{p-1}{q_i^{\alpha_i}} \text{ e } g_i = a_i^{\beta_i}, i = 1, \ldots, n.$$

Pelo Lema de Euler,

$$1 \equiv a_i^{p-1} \equiv g_i^{q_i^{\alpha_i}} \bmod p,$$

logo

$$\mathrm{ord}_p(g_i)|q_i^{\alpha_i}$$

pelo Lema (19.1). Por outro lado,

$$g_i^{q_i^{\alpha_i}} \equiv a_i^{h_i} \not\equiv 1 \bmod p.$$

Do Lema (19.9), temos $\mathrm{ord}_m(g_i) = q_i^{\alpha_i}, i = 1, \ldots, n$. Até agora, determinamos $g_1, \ldots, g_n$ tais que

$$\mathrm{ord}_p(g_i) = q_i^{\alpha_i}, i = 1, \ldots, n.$$

Defina $g = g_1 \cdots g_n$ e $t = \mathrm{ord}_p(m)$. Já vimos que $1 \leq t \leq \phi(p) = p - 1$ e $t|p-1$ pelo corolário do Lema (19.1). Suponha $t < \phi(p) = p - 1$. Como $t|p-1$ e $t < p-1$ segue que existe $i \in \{1, 2, \ldots, n\}$ tal que $t|h_i$ (Lema (8.3)). Sem perda de generalidade, assuma que $t|h_1$. Logo,

$$1 \equiv g^{h_1} \equiv (g_1 \cdots g_n)^{h_1} \equiv g_1^{h_1} \cdots g_n^{h_1} \equiv g_1^{h_1} \bmod p$$

pois $\mathrm{ord}_p(g_i) = q_i^{\alpha_i}$ e $q_i^{\alpha_i}|h_1$ para $i \neq 1$. Por outro lado, também temos que $\mathrm{ord}_p(g_1) = q_1^{\alpha_1}|h_1$, o que é absurdo pois $h_1 = q_1^{\alpha_1 - 1} q_2^{\alpha_2} \cdots q_n^{\alpha_n}$ (Lema (8.2)). Logo,

$$\mathrm{ord}_p(g) = p - 1 = \phi(p),$$

ou seja, g é raiz primitiva módulo p. □

Note que a demonstração acima nos dá o seguinte algoritmo para encontrar uma raiz primitiva módulo um primo ímpar.

(1) Fatore $\phi(p) = p - 1 = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$;

(2) calcule $h_i = \dfrac{p-1}{q_i}$ e determine $a_i \in \{1, 2, \ldots, p-1\}$ tal que $a_i^{h_i} \not\equiv 1 \bmod p, i = 1, 2, \ldots, n$;

(3) calcule $\beta_i = \dfrac{p-1}{q_i^{\alpha_i}}$ e $g_i = a_i^{\beta_i}, i = 1, 2, \ldots, n$;

(4) calcule $g = g_1 g_2 \cdots g_n$.

Exemplo. Seja $p = 13$ e use o algortimo para encontrar uma raiz primitiva módulo 13.

Solução. (1) $\phi(13) = 12 = 2^2 \cdot 3$;

(2) $h_1 = \dfrac{12}{2} = 6, h_2 = 4, 5^6 \not\equiv 1 \bmod 13$ e $3^4 \not\equiv 1 \bmod 13$;

(3) $\beta_1 = 3$ e $\beta_2 = 4$, logo $g_1 = 5^3 \equiv 8 \bmod 13$ e $g_2 = 3^4 \equiv 3 \bmod 13$;

(4) $g = g_1 \cdot g_2 \equiv 8 \cdot 3 \equiv 11 \bmod 13$, logo 11 é raiz primitiva módulo 13.

Lema 19.11. Sejam $p \in \mathbb{P}$ ímpar e d divisor positivo de $p-1$. Então há exatamente $\phi(d)$ elementos de $E(p) = \{1, 2, \ldots, p-1\}$ com ordem d módulo p.

Demonstração. Pelo teorema anterior, sabemos que existe raiz primitiva $g \in E(p)$ módulo p. Também sabemos pelo Lema (19.4) que $\left\{1, g, \ldots, g^{\phi(p)-1}\right\}$ é SRR módulo p. Pelo Lema de Euler,

$$g^{p-1} \equiv 1 \bmod p$$

e podemos reescrever esse SRR como

$$\left\{g, g^2, \ldots, g^{p-2}, g^{p-1}\right\}.$$

Como $E(p)$ também é SRR módulo p, então para todo $a \in E(p)$ existe $t \in E(p)$ tal que

$$a \equiv g^t \bmod p.$$

O Lema (19.6) nos diz que

$$\operatorname{ord}_p(a) = \operatorname{ord}_p(g^t) = \frac{p-1}{\operatorname{mdc}(t, p-1)},$$

logo

$$\operatorname{ord}_p(g^t) = d \Leftrightarrow \operatorname{mdc}(t, p-1) = \frac{p-1}{d}.$$

Defina

$$T_{\frac{p-1}{d}} = \left\{t \in E(p) \mid \operatorname{mdc}(t, p-1) = \frac{p-1}{d}\right\}.$$

Definimos $T_{\frac{p-1}{d}}$ na demonstração do Lema (16.16), onde mostramos que $\left|T_{\frac{p-1}{d}}\right| = \phi(d)$, i.e., existem exatamente $\phi(d)$ elementos t em $E(p)$ tais que $\operatorname{ord}_p(g^t) = d$. □

Observação 19.3. Este resultado ressignifica o Lema (16.16), que diz que:

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

Lema 19.12. Seja $p \in \mathbb{P}$. Existe $g \in \mathbb{N}$ tal que $\operatorname{ord}_p(g) = p-1$ e $g^{p-1} \equiv 1 \bmod p^2$.

Demonstração. Pelo Lema (19.11), sabemos que em $E(p)$ há exatamente $\phi(\phi(p))$ raízes primitivas. Seja $h \in E(p)$ tal que $\operatorname{ord}_p(h) = \phi(p) = p-1$ e suponha que $h^{p-1} \equiv 1 \bmod p^2$. Como $\operatorname{mdc}(h, p) = 1$, então $\operatorname{mdc}(h+p, p) = 1$, i.e., $h+p \in E(p^2)$. Denote $g = h+p$ e note que

$$\forall m \in \mathbb{N}, h^m \equiv g^m \equiv (h+p)^m \bmod p \Rightarrow \operatorname{ord}_p(g) = \operatorname{ord}_p(h) = \phi(p).$$

