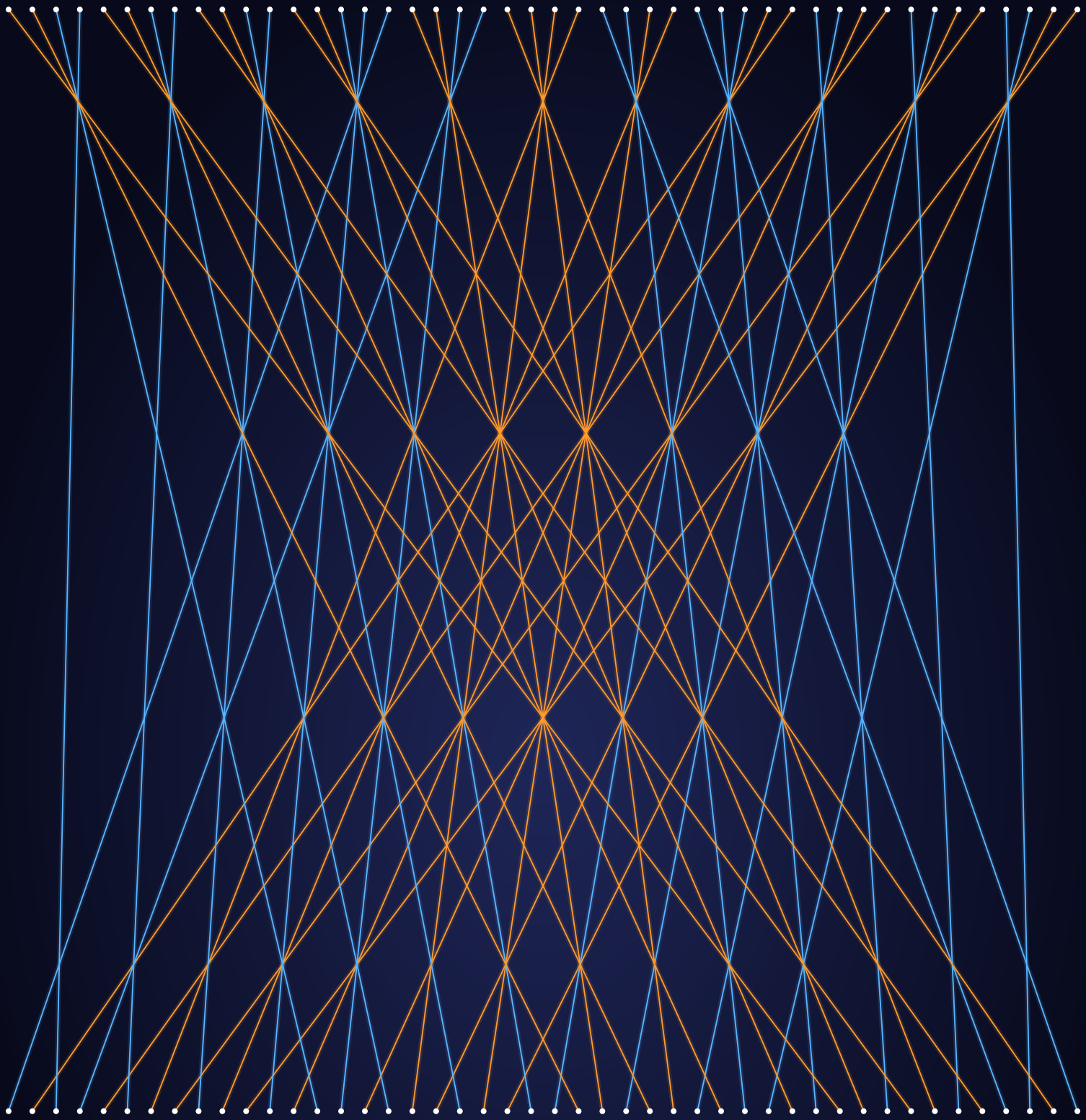


Teoria dos Números

Ramon M. Nunes

Versão de 16 de novembro de 2026

Página intencionalmente deixada em branco.

Teoria dos Números

Ramon M. Nunes

Versão de 16 de novembro de 2026

Página intencionalmente deixada em branco.

Índice

Sobre este livro **iv**

1 Divisibilidade **1**
1.1 Indução . . . 1
1.2 Divisibilidade . . . 2
1.3 Algoritmo da Divisão . . . 3
1.4 Máximo Divisor Comum . . . 4
1.4.1 Propriedades do mdc . . . 6
1.4.2 Algoritmo de Euclides . . . 7
1.4.3 O mdc como Combinação Linear . . . 8
1.5 Números Primos . . . 9
1.5.1 Infinitude dos Primos . . . 11
1.5.2 Teste de Primalidade . . . 12
1.5.3 Crivo de Eratóstenes . . . 12
1.6 Mínimo Múltiplo Comum (mmc) . . . 13
1.7 Divisores de um Produto . . . 13
1.8 Critérios de Divisibilidade . . . 14
1.8.1 Divisibilidade por 2 e 5 . . . 14
1.8.2 Divisibilidade por 9 e 3 . . . 14
1.8.3 Divisibilidade por 4 . . . 15
1.8.4 Divisibilidade por 11 . . . 15
1.8.5 Divisibilidade por 7 . . . 15
1.9 Representação de um Número em Base b . . . 16
1.10 Exercícios . . . 17

2 Congruências **21**
2.1 Definição e Propriedades Básicas . . . 21
2.2 Sistema Completo de Restos (SCR) . . . 22
2.3 Congruências Lineares . . . 24
2.4 Outras Propriedades das Congruências . . . 26
2.5 Teoremas de Fermat e Euler . . . 27
2.6 Sistema Reduzido de Restos (SRR) . . . 29
2.7 Teorema de Wilson . . . 30
2.8 Teorema Chinês dos Restos . . . 31
2.9 Cálculo de $\phi(m)$ . . . 35
2.10 Congruências Módulo Potência de Primo . . . 37
2.10.1 Motivação . . . 37
2.10.2 Derivada de um Polinômio . . . 38

2.10.3 O Lema de Hensel . . . 38
2.10.4 Exemplo: $x^3 + 3x + 1 \equiv 0 \pmod{7^3}$ . . . 39
2.10.5 Variações do Lema de Hensel . . . 40
2.10.6 Exemplo: $x^2 + x + 223 \equiv 0 \pmod{3^j}$ . . . 41
2.11 Congruências Polinomiais Módulo p . . . 42
2.11.1 Número de Soluções de $f(x) \equiv 0 \pmod{p}$ . . . 43
2.11.2 Fatoração de $x^p - x$ e Algoritmo da Divisão . . . 44
2.11.3 Caracterização do Número Máximo de Soluções . . . 45
2.11.4 Resumo dos Resultados sobre Congruências Polinomiais . . . 46
2.11.5 Aplicação: Soluções de $x^d - 1 \equiv 0 \pmod{p}$ . . . 46
2.11.6 Propriedades dos Coeficientes e Teorema de Wolstenholme . . . 46
2.12 Exercícios . . . 47