Agora,

$$g^{p-1} = (h+p)^{p-1} = h^{p-1} + (p-1)ph^{p-2} + Mp^2$$

de modo que se

$$g^{p-1} \equiv 1 \bmod p^2,$$

então

$$h^{p-1} + (p-1)ph^{p-2} \equiv 1 \bmod p^2.$$

Como $h^{p-1} \equiv 1 \bmod p^2$, temos

$$(p-1)ph^{p-2} \equiv 0 \bmod p^2,$$

i.e.,

$$h^{p-2} \equiv 0 \bmod p^2.$$

Como $\mathrm{mdc}(h,p) = 1$, isto é absurdo. Logo,

$$g^{p-1} \not\equiv 1 \bmod p^2.$$

□

Lema 19.13. Seja $p \in \mathbb{P}$ ímpar. Então $g \in \mathbb{N}$ tal que $\mathrm{ord}_p(g) = p-1$ e para todo $t \geq 2$

$$g^{\phi(p^{t-1})} \not\equiv 1 \bmod p^t.$$

Demonstração. (Indução em t) Para $t = 2$, aplique o Lema (19.12). Suponha, então,

$$g^{\phi(p^{k-1})} \not\equiv 1 \bmod p^k.$$

Por Euler,

$$g^{\phi(p^{k-1})} \equiv 1 \bmod p^{k-1}.$$

Daí, segue que

$$g^{\phi(p^{k-1})} = 1 + np^{k-1} \text{ e } \mathrm{mdc}(n,p) = 1.$$

Agora,

$$\left(g^{\phi(p^{k-1})}\right)^p = (1+np^{k-1})^p = 1 + np^k + Mp^{k+1}, k \geq 2.$$

Note que

$$\phi(p^k) = p^{k-1}(p-1) = p \cdot p^{k-2}(p-1) = p \cdot \phi(p^{k-1}),$$

logo

$$g^{\phi(p^k)} = \left(g^{\phi(p^{k-1})}\right)^p \equiv 1 + np^k \bmod p^{k+1}.$$

Como $\mathrm{mdc}(n,p) = 1$, segue que

$$g^{\phi(p^k)} \not\equiv 1 \bmod p^{k+1}$$

e o resultado segue por indução. □

Lema 19.14. Seja $p \in \mathbb{P}$ ímpar. Então existe $g \in \mathbb{N}$ tal que $\mathrm{ord}_p(g) = p-1$ e g é raiz primitiva módulo $p^t, \forall t \geq 2$.

Demonstração. Pelo Lema (19.13), existe $g \in \mathbb{N}$ tal que $\mathrm{ord}_p(g) = p-1$ e

$$g^{\phi(p^{t-1})} \not\equiv 1 \bmod p^t.$$

Por outro lado,

$$g^{\phi(p^t)} \equiv 1 \bmod p^t$$

por Euler. Logo, $\mathrm{ord}_{p^t}(g) | \phi(p^t) = p^{t-1}(p-1)$. Mas

$$g^{\mathrm{ord}_{p^t}(g)} \equiv 1 \bmod p,$$

logo $\mathrm{ord}_p(g) | \mathrm{ord}_{p^t}(g)$, i.e., $p-1 | \mathrm{ord}_{p^t}(g)$. Assim, segue-se que $\mathrm{ord}_{p^t}(g) = p^r(p-1), r \leq t-1$. Se $r \leq t-2$, então

$$g^{\phi(p^{t-1})} = g^{p^{t-2}(p-1)} = \left(g^{p^r(p-1)}\right)^{p^{t-2-r}} \equiv 1 \bmod p^t,$$

absurdo. Logo, $r = t-1$ e $\mathrm{ord}_{p^t}(g) = \phi(p^t), \forall t \geq 2$. □

Lema 19.15. Seja $p \in \mathbb{P}$ ímpar. Então sempre existe raiz primitiva módulo $2p^t, \forall t \geq 1$.

Demonstração. Seja g uma raiz primitiva módulo p^t, com $g \in E(p^t)$ (Lema (19.14)). Se g é par, considere

$$g + p^t \in E(2p^t), \text{ pois } \mathrm{mdc}(g + p^t, 2p) = 1$$

e observe que $g+p^t$ é ímpar e $\mathrm{ord}_{p^t}(g+p^t) = \mathrm{ord}_{p^t}(g) = \phi(p^t)$. Assim, sem perda de generalidade, podemos considerar g raiz primitiva ímpar módulo p^t, i.e., $g \in E(2p^t)$. Observe que

$$g^{\mathrm{ord}_{2p^t}(g)} \equiv 1 \bmod 2p^t,$$

ou seja, $\text{ord}_{2p^t}(g)|\phi(2p^t) = \phi(p^t)$, por Euler e pelo Lema (19.1). Por outro lado, como $2p^t|g^{\text{ord}_{2p^t}(g)} - 1$, então p^t também divide essa potência, i.e.,

$$g^{\text{ord}_{2p^t}(g)} \equiv 1 \bmod p^t,$$

logo $\text{ord}_{p^t}(g)|\text{ord}_{2p^t}(g)$. Como $\text{ord}_{p^t}(g) = \phi(p^t)$, o resultado segue. □

Teorema 19.16. Existe raiz primitiva módulo m se, e somente se, $m \in \{2, 4, p^\alpha, 2p^\alpha\}, p \in \mathbb{P}$ ímpar e $\alpha \in \mathbb{N}$.

Demonstração. Segue do corolário do Lema (19.5) e dos Lemas (19.14) e (19.15) que existe raiz primitiva para todo m em $\{2, 4, p^\alpha, 2p^\alpha\}$. Mostramos também, no mesmo corolário, que não há raiz primitiva módulo $m = 2^t, t \geq 3$.

Assim, considere $m \notin \left\{2, 4, p^\alpha, 2p^\alpha, 2^t\right\}, t \geq 3$. Logo, m é composto, ou seja,

$$m = m_1 \cdot m_2, \text{ com } 2 < m_1 < m_2 < m \text{ e } \text{mdc}(m_1, m_2) = 1.$$

Seja $l = \text{mmc}(\phi(m_1), \phi(m_2))$. Como $m_1, m_2 \geq 3$, segue que $\phi(m_1)$ e $\phi(m_2)$ são pares. Logo, $d = \text{mdc}(\phi(m_1), \phi(m_2)) \geq 2$. Seja $a \in \mathbb{Z}$ tal que $\text{mdc}(a, m) = 1$. Então,

$$a^l \equiv 1 \bmod m_1 \text{ e } a^l \equiv 1 \bmod m_2$$

por Euler e, como $\text{mdc}(m_1, m_2) = 1$, segue que

$$a^l \equiv 1 \bmod m,$$

ou seja, $\text{ord}_m(a)|l$. Mas, dos Lemas (9.2) e (16.14) segue que

$$l = \text{mmc}(\phi(m_1), \phi(m_2)) = \frac{\phi(m_1)\phi(m_2)}{\text{mdc}(\phi(m_1), \phi(m_2))} = \frac{\phi(m)}{\text{mdc}(\phi(m_1), \phi(m_2))} \leq \frac{\phi(m)}{2}.$$

Assim, $\text{ord}_m(a) \leq l \leq \phi(m)/2, \forall a \in \mathbb{Z}$ tal que $\text{mdc}(a, m) = 1$, ou seja, não há raiz primitiva módulo m. □

Observação 19.4. Seja $m \in \mathbb{N}, m \geq 2$. Vimos que se g é raiz primitiva módulo m, então $\left\{1, g, \ldots, g^{\phi(m)-1}\right\}$ é SRR módulo m. Como $g^{\phi(m)} \equiv 1 \bmod m$ (Euler), então $g^{\phi(m)} \in \overline{1}$. Logo, $\left\{g, g^2, \ldots, g^{\phi(m)}\right\}$ é também SRR módulo m. Isso nos diz que para todo inteiro a coprimo com m existe um único $t \in \{1, 2, \ldots, \phi(m)\}$ tal que $a \equiv g^t \bmod m$.

Isso motiva a seguinte definição.