3 Raízes Primitivas **54**
3.1 Ordem de um Elemento . . . 54
3.2 Raízes Primitivas . . . 56
3.3 Resíduos Potência n-ésima . . . 57
3.3.1 Exemplo: $x^6 \equiv 5 \pmod{11}$ . . . 59
3.4 Cálculo da Ordem de Elementos . . . 59
3.5 Raízes Primitivas Módulo p^2 . . . 60
3.6 Raízes Primitivas Módulo p^k . . . 62
3.7 Raízes Primitivas Módulo Potências de 2 . . . 62
3.8 Módulos Gerais . . . 63
3.9 Exercícios . . . 65

4 Resíduos Quadráticos **68**
4.1 Definição e Primeiros Exemplos . . . 68
4.2 Símbolo de Legendre . . . 69
4.3 Lema de Gauss . . . 70
4.4 Lema de Eisenstein . . . 72
4.5 Lei da Reciprocidade Quadrática . . . 73
4.6 Formas Equivalentes e Valores Pequenos . . . 76
4.6.1 Símbolo para $a = 2, 3, 5, 7$ . . . 76
4.7 Símbolo de Jacobi . . . 77
4.7.1 Propriedades do Símbolo de Jacobi . . . 78
4.7.2 Lei da Reciprocidade Quadrática para o Símbolo de Jacobi . . . 79
4.8 O Menor Resíduo Não-Quadrático . . . 80

5 Funções Aritméticas **81**
5.1 Definição e Exemplos Iniciais . . . 81
5.2 Função Parte Inteira . . . 81
5.2.1 Aplicação: Maior Potência de um Primo p que Divide $n!$ (Fórmula de Legendre) . . . 82
5.3 Outros Exemplos de Funções Aritméticas . . . 83
5.4 Funções Multiplicativas . . . 83
5.4.1 Cálculo a Partir da Fatoração em Primos . . . 84
5.5 Convolução de Dirichlet . . . 85
5.6 Função de Möbius e Fórmula de Inversão . . . 87
5.7 Inversa de Dirichlet . . . 88

5.8 Exercícios 88

6 Representação de Inteiros como Soma de Quadrados **91**
6.1 Resultados Principais 91
6.1.1 Tabela de Exemplos ($n = 1$ a 20) 92
6.2 Demonstração do Teorema dos Dois Quadrados 92
6.3 Soma de Quatro Quadrados 94
6.3.1 Identidade dos Quatro Quadrados de Euler 94
6.3.2 Teorema de Lagrange 94
6.4 Número de Representações como Soma de Dois Quadrados 96
6.4.1 Recapitulação e Objetivo 96
6.4.2 Proposições Auxiliares 96
6.4.3 Unicidade da Representação de Primos 97
6.4.4 Fórmula para o Número de Soluções $r(n)$ 98
6.5 Exercícios 98

Bibliografia **100**

Sobre este livro

Estas notas foram tomadas enquanto eu ministrava a disciplina de Introdução à Teoria dos Números no Bacharelado em Matemática da Universidade Federal do Ceará (UFC).

O texto foi feito a partir de fotos, que foram transformadas em LaTeX com a ajuda do Gemini. Outras alterações foram feitas com a ajuda do Claude.

Capítulo 1

Divisibilidade

1.1 Indução

Três formas equivalentes de indução:
1. Princípio da indução:
Digamos que P é uma propriedade sobre números. Suponha que:

i) O número 1 satisfaz a propriedade P.

ii) Sempre que o número n satisfaz a propriedade P, o número $n+1$ também satisfaz.

Então todos os inteiros positivos satisfazem a propriedade P.

Exemplos.

$$1 + x + x^2 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}$$

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

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

2. Princípio da Indução forte:
Digamos que P é uma propriedade sobre números. Suponha que:

i) O número 1 satisfaz a propriedade P.

ii) Se os números $1, 2, 3, \ldots, n$ satisfazem P, então $n+1$ satisfaz P.

Então todos os inteiros positivos satisfazem P.

Exemplo (detalhes no Teorema 17)**.** Teorema Fundamental da Aritmética: Todo número inteiro maior que 1 se escreve como produto de números primos.

3. Princípio da Boa ordem:
Todo conjunto não-vazio de inteiros positivos possui um menor elemento.

Teorema 1. *Os princípios 1, 2 e 3 são equivalentes (ver [San98, Apêndice A]).*

1.2 Divisibilidade

$\mathbb{Z}$ = conjunto dos números inteiros = $\{\dots, -2, -1, 0, 1, 2, 3, \dots\}$
$\mathbb{N} = \mathbb{Z}_{>0}$ = conjunto dos inteiros positivos = $\{1, 2, 3, \dots\}$.

Definição. Sejam a e b números inteiros, dizemos que a divide b (denotamos $a|b$) se existe um número inteiro c tal que $b = a \cdot c$. Se a não divide b, denotamos $a \nmid b$.

Exemplos.

- $1|b$ para qualquer b, pois $1 \cdot b = b$.
- $a|0$ para qualquer a, pois $a \cdot 0 = 0$.
- $2 \nmid 3$. De fato, se $c \leq 1$, então $2c \leq 2$. Se $c \geq 2$, então $2c \geq 4$. Ou seja, para inteiros temos 2 possibilidades:

$$2c \leq 2 \text{ ou } 2c \geq 4.$$

Assim, não é possível que $2c = 3$.

Proposição 2 (Transitividade)**.** *Se a, b, c são inteiros tais que $a|b$ e $b|c$, então $a|c$.*

Demonstração. Como $a|b$, existe um inteiro d tal que $a \cdot d = b$. Da mesma maneira, como $b|c$, existe um inteiro e tal que $b \cdot e = c$. Substituindo a primeira na segunda:

$$a(d \cdot e) = c.$$

Pondo $f = d \cdot e$ (inteiro), temos $a \cdot f = c$. Conclusão: $a|c$. □

Exemplo. $2|6$ e $6|30 \implies 2|30$ (De fato, $30 = 2 \cdot 15$).

Proposição 3. *Sejam a, b, c, m, n inteiros. Se $a|b$ e $a|c$, então $a|(mb + nc)$.*

Demonstração. Como $a|b$, existe $d \in \mathbb{Z}$ tal que $b = ad$. Como $a|c$, existe $e \in \mathbb{Z}$ tal que $c = ae$. Substituindo em $mb + nc$:

$$mb + nc = m(ad) + n(ae) = a(md + ne).$$

Como a soma de produtos de inteiros é um inteiro, tomando $f = md + ne$, temos que $a|mb + nc$. □

Exemplo. $3|15$ e $3|42 \implies 3|(8 \cdot 15 - 7 \cdot 42) = 3|(-174)$.