Definição. Sejam g raiz primitiva módulo m, e $a \in \mathbb{Z}$ tal que $\text{mdc}(a, m) = 1$. O único $t \in \{1, 2, \ldots, \phi(m)\}$ tal que

$$a \equiv g^t \bmod m$$

é chamado de *índice de a módulo m na base g*, denotado por $t = \text{ind}_g(a)$.

Exemplo. Seja $p = 17$. Temos que 3 é raiz primitiva módulo 17. Assim, módulo 17, temos

$$\begin{aligned}
3^1 = 3 &\Longrightarrow \text{ind}_3(3) = 1,\\
3^2 = 9 &\Longrightarrow \text{ind}_3(9) = 2,\\
3^3 = 10 &\Longrightarrow \text{ind}_3(10) = 3,\\
3^4 = 13 &\Longrightarrow \text{ind}_3(13) = 4,\\
3^5 = 5 &\Longrightarrow \text{ind}_3(5) = 5,\\
3^6 = 15 &\Longrightarrow \text{ind}_3(15) = 6,\\
3^7 = 11 &\Longrightarrow \text{ind}_3(11) = 7,\\
3^8 = 16 &\Longrightarrow \text{ind}_3(16) = 8,\\
3^9 = 14 &\Longrightarrow \text{ind}_3(14) = 9,\\
3^{10} = 8 &\Longrightarrow \text{ind}_3(8) = 10,\\
3^{11} = 7 &\Longrightarrow \text{ind}_3(7) = 11,\\
3^{12} = 4 &\Longrightarrow \text{ind}_3(4) = 12,\\
3^{13} = 12 &\Longrightarrow \text{ind}_3(12) = 13,\\
3^{14} = 2 &\Longrightarrow \text{ind}_3(2) = 14,\\
3^{15} = 6 &\Longrightarrow \text{ind}_3(6) = 15,\\
3^{16} = 1 &\Longrightarrow \text{ind}_3(1) = 16.
\end{aligned}$$

Lema 19.17. Sejam g raiz primitiva módulo m e $a, b \in \mathbb{Z}$ tais que $\text{mdc}(ab, m) = 1$. Então

$$a \equiv b \bmod m \Longleftrightarrow \text{ind}_g(a) \equiv \text{ind}_g(b) \bmod \phi(m).$$

Demonstração. Sejam $t = \text{ind}_g(a)$ e $h = \text{ind}_g(b)$. Queremos mostrar que

$$g^t \equiv g^h \bmod m \Longleftrightarrow t \equiv h \bmod \phi(m)$$

que é o resultado do Lema (19.2), já que $\text{ord}_m(g) = \phi(g)$. □

Lema 19.18. Sejam g raiz primitiva módulo m e $a, b \in \mathbb{Z}$ tais que $\text{mdc}(ab, m) = 1$. Então:

(i) $\text{ind}_g(ab) \equiv \text{ind}_g(a) + \text{ind}_g(b) \bmod \phi(m)$;

(ii) $\text{ind}_g(a^k) \equiv k \,\text{ind}_g(a) \bmod \phi(m), \forall k \in \mathbb{N}$.

Demonstração. Sejam $r = \text{ind}_g(a), s = \text{ind}_g(b)$ e $t = \text{ind}_g(ab)$. Logo,

$$g^t \equiv ab \equiv g^r \cdot g^s \equiv g^{r+s} \bmod m.$$

Da demonstração do Lema (19.17), segue que $t \equiv r + s \bmod \phi(m)$ e o item (i) está provado. Agora, seja $u = \text{ind}_g(a^k)$, de modo que

$$g^u \equiv a^k \equiv (g^r)^k \equiv g^{rk} \bmod m,$$

e segue de modo análogo que $u \equiv rk \bmod \phi(m)$, provando (ii). □

Lema 19.19. Seja $m \in \mathbb{N}, m \geq 2$, e suponha que exista raiz primitiva módulo m. Sejam $a, k \in \mathbb{N}$ e suponha que $\text{mdc}(a, m) = 1$. Escreva $d = \text{mdc}(k, \phi(m))$. Então a congruência $x^k \equiv a \bmod m$ tem solução se, e só se, $a^{\phi(m)/d} \equiv 1 \bmod m$.

Demonstração. Seja g raiz primitiva módulo m. Segue do Lema (19.18) que a congruência $x^k \equiv a \bmod m$ tem solução se, e só se, a congruência $k \,\text{ind}_g(a) \equiv \text{ind}_g(a) \bmod \phi(m)$ tem solução. Por outro lado, essa congruência linear tem solução se, e só se, $d | \,\text{ind}_g(a)$, pelo Lema (16.2). Observe também que pelo Lema (19.18), temos

$$\begin{aligned} a^{\phi(m)/d} \equiv 1 \bmod m &\iff \frac{\phi(m)}{d} \,\text{ind}_g(a) \equiv \text{ind}_g(1) \equiv 0 \bmod \phi(m) \\ &\iff \frac{\phi(m)}{d} \,\text{ind}_g(a) = \phi(m)\lambda \\ &\iff \text{ind}_g(a) = \lambda \\ &\iff d | \,\text{ind}_g(a) \end{aligned}$$

e o resultado segue. □

Corolário 19.19.1. $x^k \equiv a \bmod m$ tem solução se, e só se, $x^d \equiv a \bmod m$ tem solução.

Demonstração. Note que a condição dada pelo lema (19.19)

$$a^{\phi(m)/d} \equiv 1 \bmod m$$

é igual para ambas as equações. □

Lema 19.20. Sejam $m \in \mathbb{N}, m \geq 2$, e suponha que há raiz primitiva módulo m. Sejam $a, k \in \mathbb{Z}$ com $\text{mdc}(a, m) = 1$ e $d = \text{mdc}(k, \phi(m))$. Se $x^k \equiv a \bmod m$ tem solução, então ela tem exatamente d soluções incongruentes.

Demonstração. Sabemos que $x^k \equiv a \bmod m$ tem solução se, e só se, $k \,\text{ind}_g(a) \equiv \text{ind}_g(a) \bmod \phi(m)$ tem solução. Do Lema (16.2), segue que se essa congruência linear tem solução, então há exatamente d soluções incongruentes módulo m. □

Observação 19.5. O índice módulo m na base g tem as mesmas propriedades da função logaritmo, mas em um ambiente discreto de congruência módulo m.

Exemplo. Existe solução para $13x^{20} \equiv 8 \bmod 19$?

Solução. Queremos aplicar o Lema (19.19), mas para isso precisamos mudar a forma da congruência. Como $\text{mdc}(13, 19) = 1$, existe solução única para $13z \equiv 1 \bmod 19$ e, fazendo as contas, temos $z = 3$. Assim, $13x^{20} \equiv 8 \bmod 19$ é equivalente a $x^{20} \equiv 5 \bmod 19$. Pelo Lema (19.19), há solução se, e só se

$$5^{\phi(19)/d} \equiv 1 \bmod 19, \text{ com} d = \text{mdc}(20, \phi(19)) = 2,$$

ou seja, se e só se

$$5^9 \equiv 1 \bmod 19,$$

que é verdade. Portanto, a congruência tem solução e, pelo Lema (19.20), exatamente duas soluções.

Exemplo. Encontre as soluções de $8y^6 \equiv 1 \bmod 17$.

Solução. Vimos que 3 é raiz primitiva módulo 17, logo $8y^6 \equiv 1 \bmod 17$ tem solução se, e só se, $\text{ind}_3(8) + 8\,\text{ind}_3(y) \equiv \text{ind}_3(1) \bmod \phi(17)$ tem solução. Temos então

$$10 + 6x \equiv 16 \equiv 0 \bmod 16 \iff 6x \equiv 6 \bmod 16, \text{ que tem solução.}$$

Como $\text{mdc}(6, 16) = 2$, há duas soluções: $x_1 = 1$ e $x_2 = 1 + 16/2 = 9$. Agora, $\text{ind}_3(y) = 1$ implica $y =$ e $\text{ind}_3(y) = 9$ implica $y = 14$, que são as soluções buscadas.

Exemplo. Existe solução para $x^{33} \equiv 7 \bmod 19$?

Solução. Aplicando o Lema (19.19), precisamos verificar se

$$7^6 \equiv 1 \bmod 19, \text{ pois} \phi(19) = 18 \text{ e} 3 = \text{mdc}(33, 18).$$

Isso de fato é verdade, e pelo Lema (19.20) há 3 soluções incongruentes. Vamos encontrá-las.

Os divisores positivos de 18 são: $1, 2, 3, 6, 9, 18$ (possíveis ordens). Fazendo as contas, temos que 3 é raiz primitiva módulo 19, e também que $3^6 \equiv 7$. Assim, $x^{33} \equiv 7 \bmod 19$ tem solução se, e só se, $33z \equiv 6 \bmod 18$ tem solução, com $z = \text{ind}_3(x)$. Como $\text{mdc}(33, 18) = 3$ e $3|6$, essa congruência tem exatamente 3 soluções incongruentes. Temos

$$3 = 18(2) + 33(-1) \Longrightarrow 6 = 18(4) + 33(-2) \Longrightarrow z_0 = -2 \equiv 16 \bmod 18 \text{ é solução.}$$

As demais soluções são $z_1 = -2 + 18/3 = 4$ e $z_2 = -2 + (18/3)2 = 10$. Assim, as três soluções que buscamos são

$$\begin{cases} \text{ind}_3(x) = 16 \\ \text{ind}_3(x) = 4 \\ \text{ind}_3(x) = 10 \end{cases} \Longrightarrow \begin{cases} x = 17 \\ x = 5 \\ x = 16 \end{cases}.$$

Observação 19.6. Vimos que $3 = \text{mdc}(33, 18)$ e, pelo corolário do Lema (19.19),

$$x^{33} \equiv 7 \bmod 19 \text{ tem solução } \iff x^3 \equiv 7 \bmod 19 \text{ tem solução.}$$

Vimos também que a primeira congruência tem 5, 16 e 17 como soluções incongruentes. Repetindo argumentos análogos ao exemplo acima, as soluções da segunda congruência são $4, 6$ e 9. Assim, apesar de ambas as congruências terem a mesma quantidade de soluções, elas são distintas!

20 Resíduos Quadráticos

Até o momento estudamos equações de congruência do tipo $ax^k \equiv b \bmod m$, com $k \in \mathbb{N}$. Agora, gostaríamos de olhar mais de perto o caso quadrático: $k = 2$.

Definição. Seja p primo ímpar e $a \in \mathbb{N}$ tal que $\text{mdc}(a, p) = 1$. Dizemos que a é *resíduo quadrático módulo* p se existir $b \in \mathbb{N}$ tal que $a \equiv b^2 \bmod p$.

Seja p primo ímpar. Como observamos anteriormente, basta buscar resíduos quadráticos em $E(p)$, pois ele forma um SRR módulo p (ver Lemas (15.3) e (16.9)). Denotando por F_p^2 o conjunto dos resíduos quadráticos módulo p, temos

$$F_p^2 = \left\{a^2 \mid a \in E(p)\right\}.$$

Exemplo. Seja $p = 11, E(11) = \{1, 2, \ldots, 10\}$. Como

$$6 \equiv -5, 7 \equiv -4, 8 \equiv -3, 9 \equiv -2, 10 \equiv -1 \bmod 11,$$

segue que

$$F_{11}^2 = \left\{(\pm a)^2 \mid a = 1, 2, 3, 4, 5\right\} = \{1, 3, 4, 5, 9\}$$

pois

$$(\pm 1)^2 \equiv 1, (\pm 2)^2 \equiv 4, (\pm 3)^2 \equiv 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3 \bmod 11.$$

Observação 20.1. A ideia apresentada acima será bastante usada, i.e.,

$$-a \equiv p - a \bmod p.$$

Lema 20.1 (Critério de Euler)**.** Seja p primo ímpar e $a \in \mathbb{N}$ com $\text{mdc}(a, p) = 1$. Então a é resíduo quadrático módulo p se, e só se, $a^{(p-1)/2} \equiv 1 \bmod p$.

Demonstração. Esse lema é consequência direta do Lema (19.19), pois a ser resíduo quadrático módulo p significa que $x^2 \equiv a \bmod p$ tem solução, o que acontece se, e só se, $a^{\phi(p)/d} \equiv 1 \bmod p$. Mas então o resultado segue, pois $\phi(p) = p - 1$ e $d = \text{mdc}(2, p - 1) = 2$. □

Lema 20.2. Seja p primo ímpar. Então -1 é resíduo quadrático módulo p se, e só se, $p \equiv 1 \bmod 4$.

Demonstração. Temos que -1 é resíduo quadrático módulo p se, e só se, $(-1)^{(p-1)/2} \equiv 1 \bmod p$, pelo Lema (20.1). Como $p \equiv 1 \bmod 4$, então $4|p-1$, de modo que $(p-1)/2$ é par e o resultado segue. □

Nosso objetivo é determinar critérios, como vimos no Lema (20.2), para outros valores de a. Observe que se o primo for muito grande, o critério de Euler não será facilmente aplicado.

Lema 20.3. Seja p primo ímpar. Então existem $\dfrac{p-1}{2}$ resíduos quadráticos módulo p.

Demonstração. Queremos mostrar que $\left|F_p^2\right| = \dfrac{p-1}{2}$. Como vimos, podemos considerar o SRR módulo p

$$1, 2, \ldots, \frac{p-1}{2}, -\left(\frac{p-1}{2}\right), \ldots, -2, -1$$

pois se $a \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, então

$$-a \equiv p - a \bmod p$$

e $p-a \in \left\{\dfrac{p+1}{2}, \ldots, p-3, p-2, p-1\right\}$. Além disso, temos que se $b \equiv a^2 \bmod p$, então $b \equiv (-a)^2 \bmod p$. Assim, basta considerar os elementos de $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$. Sejam a, b elementos distintos nesse conjunto, $a < b$. Então, $b^2 - a^2 = (b-a)(b+a)$. Observe que

$$1 \leq b - a < \frac{p-1}{2},$$
$$3 \leq b + a < p - 1,$$

logo $b - a \not\equiv 0 \bmod p$ e $b + a \not\equiv 0 \bmod p$, de modo que $b^2 - a^2 \not\equiv 0 \bmod p$, i.e., $1^2, 2^2, \ldots, \left(\dfrac{p-1}{2}\right)^2$ são dois a dois incongruentes módulo p e o resultado segue. □

Definição (Símbolo de Legendre)**.** Seja p primo ímpar e $a \in \mathbb{N}$ com $\text{mdc}(a, p) = 1$. Defina