Observação. Mesmo que $2 \cdot \frac{3}{2} = 3$, isso não quer dizer que 2 divide 3, pois $\frac{3}{2}$ não é um número inteiro.

Proposição 4. *Sejam a, d, n inteiros. Então:*

i) $n|n$

ii) se $d|n$ então $ad|an$

iii) se $ad|an$ e $a \neq 0$, então $d|n$

iv) $1|n$

v) $n|0$

vi) *se* $d|n$ *e* $n \neq 0$, *então* $|d| \leq |n|$

vii) *se* $d|n$ *e* $n|d$, *então* $|d| = |n|$ *(ou seja,* $d = \pm n$*)*

viii) *se* $d|n$ *e* $d \neq 0$, *então* $\frac{n}{d}$ *é inteiro e* $\frac{n}{d}|n$

Demonstração. i), iv) e v) são imediatos.

ii) Se $d|n$, existe c inteiro tal que $dc = n$. Multiplicando por a:

$$adc = an \implies (ad)c = an \implies ad|an.$$

iii) Se $ad|an$, existe c inteiro tal que

$$adc = an \implies a(dc - n) = 0.$$

Como $a \neq 0$, temos

$$dc - n = 0 \implies dc = n \implies d|n.$$

vi) Lembre que

$$|0| = 0, \quad |\pm 1| = 1, \quad |\pm 2| = 2, \quad |\pm 3| = 3, \quad \ldots.$$

Assim, se $c \neq 0$, então $|c| \geq 1$. Como $d|n$, existe c tal que

$$n = dc \implies |n| = |d| \cdot |c|.$$

Como $n \neq 0$, temos $c \neq 0 \implies |c| \geq 1$. Assim, $|n| = |d| \cdot |c| \geq |d| \cdot 1 \implies |n| \geq |d|$.

vii) Os casos em que $n = 0$ ou $d = 0$ ficam como exercício. Suponha agora que $n \neq 0$ e $d \neq 0$. Por vi), $|d| \leq |n|$ e $|n| \leq |d|$. Logo $|d| = |n|$.

viii) Se $d|n$, existe c inteiro tal que $n = dc$. Considerando essa igualdade em números racionais, nota-se que $\frac{n}{d} = c$. Como c é inteiro e $\frac{n}{d} \cdot d = n$, temos $\frac{n}{d} \mid n$.

□

1.3 Algoritmo da Divisão

Vamos começar com alguns exemplos.

- 11 não é múltiplo de 2, mas 10 é $(10 = 2 \cdot 5)$.
  Além disso, temos $11 = 2 \cdot 5 + 1$.
- 704 não é múltiplo de 3, mas 702 é $(702 = 3 \cdot 234)$.
  Além disso, temos $704 = 3 \cdot 234 + 2$.
- 897 não é múltiplo de 11, mas 891 é $(891 = 11 \cdot 81)$.
  Além disso, temos $897 = 11 \cdot 81 + 6$.

Teorema 5 (Algoritmo da divisão)**.** *Dados inteiros a e b com $b > 0$, existe um único par de inteiros q, r tais que:*

$$\begin{cases} a = bq + r, \\ 0 \leq r < b. \end{cases}$$

q e r são chamados, respectivamente, de quociente e resto da divisão de a por b.

Demonstração. Considere o conjunto

$$\mathcal{B} = \{n \in \mathbb{Z};\ n = bq - a \text{ para algum } q \in \mathbb{Z},\ n > 0\}.$$

Veja que $\mathcal{B}$ é infinito pois $\{n = bq;\ q > 0\}$ é infinito e o conjunto $\{1, 2, \ldots, a\}$ é finito. Portanto existem elementos no primeiro conjunto que não estão no segundo. Ou seja, existe q inteiro tal que $bq > a \iff bq - a > 0$. Isto é, um elemento de $\mathcal{B}$. Agora, como $\mathcal{B}$ é não-vazio, pelo Princípio da Boa Ordem, $\mathcal{B}$ possui um menor elemento n_0. Escreva $n_0 = bq_0 - a$. Por definição, $n_0 - b = b(q_0 - 1) - a$ não está em $\mathcal{B}$. Ou seja, $b(q_0 - 1) - a \leq 0$. Afirmação: Tomando $q = q_0 - 1$ e $r = a - bq$, obtemos o resultado desejado. De fato, por definição, $a = bq + r$. Por outro lado, sabemos que $b(q_0 - 1) - a \leq 0$ e $bq_0 - a > 0$. Lembrando que $q = q_0 - 1$, temos

$$bq - a \leq 0 \iff a - bq \geq 0 \iff r \geq 0.$$

Do mesmo modo,

$$b(q + 1) - a > 0 \iff a - bq < b \iff r < b.$$

Isso conclui a prova da existência de q e r.

Provemos agora a unicidade: Suponha que existam q_1, q_2, r_1, r_2 tais que:

$$\begin{aligned} a = bq_1 + r_1 = bq_2 + r_2, \\ 0 \leq r_1, r_2 < b. \end{aligned} \tag{$\star$}$$

A partir das igualdades acima, segue que

$$b(q_1 - q_2) = r_2 - r_1.$$

Isso implica que $b|(r_2 - r_1)$. Pela Proposição 4 (item vi), segue que ou temos $r_2 - r_1 = 0$ ou $b = |b| \leq |r_2 - r_1|$. Vamos mostrar que o segundo caso não pode ocorrer. Usando as desigualdades ($\star$),

$$-b = 0 - b < r_2 - r_1 < b - 0 = b.$$

Ou seja, $|r_2 - r_1| < b$. Portanto, tem-se que $r_1 = r_2$. Consequentemente, $b(q_1 - q_2) = 0$, e como $b > 0$, temos $q_1 = q_2$.

□

Exercício 1. O número q obtido pelo algoritmo da divisão é dado por $\lfloor \frac{a}{b} \rfloor$.

1.4 Máximo Divisor Comum

Definição. Dados inteiros a e b com $a \neq 0$ ou $b \neq 0$, o máximo divisor comum (mdc) de a e b é o maior inteiro positivo que divide a e b simultaneamente. Notação: $\text{mdc}(a, b)$ ou (a, b).

Observação. Para garantir a existência do mdc, devemos mostrar que o conjunto dos divisores comuns

$$\mathcal{D} = \{d \in \mathbb{Z};\ d \mid a \text{ e } d \mid b\}$$

é não-vazio e finito.

- **NÃO-VAZIO**: O número 1 sempre pertence ao conjunto. De fato, $1 > 0$, $1|a$ e $1|b$ para quaisquer a, b.
- **FINITO**: Se $a \neq 0$, pela Proposição 4 (item vi), qualquer divisor d satisfaz $|d| \leq |a|$. Se $a = 0$, temos por hipótese que $b \neq 0$. Logo $|d| \leq |b|$. Em ambos os casos, o conjunto é limitado e, portanto, possui um elemento máximo.