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1, & \text{caso contrário.} \end{cases}$$

Exemplo. Seja $p = 7$ e $E(7) = \{1, 2, 3, 4, 5, 6\}$. Temos:

$$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1 \bmod 7,$$

logo

$$\left(\frac{1}{7}\right) = 1, \left(\frac{2}{7}\right) = 1, \left(\frac{4}{7}\right) = 1$$

e

$$\left(\frac{3}{7}\right) = -1, \left(\frac{5}{7}\right) = -1, \left(\frac{6}{7}\right) = -1$$

logo

$$F_7^2 = \{1, 2, 4\}.$$

Lema 20.4. Seja p primo ímpar e $a \in \mathbb{N}$ tal que $\text{mdc}(a, p) = 1$. Então

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p.$$

Demonstração. Pelo Teorema de Lagrange, $x^2 \equiv 1 \bmod p$ tem exatamente duas soluções módulo p, $x = 1$ e $x = -1$. Por outro lado, note que

$$\left(a^{(p-1)/2}\right)^2 = a^{p-1} \equiv 1 \bmod p$$

por Euler, ou seja, $a^{(p-1)/2} = \pm 1 \bmod p$ e o resultado segue do critério de Euler. □

Lema 20.5. Seja p primo ímpar e $a, b \in \mathbb{N}$ tais que $\text{mdc}(ab, p) = 1$. Então

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Demonstração. Pelo Lema (20.4), temos

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv (a)^{(p-1)/2}(b)^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \bmod p.$$

Note que

$$-2 \leq \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \leq 2.$$

Como p é primo ímpar e p divide essa diferença, então essa diferença deve ser igual a 0, e o resultado segue. □

Exemplo. Determine todos os resíduos quadráticos módulo 31.

Solução. Pelo Lema (20.3), sabemos que $\left|F_{31}^2\right| = 15$. Como $31 \equiv 3 \bmod 4$, segue que

$$\left(\frac{-1}{31}\right) = -1, \text{ pelo Lema (20.2).}$$

Pelo Lema (20.5),

$$\left(\frac{-a}{31}\right) = -\left(\frac{a}{31}\right).$$

Como $1, 4, 9, 16, 25 \in E(31)$ são quadrados, segue que

$$\left(\frac{1}{31}\right) = \left(\frac{4}{31}\right) = \left(\frac{9}{31}\right) = \left(\frac{16}{31}\right) = \left(\frac{25}{31}\right) = 1.$$

Por outro lado, $16 \equiv -15 \bmod 31$, logo

$$1 = \left(\frac{16}{31}\right) \Rightarrow \left(\frac{-15}{31}\right) = -1$$

e o mesmo ocorre para os outros quadrados:

$$\left(\frac{6}{31}\right) = \left(\frac{22}{31}\right) = \left(\frac{27}{31}\right) = \left(\frac{30}{31}\right) = -1.$$

Agora, $6^2 \equiv 5 \bmod 31$, logo $\left(\frac{5}{31}\right) = 1$. Mas

$$\begin{aligned}
-1 = \left(\frac{15}{31}\right) = \left(\frac{3}{31}\right) \cdot \left(\frac{5}{31}\right) &\Rightarrow \left(\frac{3}{31}\right) = -1, \\
-1 = \left(\frac{6}{31}\right) = \left(\frac{2}{31}\right) \cdot \left(\frac{3}{31}\right) &\Rightarrow \left(\frac{2}{31}\right) = 1, \\
-1 = \left(\frac{22}{31}\right) = \left(\frac{2}{31}\right) \cdot \left(\frac{11}{31}\right) &\Rightarrow \left(\frac{11}{31}\right) = -1, \\
\left(\frac{10}{31}\right) = \left(\frac{2}{31}\right) \cdot \left(\frac{5}{31}\right) &= 1.
\end{aligned}$$

Como $-5 \equiv 26 \bmod 31$, temos

$$\left(\frac{26}{31}\right) = -1 = \left(\frac{2}{31}\right) \cdot \left(\frac{13}{31}\right) \Rightarrow \left(\frac{13}{31}\right) = -1.$$

Temos também $-2 \equiv 29, -3 \equiv 28, -11 \equiv 20, -13 \equiv 18$, logo

$$\left(\frac{29}{31}\right) = -1, \left(\frac{28}{31}\right) = 1, \left(\frac{20}{31}\right) = 1, \left(\frac{18}{31}\right) = 1.$$

Daí, temos

$$1 = \left(\frac{28}{31}\right) = \left(\frac{4}{31}\right) \cdot \left(\frac{7}{31}\right) \Rightarrow \left(\frac{7}{31}\right) = 1.$$

Como $7 \equiv -24 \bmod 31$, temos

$$-1 = \left(\frac{24}{31}\right) = \left(\frac{8}{31}\right) \cdot \left(\frac{3}{31}\right) \Rightarrow \left(\frac{8}{31}\right) = 1$$

mas $-8 \equiv 23 \bmod 31$, logo $\left(\frac{23}{31}\right) = -1$. Também temos

$$\begin{aligned}
\left(\frac{21}{31}\right) = \left(\frac{3}{31}\right) \cdot \left(\frac{7}{31}\right) &= -1, \\
\left(\frac{11}{31}\right) = \left(\frac{4}{31}\right) \cdot \left(\frac{3}{31}\right) &= -1, \\
\left(\frac{14}{31}\right) = \left(\frac{2}{31}\right) \cdot \left(\frac{7}{31}\right) &= 1, \\
\left(\frac{19}{31}\right) = \left(\frac{-12}{31}\right) &= 1, \\
\left(\frac{17}{31}\right) = \left(\frac{-14}{31}\right) &= -1.
\end{aligned}$$

Logo, $F_{31}^2 = \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$.

Esse exemplo ilustra a simetria entre a e $-a$ e a relação com resíduos quadráticos. Segue do Lema (20.2) que

$$\left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right) \iff p \equiv 1 \bmod 4,$$
$$\left(\frac{-a}{p}\right) = -\left(\frac{a}{p}\right) \iff p \equiv 3 \bmod 4.$$

Definição (Resto principal)**.** Seja p primo ímpar. O conjunto

$$\mathcal{R}_p = \left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -2, -1, 2, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\right\}$$

é SRR módulo p, pois $\forall a \in \left\{\frac{p+1}{2}, \ldots, p-1\right\} \exists b \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ tal que

$$a \equiv p - b \equiv -b \bmod p.$$

Seja $a \in \mathbb{Z}$ tal que $\text{mdc}(a, p) = 1$. Então existe $r(a) \in \mathcal{R}_p$ único tal que

$$a \equiv r(a) \bmod p,$$

que é chamado de *resto principal de a módulo p*.