Teorema 6 (Teorema de Bézout)**.** *Sejam a e b inteiros, não ambos nulos, e $d = \text{mdc}(a, b)$. Então existem inteiros m e n tais que:*

$$d = am + bn.$$

Demonstração. Seja $\mathcal{B} = \{r \in \mathbb{Z}_{>0};\ r = am + bn, m, n \in \mathbb{Z}\}$. Pelo Princípio da Boa Ordem, $\mathcal{B}$ tem um menor elemento $c = am_0 + bn_0$ ($\mathcal{B}$ é não-vazio, pois $a^2 + b^2 \in \mathcal{B}$). Vamos provar que $c|a$ e $c|b$. Pelo algoritmo da divisão, existem q, r tais que $a = cq + r$ com $0 \leq r < c$. Se $r > 0$, então $r = a - cq = a - (am_0 + bn_0)q = a(1 - m_0q) + b(-n_0q) \in \mathcal{B}$. Mas $r < c$, o que contradiz a minimalidade de c. Logo $r = 0$ e $c|a$. De modo análogo, $c|b$. Como d é o máximo divisor comum e c é um divisor comum, $c \leq d$. Por outro lado, como $d|a$ e $d|b$, temos $d|(am_0 + bn_0)$, ou seja, $d|c$. Como $c > 0$, $d \leq c$. Conclusão: $d = c = am_0 + bn_0$. □

Observação. Qualquer divisor comum de a e b divide o $\text{mdc}(a, b)$.

Exemplo. $a = 30, b = 140$.
Divisores de 30: $1, 2, 3, 5, 6, 10, 15, 30$.
Divisores de 140: $1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, 140$.
Divisores comuns: $1, 2, 5, 10$, $\text{mdc}(30, 140) = 10$.
Note que todos os divisores comuns dividem 10.

Proposição 7. *Para todo inteiro positivo t,*

$$\text{mdc}(ta, tb) = t \cdot \text{mdc}(a, b).$$

Demonstração. Seja $d = \text{mdc}(a, b)$. Como $d \mid a$, segue que $td \mid ta$. Analogamente, temos que $td \mid tb$. Ou seja, td é um divisor comum de ta e tb. Em particular, pela definição de máximo divisor comum, temos:

$$td \leq \text{mdc}(ta, tb).$$

Pelo Teorema de Bézout, existem inteiros m, n tais que $d = am + bn$. Multiplicando a igualdade acima por t, obtemos:

$$td = t(am + bn) = (ta)m + (tb)n.$$

Como $\text{mdc}(ta, tb)$ é um divisor comum de ta e tb, ele divide qualquer combinação linear de ta e tb. Logo, $\text{mdc}(ta, tb)|td$. Considerando que $td > 0$, o item vi da Proposição 4 nos diz que:

$$\text{mdc}(ta, tb) \leq |td| = td.$$

Como mostramos que $td \leq \text{mdc}(ta, tb)$ e $\text{mdc}(ta, tb) \leq td$, segue que $\text{mdc}(ta, tb) = td$. Substituindo d, concluímos que $\text{mdc}(ta, tb) = t \cdot \text{mdc}(a, b)$. □

Corolário 8. *Se $c|a$ e $c|b$ com $c > 0$, então:*

$$\text{mdc}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{mdc}(a,b)}{c}.$$

Em particular, se $d = \text{mdc}(a,b)$, então $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

1.4.1 Propriedades do mdc

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

Definição. Sejam $a_1, a_2, \ldots, a_n$ números inteiros, pelo menos um dos quais é não-nulo. O *máximo divisor comum* de $a_1, \ldots, a_n$, denotado por $\text{mdc}(a_1, \ldots, a_n)$ ou $(a_1, \ldots, a_n)$, é o maior inteiro positivo que divide $a_1, a_2, \ldots, a_n$ simultaneamente.

Exemplo. Sejam $a_1 = 12, a_2 = 36, a_3 = 42$.

- Divisores de 12: $1, 2, 3, 4, 6, 12$
- Divisores de 36: $1, 2, 3, 4, 6, 9, 12, 18, 36$
- Divisores de 42: $1, 2, 3, 6, 7, 14, 21, 42$

O maior divisor comum entre eles é $\text{mdc}(12, 36, 42) = 6$.

Proposição 9. *Seja $d = \text{mdc}(a_1, \ldots, a_n)$. Então existem inteiros $m_1, \ldots, m_n$ tais que:*

$$d = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n.$$

Demonstração. Exercício (segue os mesmos passos do caso $n = 2$). □

Assim como no caso $n = 2$, vale a fórmula de homogeneidade:

$$\text{mdc}(ta_1, ta_2, \ldots, ta_n) = t \cdot \text{mdc}(a_1, a_2, \ldots, a_n)$$

para qualquer inteiro positivo t.

Proposição 10. *Dados inteiros a, b, c, temos:*

$$\text{mdc}(a,b) = \text{mdc}(a, b + ac).$$

Demonstração. Sejam

$$\mathcal{D} = \{ma + nb : m, n \in \mathbb{Z}\},$$
$$\mathcal{D}' = \{ma + n(b + ac) : m, n \in \mathbb{Z}\}.$$

Sabemos que $\text{mdc}(a,b)$ é o menor elemento positivo de $\mathcal{D}$ e $\text{mdc}(a, b + ac)$ é o menor elemento positivo de $\mathcal{D}'$. Logo, é suficiente mostrar que $\mathcal{D} = \mathcal{D}'$.

Seja $t \in \mathcal{D}'$. Então existem inteiros m, n tais que:

$$t = ma + n(b + ac) = (m + nc)a + nb.$$

Como $m + nc$ e n são inteiros, isso implica que $t \in \mathcal{D}$, logo $\mathcal{D}' \subseteq \mathcal{D}$.

Reciprocamente, se $t \in \mathcal{D}$, existem inteiros m, n tais que:

$$t = ma + nb = ma - nac + nb + nac = (m - nc)a + n(b + ac).$$

Como $m - nc$ e n são inteiros, temos $t \in \mathcal{D}'$, logo $\mathcal{D} \subseteq \mathcal{D}'$. Isso conclui a prova de que $\mathcal{D} = \mathcal{D}'$. □

Corolário 11. *Sejam a, b inteiros e r o resto da divisão de a por b. Então*

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

Proposição 12. *Dados $a_1, \ldots, a_n, q_1, \ldots, q_{n-1}$ inteiros, vale:*

$$\text{mdc}(a_1, \ldots, a_{n-1}, a_n) = \text{mdc}(a_1, \ldots, a_{n-1}, a_1q_1 + \cdots + a_{n-1}q_{n-1} + a_n).$$

Demonstração. A prova é análoga ao caso anterior. □

Exercício 2. Mostre que dados inteiros a, b, x, y, z, w tais que $xw - yz = 1$, vale a igualdade:

$$\text{mdc}(a, b) = \text{mdc}(xa + yb, za + wb).$$

1.4.2 Algoritmo de Euclides

O que é: É um algoritmo para encontrar o mdc de dois inteiros a e b.

Como funciona: Construímos uma sequência de restos da seguinte forma:

1. $r_0 = a, r_1 = |b|$.
2. r_{n+1} = resto da divisão de r_{n-1} por r_n.

O processo continua até que $r_n = 0$ para algum $n \geq 1$. O mdc de a e b é o último resto não nulo.

Exemplo. $a = 84$, $b = 58$.

- $r_0 = 84$, $r_1 = 58$.
- $84 = 58 \cdot 1 + 26 \implies r_2 = 26$
- $58 = 26 \cdot 2 + 6 \implies r_3 = 6$
- $26 = 6 \cdot 4 + 2 \implies r_4 = 2$
- $6 = 2 \cdot 3 + 0 \implies r_5 = 0$

Conclusão: $\text{mdc}(84, 58) = 2$.

Exemplo. Calcular $\text{mdc}(1126, 522)$:

- $r_0 = 1126$, $r_1 = 522$.
- $1126 = 522 \cdot 2 + 82 \implies r_2 = 82$
- $522 = 82 \cdot 6 + 30 \implies r_3 = 30$
- $82 = 30 \cdot 2 + 22 \implies r_4 = 22$
- $30 = 22 \cdot 1 + 8 \implies r_5 = 8$
- $22 = 8 \cdot 2 + 6 \implies r_6 = 6$
- $8 = 6 \cdot 1 + 2 \implies r_7 = 2$

- $6 = 2 \cdot 3 + 0 \implies r_8 = 0$

Conclusão: $\text{mdc}(1126, 522) = 2$.

Teorema 13. *O algoritmo de Euclides funciona. Ou seja, se a e b são inteiros com $b \neq 0$, o processo termina após um número finito de passos e o último resto não nulo é* $\text{mdc}(a, b)$.

Prova do Teorema. Primeiro vamos mostrar que se n_0 é o menor inteiro tal que $r_{n_0} = 0$, então $r_{n_0-1} = \text{mdc}(a, b)$. Pelo corolário da proposição anterior, temos:

$$\text{mdc}(a, b) = \text{mdc}(r_0, r_1) = \text{mdc}(r_1, r_2) = \cdots = \text{mdc}(r_{n_0-1}, r_{n_0}).$$

Como $r_{n_0} = 0$, temos então que

$$\text{mdc}(a, b) = \text{mdc}(r_{n_0-1}, 0) = r_{n_0-1}.$$

Resta mostrar que o processo termina (ou seja, que n_0 existe). Note que ao efetuar a divisão de a por b, o resto r satisfaz

$$0 \leq r < |b|.$$

Deste modo, se tivéssemos que $r_n \neq 0$ para todo n, teríamos uma sequência infinita de inteiros positivos estritamente decrescente:

$$|b| = r_1 > r_2 > r_3 > r_4 > \cdots > 0.$$

O que é um absurdo. □

1.4.3 O mdc como Combinação Linear

O algoritmo de Euclides nos dá uma forma efetiva de encontrar os coeficientes da combinação linear $d = am + bn$.

Exemplo. Sejam, mais uma vez, $a = 84, b = 58$. Do algoritmo de Euclides, temos:

(1) $26 = 84 - 58$

(2) $6 = 58 - 2 \cdot 26$

(3) $2 = 26 - 4 \cdot 6$

Substituindo (2) em (3):

$$2 = 26 - 4(58 - 2 \cdot 26) = 26 - 4 \cdot 58 + 8 \cdot 26 = 9 \cdot 26 - 4 \cdot 58.$$

Substituindo (1) no resultado:

$$2 = 9(84 - 58) - 4 \cdot 58 = 9 \cdot 84 - 9 \cdot 58 - 4 \cdot 58 = 9 \cdot 84 - 13 \cdot 58.$$

Ou seja:

$$\text{mdc}(84, 58) = 2 = 9 \cdot 84 + (-13) \cdot 58.$$

1.5 Números Primos

Definição. Um número inteiro positivo $n > 1$ é chamado de **primo** se n possui exatamente 2 divisores positivos: 1 e n. Se $n > 1$ não é primo, dizemos que n é **composto**.

Exemplos.

- 2, 3, 5 são primos (basta testar).
- 4 e 6 são compostos (visto que $2|4$ e $2|6$).

Proposição 14 (Lema de Euclides)**.** *Seja p um número primo e sejam a, b inteiros tais que $p|ab$. Então $p|a$ ou $p|b$.*

Observação. A proposição acima não vale sem a hipótese de que p é primo. Por exemplo, $6|2 \cdot 3$, mas $6 \nmid 2$ e $6 \nmid 3$.

A proposição acima segue do seguinte resultado sobre mdc:

Proposição 15 (Lema de Euclides, versão geral)**.** *Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração. Pelo Teorema de Bézout, existem m, n inteiros tais que:

$$am + bn = 1.$$

Multiplicando a igualdade por c:

$$acm + bcn = c.$$

Como $a|bc$, segue que a divide os dois termos do lado esquerdo da igualdade ($a|acm$ e $a|bcn$). Portanto, $a|c$. □

Prova do Lema de Euclides. Se $p|a$, não há nada a fazer. Se $p \nmid a$, segue que $(p, a) = 1$. De fato, (p, a) tem de ser 1 ou p. Como $(p, a) = p$ só ocorre quando $p|a$, temos necessariamente que $(p, a) = 1$. Segue, portanto, da Proposição 15 que $p|b$. □

Aplicando o Lema de Euclides repetidas vezes, temos o seguinte corolário

Corolário 16. *Seja p um número primo e sejam $a_1, \ldots, a_n$ inteiros tais que $p|a_1 \ldots a_n$. Então $p|a_i$ para algum i.*

Teorema 17 (Teorema Fundamental da Aritmética)**.** *Todo número inteiro $n > 1$ possui uma expressão como produto de números primos. Essa expressão é única a menos da ordem.*

Observação. Aqui consideramos que o produto pode consistir de um só elemento, o que ocorre exatamente quando n é primo. Será conveniente também considerar que o número 1 também se escreve de maneira única como produto (vazio) de números primos.

Demonstração. Vamos dividir a prova em duas partes: *existência* e *unicidade*.

Existência: A prova será por indução (forte).

- **Caso inicial:** $n = 2$. Então $2 = 2$ é uma expressão como produto de números primos.

- **Hipótese de indução:** Suponha que todo inteiro $1 < n \leq N$ possa ser escrito como produto de números primos.