Exemplo. Seja $p = 19$. Então

$$\mathcal{R}_{19} = \{-9, -8, \ldots, -1, 1, \ldots, 8, 9\}.$$

Vamos calcular alguns restos principais:

$$r(13) \equiv 13 \equiv -6 \bmod 19 \Rightarrow r(13) = -6 \in \mathcal{R}_{19},$$
$$r(8) \equiv 8 \bmod 19 \Rightarrow r(8) = 8 \in \mathcal{R}_{19},$$
$$r(79) \equiv 3 \bmod 19 \Rightarrow r(79) = 3 \in \mathcal{R}_{19},$$
$$r(145) \equiv 12 \equiv -7 \bmod 19 \Rightarrow r(145) = -7 \in \mathcal{R}_{19}.$$

Lema 20.6 (Gauss)**.** Seja p primo ímpar e $a \in \mathbb{Z}$ tal que $\text{mdc}(a, p) = 1$. Defina o conjunto

$$S_a = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a\right\}$$

e seja μ o número de restos principais negativos dos elementos de S_a. Então

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Demonstração. Seja $S = \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$ e denote por $r_j = r(ja), j \in S$. Então $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ são os restos principais dos elementos de S_a. Vamos mostrar que os $r_j's$ têm duas propriedades:

(1) $r_i = r_j \iff i = j$

Nesse caso, $r_i = r_j$ implica

$$ia \equiv r_i \equiv r_j \equiv ja \bmod p \iff i \equiv j \bmod p$$

pois $\text{mdc}(a,p) = 1$. Como $1 \leq i \leq j \leq \dfrac{p-1}{2}$, então $0 \leq j - i < p$ e, como $p|j-i$, segue que $j = i$. A volta é imediata.

(2) $r_i \neq -r_j, \forall i, j \in S$

Nesse caso, se $r_i = -r_j$, então

$$r_i \equiv ia \equiv -ja \equiv -r_j \bmod p \iff i \equiv -j \bmod p$$

pois $\text{mdc}(a,p) = 1$. Mas $2 \leq i + j < p$, logo isso é absurdo.

De (1) e (2), temos que $|r_i| \neq |r_j|$ se $i \neq j$. Por definição, $|r_i| \in S$ e como são todos dois a dois distintos, segue que

$$S = \left\{|r_1|, |r_2|, \ldots, |r_{\frac{p-1}{2}}|\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Logo

$$\begin{aligned} a \cdot 2a \cdots \frac{p-1}{2} \cdot a &\equiv r_1 \cdot r_2 \cdots r_{\frac{p-1}{2}} \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! \bmod p \\ &\iff a^{\frac{p-1}{2}} \equiv (-1)^\mu \bmod p. \end{aligned}$$

Pelo Lema (20.4), segue que

$$(-1)^\mu \equiv \left(\frac{a}{p}\right) \bmod p.$$

Como $p \geq 3$ e $-2 \leq (-1)^\mu - \left(\frac{a}{p}\right) \leq 2$, então $(-1)^\mu = \left(\frac{a}{p}\right)$. □

Exemplo. Seja $p = 37$. Usando o Lema de Gauss, vamos calcular $\left(\dfrac{3}{37}\right)$. O conjunto dos restos principais módulo 37 é

$$\mathcal{R}_{37} = \{-18, -17, \ldots, -1, 1, \ldots, 17, 18\}.$$

Para usar o Lema de Gauss, determinamos S_3:

$$S_3 = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54\}.$$

O conjunto dos restos principais é

$$\mathcal{B} = \{3, 6, 9, 12, 15, 18, -16, -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17\}.$$

É importante notar que $\mathcal{B} \subset \mathcal{R}_{37}$. Assim, podemos escrever

$$S_3 = P \cup N = \{3, 6, 9, 12, 15, 18, 39, 42, 45, 48, 51, 54\} \cup \{21, 24, 27, 30, 33, 36\},$$

com P o conjunto dos números com restos principais positivos e N o conjunto dos números com restos principais negativos. Note que $\mu = |N| = 6$, logo

$$\left(\frac{3}{37}\right) = (-1)^{\mu} = 1$$

e 3 é resíduo quadrático módulo 37.

Lema 20.7. Seja p primo ímpar. Então

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \bmod 8.$$

Demonstração. Vamos usar o Lema de Gauss. Seja

$$S_2 = \{2, 4, 6, \ldots, p-5, p-3, p-1\}, |S_2| = \frac{p-1}{2}.$$

Escreva

$$S_2 = P \cup N,$$

com P e N os conjuntos dos elementos de S_2 com restos principais positivos e negativos, respectivamente. Note que

$$P \subset \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \text{ e } N \subset \left\{\frac{p+1}{2}, \ldots, p-2, p-1\right\},$$

consequência da definição de resto principal. Para determinar $\mu = |N|$, temos de entender se $\frac{p-1}{2}$ pertence a P ou não.

(i) $\frac{p-1}{2}$ par

Nesse caso, temos

$$\frac{p-1}{2} \in P \subset S_2,$$

logo

$$|P| = \frac{p-1}{4} = |N|.$$

Por Gauss, segue que

$$\left(\frac{2}{p}\right) = 1 \iff \frac{p-1}{4} \text{ é par } \iff p \equiv 1 \bmod 8.$$

(ii) $\frac{p-1}{2}$ ímpar

Nesse caso, temos

$$\frac{p-1}{2} - 1 = \frac{p-3}{2} \in P \subset S_2,$$

logo

$$|P| = \frac{p-3}{4}, |N| = \frac{p+1}{4}.$$

Por Gauss, segue que

$$\left(\frac{2}{p}\right) = 1 \iff \frac{p+1}{4} \text{ é par } \iff p \equiv -1 \bmod 8.$$

□

21 Observação Geral

Seja p primo ímpar. Até agora, sabemos calcular $\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right)$ (ver Lemas (20.2) e (20.7)). Note que se $a \in \mathbb{Z}, a < 0$ com $\text{mdc}(a,p) = 1$, podemos escrever $a = -b, b \in \mathbb{N}$. Pelo Lema (20.5), temos

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right).$$

Logo, se sabemos calcular $\left(\frac{b}{p}\right)$ com $b \in \mathbb{N}$ e $\text{mdc}(b,p) = 1$, sabemos calcular $\left(\frac{a}{p}\right) \forall a \in \mathbb{Z}$ com $\text{mdc}(a,p) = 1$.

Então suponha que $a \in \mathbb{N}$ com $\text{mdc}(a,p) = 1$ e escreva

$$a = 2^{\beta_0} \cdot q_1^{\beta_1} \cdots q_n^{\beta_n}, \beta_i \in \mathbb{N} \cup \{0\}, 0 \leq j \leq n \text{ e } q_1, \ldots, q_n \text{ primos ímpares distintos.}$$

Pelo Lema (20.5),

$$\left(\frac{a}{p}\right) = \left(\frac{2^{\beta_0}}{p}\right)\left(\frac{q_1^{\beta_1}}{p}\right) \cdots \left(\frac{q_n^{\beta_n}}{p}\right).$$

Note que

$$\left(\frac{q^{2m}}{p}\right) = 1 \forall m \in \mathbb{N}, \text{ pois } (q^m)^2 \equiv q^{2m} \bmod p,$$

ou seja, q^{2m} é sempre resíduo quadrático módulo p. Logo

$$\left(\frac{q^{2m+1}}{p}\right) = \left(\frac{q^{2m}}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)$$

de onde segue que

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^{\epsilon_0}\left(\frac{q_1}{p}\right)^{\epsilon_1} \cdots \left(\frac{q_n}{p}\right)^{\epsilon_n}, \epsilon_j \in \{0,1\}, \epsilon_j \equiv \beta_j \bmod 2 \text{ e } 0 \leq j \leq n.$$

Nós já sabemos calcular $\left(\frac{2}{p}\right)$ pelo Lema (20.7). Precisamos então aprender a calcular $\left(\frac{q}{p}\right)$, com p e q primos ímpares distintos.