- **Passo indutivo:** Seja $n = N + 1$. Se n é primo não há nada a fazer, $n = n$ é uma expressão de n como produto de números primos. Se n não é primo, significa que n possui um divisor d tal que $d \neq 1,\ d \neq n$. Ou seja, $1 < d < n$. Como $d \mid n$, $\frac{n}{d}$ é inteiro e satisfaz $1 < \frac{n}{d} < n$. Assim, pela hipótese de indução, tanto d quanto $\frac{n}{d}$ possuem expressões como produto de números primos:

  $$d = p_1 \cdots p_k,\ \frac{n}{d} = q_1 \cdots q_\ell.$$

  Multiplicando as duas equações, temos que

  $$n = p_1 \cdots p_k q_1 \cdots q_\ell,$$

  que é uma expressão de n como produto de números primos.

Unicidade: A prova será mais uma vez por indução (forte).

- **Caso inicial:** $n = 2$. Suponha que $2 = p_1 \cdots p_k$. Segue que $p_i \mid 2$ para todo i. Como 2 é primo e $p_i > 1$, segue que $p_i = 2$. Substituindo, segue que $k = 1$. Assim, temos que $2 = 2$ é a única expressão de 2 como produto de números primos.

- **Hipótese de indução:** Suponha que todo inteiro n com $1 < n \leq N$ admita uma única expressão como produto de números primos a menos da ordem.

- **Passo indutivo:** Seja $n = N + 1$. Suponha que

  $$n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_\ell,$$

  onde p_i e q_j são primos. Queremos mostrar que $k = \ell$ e que, após uma reordenação, $p_i = q_i$.

  Considere o primo p_1. Como p_1 divide n, temos que $p_1 \mid q_1 q_2 \ldots q_\ell$. Pelo corolário do Lema de Euclides, p_1 deve dividir algum q_j. Sem perda de generalidade (basta reordenar), suponha que $p_1 | q_1$.

  Como q_1 é primo, seus únicos divisores são 1 e q_1. Como $p_1 > 1$, concluímos que $p_1 = q_1$. Dividindo a igualdade original por p_1, obtemos:

  $$\frac{n}{p_1} = p_2 p_3 \ldots p_k = q_2 q_3 \ldots q_\ell.$$

  Se $\frac{n}{p_1} = 1$, então $k = \ell = 1$ e não há nada a provar. Caso contrário, pela hipótese de indução, $\frac{n}{p_1}$ possui uma única expressão como produto de números primos. Assim, segue que $k = \ell$ e $p_2, \ldots, p_k$ são iguais a $q_2, \ldots, q_\ell$ a menos de uma reordenação. Portanto, o mesmo vale para $p_1, \ldots, p_k$ e $q_1, \ldots, q_\ell$, concluindo a demonstração.

□

Observação. Agrupando os primos iguais, obtemos que todo inteiro $n > 1$ se escreve de maneira única como

$$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$$

onde p_i são primos distintos e $a_i \geq 1$. Esta expressão é chamada de **fatoração em primos** ou **decomposição canônica** de n.

Observação. Em alguns casos vai ser interessante escrever $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ com $a_i \geq 0$. Neste caso a expressão não será única.

Exemplo. $84 = 2^2 \cdot 3^1 \cdot 7^1 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1 = 2^2 \cdot 3^1 \cdot 7^1 \cdot 11^0$

Proposição 18. *Seja $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, com p_i primos distintos e $a_i \geq 0$. Então o conjunto dos divisores positivos de n é dado por*

$$\{p_1^{b_1} p_2^{b_2} \dots p_k^{b_k};\ 0 \leq b_i \leq a_i\}.$$

Demonstração. É fácil ver que se $d = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ com $0 \leq b_i \leq a_i$, então $n = dm$, onde

$$m = p_1^{a_1 - b_1} p_2^{a_2 - b_2} \dots p_k^{a_k - b_k}.$$

Seja agora d um divisor de n e seja $d = q_1^{c_1} q_2^{c_2} \dots q_\ell^{c_\ell}$ a fatoração em primos de d. Segue que $q_j \mid n$ para todo j. Argumentando como na prova da unicidade do Teorema Fundamental da Aritmética, é possível mostrar que $q_j = p_{i_j}$ para algum i_j, com todos os i_j distintos. Trocando cada q_j pelo p_{i_j} correspondente e, incluindo p_i^0 quando p_i não aparecer em $q_1, q_2, \dots, q_\ell$, é possível escrever $d = p_1^{b_1} \dots p_k^{b_k}$. Resta provar que $b_i \leq a_i$. Suponha por absurdo que exista r tal que $b_r > a_r$. Como $p_r^{b_r} \mid d$, segue que

$$p_r^{b_r} \mid \prod_{i=1}^{k} p_i^{a_i}.$$

Dividindo os dois lados por $p_r^{a_r}$, temos que

$$p_r^{b_r - a_r} \mid \prod_{\substack{i=1 \\ i \neq r}}^{k} p_i^{a_i}.$$

Como $b_r > a_r$, usando mais uma vez o corolário do Lema de Euclides, teríamos que p_r divide algum p_i com $i \neq r$. O que é uma contradição. Logo, mostramos que d é da forma desejada. □

1.5.1 Infinitude dos Primos

Teorema 19 (Euclides)**.** *A sequência dos números primos é infinita.*

Demonstração. Suponha, por absurdo, que a sequência de primos seja finita: $p_1, p_2, \dots, p_k$. Considere o número:

$$N = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1.$$

Veja que $N > p_i$ para todo $i = 1, \dots, k$. Logo, N não pode ser um dos primos da lista. Porém, pelo Teorema Fundamental da Aritmética, N possui uma fatoração em números primos. Em particular, N possui pelo menos um divisor primo p_i da nossa lista.

Assim, $p_i | N$. Como também sabemos que $p_i | (p_1 \cdot p_2 \cdot \dots \cdot p_k)$, então p_i deve dividir a diferença:

$$p_i | N - p_1 \cdot p_2 \cdot \dots \cdot p_k \implies p_i | 1.$$

Isso é um absurdo, pois nenhum número primo divide 1. Portanto, a sequência de primos deve ser infinita. □

1.5.2 Teste de Primalidade

Teorema 20. *Se $n > 1$ não é primo, então n possui um divisor primo p tal que $p \leq \sqrt{n}$.*

Demonstração. Se n não é primo, existe um divisor d tal que $1 < d < n$. Podemos escrever $n = d \cdot e$. Se $d \leq \sqrt{n}$, como $d > 1$, ele possui um divisor primo p. Como $p|d$ e $d|n$, então $p|n$ e $p \leq d \leq \sqrt{n}$. Se $d > \sqrt{n}$, então $e = n/d < n/\sqrt{n} = \sqrt{n}$. Como $e > 1$, ele possui um divisor primo p. Como $p|e$ e $e|n$, então $p|n$ e $p \leq e < \sqrt{n}$. Em ambos os casos, n possui um divisor primo $\leq \sqrt{n}$. □

Exemplo. Verificar se $n = 127$ é primo. Pelo teorema, se n não for primo, ele deve ter um divisor primo $p \leq \sqrt{127} \approx 11{,}26$. Os primos a testar são: 2, 3, 5, 7 e 11.

- 127 não é divisível por 2 pois é ímpar.
- $127 = 3 \cdot 42 + 1$. Logo não é divisível por 3.
- $127 = 5 \cdot 25 + 2$. Logo não é divisível por 5.
- $127 = 7 \cdot 18 + 1$. Logo não é divisível por 7.
- $127 = 11 \cdot 11 + 6$. Logo não é divisível por 11.

Conclusão: 127 é primo.

1.5.3 Crivo de Eratóstenes

Para listar todos os primos até 100, escrevemos os números de 1 a 100 e riscamos os múltiplos próprios de 2, 3, 5 e 7, que são os primos até $\sqrt{100} = 10$ (circulados na figura). Pelo teorema acima, os números maiores que 1 que não foram riscados são primos (sublinhados na figura).

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~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

1.6 Mínimo Múltiplo Comum (mmc)

Definição. Dados inteiros positivos a e b, o **mínimo múltiplo comum** de a e b, denotado por $\text{mmc}(a, b)$ ou $[a, b]$, é o menor inteiro positivo que é múltiplo de a e b simultaneamente.

Observação. A existência do mmc segue do Princípio da Boa Ordem, dado que o conjunto de múltiplos comuns positivos é não-vazio (pois $a \cdot b$ é um múltiplo comum).

Teorema 21. *Sejam* $a = p_1^{a_1} \dots p_k^{a_k}$ *e* $b = p_1^{b_1} \dots p_k^{b_k}$, *com* p_i *primos distintos e* $a_i, b_i \geq 0$. *Então:*

a) $\text{mdc}(a, b) = p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)}$

b) $\text{mmc}(a, b) = p_1^{\max(a_1, b_1)} \dots p_k^{\max(a_k, b_k)}$

c) $a \cdot b = \text{mdc}(a, b) \cdot \text{mmc}(a, b)$

Demonstração. As partes (a) e (b) seguem da caracterização de divisores e múltiplos através da fatoração. Um número d divide a e b se, e somente se, seus expoentes e_i satisfazem $e_i \leq a_i$ e $e_i \leq b_i$, ou seja, $e_i \leq \min(a_i, b_i)$. O maior deles ocorre na igualdade. O raciocínio para o mmc é análogo com $e_i \geq \max(a_i, b_i)$. A parte (c) segue da identidade $\min(r, s) + \max(r, s) = r + s$ para quaisquer números reais r, s. □

Definição. Dados inteiros positivos $m_1, \dots, m_k$, o **mínimo múltiplo comum** de $m_1, \dots, m_k$ denotado por $\text{mmc}(m_1, \dots, m_k)$ ou $[m_1, \dots, m_k]$, é o menor inteiro positivo que é múltiplo de $m_1, \dots$ e m_k simultaneamente.

Proposição 22. *Sejam* $m_1, \dots, m_k$ *inteiros positivos. Então* m *é um múltiplo comum de* $m_1, \dots, m_k$ *se, e somente se,* m *é múltiplo de* $[m_1, \dots, m_k]$.

Demonstração. Exercício. Dica: A prova tem três ingredientes. 1. Indução para reduzir ao caso $k = 2$. 2. Lema de Euclides. 3. O item c) do teorema acima. □

1.7 Divisores de um Produto

Exemplo. $a = 8, b = 35$.

- Divisores de 8: $1, 2, 4, 8$.
- Divisores de 35: $1, 5, 7, 35$.
- Divisores de 280: $1, 2, 4, 5, 7, 8, 10, 14, 20, 28, 35, 40, 56, 70, 140, 280$.

- $1 = 1 \cdot 1$
- $2 = 2 \cdot 1$
- $4 = 4 \cdot 1$
- $5 = 1 \cdot 5$
- $7 = 1 \cdot 7$
- $8 = 8 \cdot 1$
- $10 = 2 \cdot 5$
- $14 = 2 \cdot 7$
- $20 = 4 \cdot 5$
- $28 = 4 \cdot 7$
- $35 = 1 \cdot 35$
- $40 = 8 \cdot 5$
- $56 = 8 \cdot 7$
- $70 = 2 \cdot 35$
- $140 = 4 \cdot 35$
- $280 = 8 \cdot 35$

Proposição 23. *Sejam a e b inteiros positivos primos entre si. Para todo divisor positivo d de ab, existe um único par de divisores positivos d_1 de a e d_2 de b tais que $d = d_1 \cdot d_2$. Reciprocamente, se $d_1|a$ e $d_2|b$, então $d = d_1 d_2$ é um divisor de ab.*

Demonstração. Sejam as fatorações $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ e $b = q_1^{\beta_1} \dots q_l^{\beta_l}$. Como $\text{mdc}(a, b) = 1$, os primos p_i e q_j são todos distintos. Assim, a fatoração de ab é o produto das duas fatorações. Todo divisor d de ab deve ter a forma:

$$d = p_1^{c_1} \dots p_n^{c_n} \cdot q_1^{e_1} \dots q_l^{e_l}$$

com $c_i \leq \alpha_i$ e $e_j \leq \beta_j$. Definindo $d_1 = p_1^{c_1} \dots p_n^{c_n}$ e $d_2 = q_1^{e_1} \dots q_l^{e_l}$, temos que $d_1|a$, $d_2|b$ e $d = d_1 d_2$. A unicidade segue da unicidade do Teorema Fundamental da Aritmética. □

Prova Alternativa. Seja d um divisor de ab. Tome $d_1 = \text{mdc}(d, a)$ e $d_2 = d/d_1$. Já sabemos que $d_1|a$. Pode-se mostrar que $d_2|b$. A prova é uma variação do Lema de Euclides. Como $d = d_1 \cdot d_2$, a existência está garantida.

Para provar a unicidade, sejam d_1, d_2, d_1', d_2' inteiros tais que d_1 e d_1' dividem a e d_2 e d_2' dividem b e $d = d_1 d_2 = d_1' d_2'$. Como $d_1 d_2 = d_1' d_2'$ então $d_1 \mid d_1' d_2'$. Como $d_1 \mid a$ e $d_2' \mid b$, temos que $(d_1, d_2') = 1$. A partir disto deduzimos que d_1 divide d_1'. De maneira completamente análoga mostramos que $d_1' \mid d_1$. Segue então que $d_1 = d_1'$ e, automaticamente, $d_2 = d_2'$. □

1.8 Critérios de Divisibilidade

Consideramos um número n representado em sua expansão decimal:

$$n = (a_k a_{k-1} \dots a_1 a_0)_{10} = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k,$$

onde $a_i \in \{0, 1, \dots, 9\}$ são os dígitos de n.

1.8.1 Divisibilidade por 2 e 5

Como 10 é múltiplo de 2 e de 5, qualquer potência 10^i com $i \geq 1$ também o é. Assim, todos os termos da soma, exceto possivelmente a_0, são divisíveis por 2 e 5.