Esse objetivo é alcançado com a *Lei da Reciprocidade Quadrática de Gauss*. Mas antes de apresentar esse bonito teorema, precisamos de outros resultados preliminares e uma variação do Lema de Gauss.

Exemplo. Seja $p = 19$. Se queremos calcular

$$\left(\frac{151200}{19}\right),$$

basta notar que $151200 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7$ e, daí,

$$\left(\frac{151200}{19}\right) = \left(\frac{2^5}{19}\right)\left(\frac{3^3}{19}\right)\left(\frac{5^2}{19}\right)\left(\frac{7}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{3}{19}\right)\left(\frac{7}{19}\right).$$

Como $42 = 2 \cdot 3 \cdot 7$, temos

$$\left(\frac{151200}{19}\right) = \left(\frac{42}{19}\right).$$

Definição (Função maior inteiro)**.** Seja $x \in \mathbb{R}$. Defina $[x]$ como *o maior inteiro menor ou igual* a x.

Exemplo. $[2] = 2, [3,021] = 3, [-5,1] = -6, [0,98] = 0$.

Observação 21.1. Com essa notação, podemos escrever o Teorema de Euclides como

$$a = p\left[\frac{a}{p}\right] + r, 0 \leq r < p.$$

Seja $\text{mdc}(a,p) = 1$, p primo ímpar. Se $0 < r \leq \frac{p-1}{2}$, então $r(a) = r$, o resto principal de a módulo p. Se $\frac{p+1}{2} \leq r \leq p-1$, então $-p + \frac{p+1}{2} \leq r - p \leq -1$, i.e., $r(a) = r - p$. Assim, fica mais evidente que se $r \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ então $r(a) = r > 0$, enquanto que se $r \in \left\{\frac{p+1}{2}, \ldots, p-2, p-1\right\}$ então $r(a) = r - p < 0$.

Lema 21.1 (Gauss II)**.** Sejam p primo ímpar e a inteiro ímpar tal que $\text{mdc}(a,p) = 1$. Seja

$$M = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{(p-1)a}{2p}\right].$$

Então $\left(\frac{a}{p}\right) = (-1)^M$.

Demonstração. Considere $S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}, S_a = \left\{a, 2a, \ldots, \frac{(p-1)a}{2}\right\}$. Para todo $j \in S$, temos

$$ja = p \cdot \left[\frac{ja}{p}\right] + R_j, 0 < R_j \leq p-1.$$

Não podemos ter $R_j = 0$ pois $\text{mdc}(a,p) = \text{mdc}(j,p) = 1$. Escreva $R = \left\{R_1, R_2, \ldots, R_{\frac{p-1}{2}}\right\}$, o conjunto dos restos, e escreva $R = A \cup B$ (união disjunta) com

$$A = \left\{R_j \in R \mid 1 \leq R_j \leq \frac{p-1}{2}\right\} = \{s_1, s_2, \ldots, s_\delta\},$$
$$B = \left\{R_j \in R \mid \frac{p+1}{2} \leq R_j \leq p-1\right\} = \{n_1, n_2, \ldots, n_\mu\},$$

de modo que $\delta + \mu = \dfrac{p-1}{2}$. Seja $r_j = r(ja)$ o resto principal de $ja \in S_a$ módulo p. Pela observação acima, temos que A é o conjunto de restos principais positivos e $N = \{n_1 - p, \ldots, n_\mu - p\}$ é o conjunto de restos principais negativos, com $n_j \in B$.

Na demonstração do Lema de Gauss, mostramos que

$$S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \left\{|r_1|, |r_2|, \ldots, |r_{\frac{p-1}{2}}|\right\},$$

de modo que $S = \{s_1, \ldots, s_\delta, p - n_1, p - n_2, \ldots, p - n_\mu\}$ pois $|n_j - p| = p - n_j$ já que $\dfrac{p+1}{2} \leq n_j \leq p-1$. Logo,

$$\sum_{i=1}^{\frac{p-1}{2}} i = \sum_{i=1}^{\frac{p-1}{2}} |r_i| = s_1 + \cdots + s_\delta + \mu p - (n_1 + \cdots + n_\mu).$$

Por outro lado, temos

$$\sum_{i=1}^{\frac{p-1}{2}} ia = p\left(\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right]\right) + \sum_{i=1}^{\frac{p-1}{2}} R_i,$$

de modo que

$$a\sum_{i=1}^{\frac{p-1}{2}} i = pM + (s_1 + \cdots + s_\delta) + (n_1 + \cdots + n_\mu).$$

Segue que

$$\frac{p^2-1}{8}(a-1) = p(M - \mu) + 2(n_1 + \cdots + n_\mu).$$

Como p é primo ímpar e a é ímpar, o lado esquerdo da igualdade é par. Assim, devemos ter $M - \mu$ par, ou seja, M e μ de mesma paridade. Daí, segue do Lema de Gauss que

$$(-1)^M = (-1)^\mu = \left(\frac{a}{p}\right).$$

□

Exemplo. Calcule $\left(\dfrac{3}{37}\right)$ usando o Lema de Gauss II.

Solução. Como $\frac{p-1}{2} = 18$, temos de calcular

$$M = \sum_{j=1}^{18} \left[\frac{3j}{37}\right].$$

Note que para todo $j \leq 12$, essa parte inteira é nula. Logo,

$$M = \sum_{j=13}^{18} \left[\frac{3j}{37}\right].$$

Por outro lado, note que se $\left[\frac{3j}{37}\right] \geq 2$ então $j \geq 25$. Como $13 \leq j \leq 18$, segue que

$$M = 1 + 1 + 1 + 1 + 1 + 1 = 6$$

e, daí,

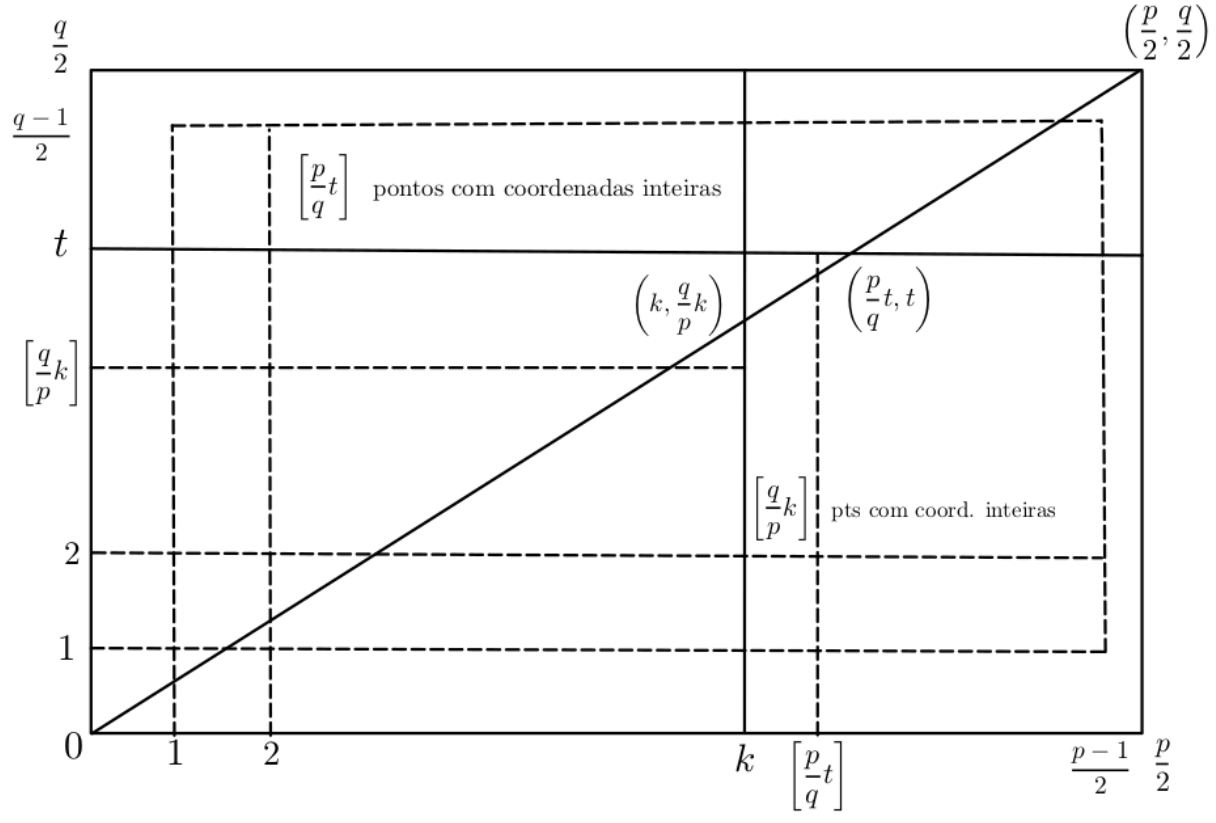
$$\left(\frac{3}{37}\right) = (-1)^6 = 1,$$

como já esperávamos.

Teorema 21.2 (Lei da Reciprocidade Quadrática - LRQ)**.** Sejam p, q primos ímpares distintos. Então

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Demonstração. Considere o retângulo $ABCD$ com vértices em $(0,0), (0,p/2), (0,q/2), (p/2,q/2)$.



A equação da reta por $(0,0),(p/2,q/2)$ é $y = x(q/p)$. Como $p/2, q/2 \notin \mathbb{Z}$, os pontos interiores ao retângulo com coordenadas inteiras são aqueles no produto cartesiano

$$Z = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \times \left\{1, 2, \ldots, \frac{p-1}{2}\right\},$$

de modo que

$$|Z| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Uma observação importante é que nenhum ponto de Z está sobre a reta $y = x(q/p)$. Queremos contar a quantidade de pontos de Z de uma maneira diferente e aplicar o Lema de Gauss II.

Considerando a região entre a reta vertical $x_0 = k$ e abaixo da reta $y = x(q/p)$, sabemos que há $\left[\frac{q}{p} \cdot k\right]$ pontos com coordenadas inteiras. Logo, no interior de ΔABC há

$$M_0 = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right]$$

pontos com coordenadas inteiras. Analogamente, considerando a reta horizontal $y_0 = t$, vemos que há exatamente

$$M_1 = \sum_{i=1}^{\frac{q-1}{2}} \left[\frac{ip}{q}\right]$$

pontos com coordenadas inteiras no triângulo δADC. Logo,

$$M_0 + M_1 = |Z| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

e, do Lema de Gauss II, segue que

$$\left(\frac{q}{p}\right) = (-1)^{M_0}, \left(\frac{p}{q}\right) = (-1)^{M_1},$$

de modo que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M_0+M_1} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

□

Lema 21.3. Seja p primo ímpar, $p \geq 5$. Então

$$\left(\frac{3}{37}\right) = 1 \iff p \equiv \pm 1 \bmod 12.$$

Demonstração. Vamos dividir em casos.

(i) $p \equiv 1 \bmod 3$ Nesse caso, $\left(\frac{p}{3}\right) = 1$. Pela LRQ,

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \Longrightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Logo,

$$\left(\frac{3}{p}\right) = 1 \Longleftrightarrow p \equiv 1 \bmod 4 \Longrightarrow p \equiv 1 \bmod 12 \text{ pois } p \equiv 1 \bmod 3.$$

(ii) $p \equiv -1 \bmod 3$ Nesse caso, $\left(\frac{p}{3}\right) = -1$. Pela LRQ,

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \Longrightarrow \left(\frac{3}{p}\right) = -(-1)^{\frac{p-1}{2}}.$$

Logo,

$$\left(\frac{3}{p}\right) = 1 \Longleftrightarrow p \equiv -1 \bmod 4 \Longrightarrow p \equiv -1 \bmod 12 \text{ pois } p \equiv -1 \bmod 3.$$

□

Exemplo. A congruência $x^2 \equiv 56 \bmod 547$ tem solução?

Solução. Temos que 547 é primo e $56 = 2^3 \cdot 7$, logo

$$\left(\frac{56}{547}\right) = \left(\frac{2^3}{547}\right)\left(\frac{7}{547}\right) = \left(\frac{2}{547}\right)\left(\frac{7}{547}\right).$$

Como $547 \not\equiv 1 \bmod 8$, segue do Lema (20.7) que $\left(\frac{2}{547}\right) = -1$. Pela LRQ,

$$\left(\frac{7}{547}\right)\left(\frac{547}{7}\right) = (-1)^{273 \cdot 3} = -1.$$

Como $547 \equiv 1 \bmod 7$, então $\left(\frac{547}{7}\right) = 1$, logo $\left(\frac{7}{547}\right) = -1$ e $\left(\frac{56}{547}\right) = 1$. Logo, a congruência tem solução.

Exemplo. A congruência $3x^2 \equiv 466 \bmod 467$ tem solução?

Solução. Precisamos primeiro reescrever a congruência no formato $x^2 \equiv b \bmod 467$ para aplicar a teoria. O primeiro passo é resolver $3z \equiv 1 \bmod 467$, obtemos $z = 156$. Como $466 \equiv -1 \bmod 467$, então $3x^2 \equiv 466 \bmod 467$ é equivalente a $x^2 \equiv -156 \bmod 467$. Determinar se esta congruência tem solução é equivalente a determinar $\left(\frac{-156}{467}\right)$. Note que $156 = 3 \cdot 4 \cdot 13$, logo

$$\left(\frac{-156}{467}\right) = \left(\frac{-1}{467}\right)\left(\frac{3}{467}\right)\left(\frac{13}{467}\right), \text{ pois 4 é quadrado.}$$

Pelos Lemas (20.2) e (21.3), $467 \not\equiv 1 \bmod 4$ e $467 \equiv 1 \bmod 12$, logo

$$\left(\frac{-156}{467}\right) = -\left(\frac{13}{467}\right).$$

Pela LRQ,

$$\left(\frac{13}{467}\right)\left(\frac{467}{13}\right) = (-1)^{6\cdot 233} = 1,$$

ou seja,

$$\left(\frac{13}{467}\right) = \left(\frac{467}{13}\right).$$

Note que $467 \equiv -1 \bmod 13$ e $13 \equiv 1 \bmod 4$, logo

$$\left(\frac{467}{13}\right) = \left(\frac{-1}{13}\right) = 1.$$

Daí, segue que

$$\left(\frac{-156}{467}\right) = -\left(\frac{13}{467}\right) = -1,$$

e a congruência não tem solução.