- n é divisível por 2 se, e somente se, o dígito das unidades a_0 for par. Ou seja, $a_0 \in \{0, 2, 4, 6, 8\}$.
- n é divisível por 5 se, e somente se, $a_0 \in \{0, 5\}$.

1.8.2 Divisibilidade por 9 e 3

Agora os números 10, 100, 1000, ...não são múltiplos de 9, mas $9 = 10 - 1, 99 = 100 - 1, 999 = 1000 - 1, \dots$ são:

$$9 = 9 \cdot 1,\ 99 = 9 \cdot 11,\ 999 = 9 \cdot 111,\ \dots.$$

De um modo geral,

$$10^k - 1 = \underbrace{99 \dots 9}_{k \text{ dígitos}} = 9 \cdot \underbrace{11 \dots 1}_{k \text{ dígitos}}.$$

Assim, escrevendo $10^i = (10^i - 1) + 1$ e substituindo na expressão de n:

$$n = \big(a_1(10-1) + \cdots + a_k(10^k - 1)\big) + (a_0 + a_1 + \cdots + a_k)\,.$$

Como o primeiro termo é múltiplo de 9, temos que

- $9|n \iff 9|(a_0 + a_1 + \cdots + a_k)$.
- $3|n \iff 3|(a_0 + a_1 + \cdots + a_k)$ (pois todo múltiplo de 9 é múltiplo de 3).

Exemplo. $n = 7985338$.
Pelo critério, n é múltiplo de 9 se, e somente se, $7+9+8+5+3+3+8 = 43$ é múltiplo de 9. Mais uma vez pelo critério: 43 é múltiplo de 9 se, e somente se, $4+3 = 7$ é múltiplo de 9, o que não é o caso. Logo, 7985338 não é múltiplo de 9.

1.8.3 Divisibilidade por 4

$4 \nmid 10$, mas $4|10^k$ para todo $k \geq 2$. Assim, se $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$, então $4|n$ se, e somente se, $4|10a_1 + a_0$. Ou seja, se, e somente se, 4 divide o número formado pelos dois últimos dígitos $(a_1a_0)_{10}$. Com um pouco mais de trabalho, é possível mostrar que $4|(a_1a_0)_{10} \iff a_0 \in \{0,4,8\}$ e a_1 é par, ou $a_0 \in \{2,6\}$ e a_1 é ímpar.

1.8.4 Divisibilidade por 11

10 não é múltiplo de 11, mas $10 + 1 = 11$ é. 100 não é múltiplo de 11, 101 também não é mas $99 = 11 \cdot 9$ é múltiplo de 11.
De um modo geral, se k é ímpar, $10^k + 1$ é múltiplo de 11; se k é par, $10^k - 1$ é múltiplo de 11 (Exercício. Dica: use as fatorações para $x^n - 1$ (n qualquer) e $x^n + 1$ (n ímpar)).

Com isso podemos escrever:

$$\begin{aligned} n &= a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k \\ &= a_0 - a_1 + a_1(10+1) + a_2 + a_2(100-1) + \cdots + (-1)^k a_k + a_k(10^k - (-1)^k). \end{aligned}$$

Como $a_1(10+1), a_2(10^2-1), \ldots a_k(10^k - (-1)^k)$ são múltiplos de 11, segue que

$$11|n \iff 11|(a_0 - a_1 + a_2 - \cdots + (-1)^k a_k).$$

Exemplo. $n = 6392837$.
Pelo critério, devemos calcular $7 - 3 + 8 - 2 + 9 - 3 + 6 = 22$. Como $11 \mid 22$, segue que 6392837 é múltiplo de 11.

1.8.5 Divisibilidade por 7

10 não está "próximo" de um múltiplo de 7: $10 = 7 \cdot 1 + 3$ mas 20 está. A base do critério da divisibilidade por 7 é a identidade $20 = 7 \cdot 3 - 1$. Primeiramente, como $\text{mdc}(2,7) = 1$, temos $7|n \iff 7|2n$.
Escreva $n = (a_k \ldots a_0)_{10}$ e seja $m = (a_k \ldots a_1)_{10}$ Então $n = 10m + a_0$. Agora,

$$7|n \iff 7|2n \iff 7|20m + 2a_0.$$

Como $20m + 2a_0 = 21m - (m - 2a_0)$, vemos que

$$7|n \iff 7|(m - 2a_0).$$

Substituindo o valor de m, chegamos ao critério

$$7|n \iff 7|(a_k \dots a_1)_{10} - 2a_0.$$

Exemplo. $n = 2026$.
Pelo critério, n é múltiplo de 7 se, e somente se, $202 - 2 \cdot 6 = 190$ é múltiplo de 7. Mais uma vez pelo critério (ou simplesmente usando o Lema de Euclides), 190 é múltiplo de 7 se, e somente se, $19 - 2 \cdot 0 = 19$ é múltiplo de 7, o que não é o caso. Assim, 2026 não é múltiplo de 7.

1.9 Representação de um Número em Base b

Seja b um número inteiro maior que 1.

Teorema 24. *Todo inteiro positivo n pode ser representado de maneira única na forma:*

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

onde cada dígito a_i satisfaz $0 \leq a_i < b$ e $a_k \neq 0$.

Demonstração. **Existência:** Aplicamos o algoritmo da divisão com divisor igual a b:

$$\begin{aligned} n &= b \cdot q_0 + a_0, \quad 0 \leq a_0 < b \\ q_0 &= b \cdot q_1 + a_1, \quad 0 \leq a_1 < b \\ q_1 &= b \cdot q_2 + a_2, \quad 0 \leq a_2 < b \\ &\vdots \end{aligned}$$

Afirmamos que para algum inteiro k, teremos $q_k = 0$. De fato, se este não fosse o caso, como

$$q_k = bq_{k+1} + a_{k+1} \geq bq_{k+1} > q_{k+1},$$

teríamos que $q_0,\ q_1,\ \dots$ seria uma sequência estritamente decrescente de inteiros positivos. Pelo Princípio da Boa Ordem isto não é possível. Seja então k o menor índice tal que $q_k = 0$. Substituindo as equações umas nas outras obtemos

$$\begin{aligned} n &= b \cdot (bq_1 + a_1) + a_0 \\ &= b^2 \cdot (bq_2 + a_2) + a_1 b + a_0 \\ &= \dots \\ &= b^k \cdot (b \cdot 0 + a_k) + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \\ &= a_k b^k + \cdots + a_1 b + a_0, \end{aligned}$$

como queríamos.

Unicidade: Procedemos por indução forte em n. Suponha que a representação é única para todo inteiro positivo menor que n, e que

$$n = (a_k \dots a_0)_b = (a'_\ell \dots a'_0)_b,$$

com $a_k \neq 0$ e $a'_\ell \neq 0$. Sejam $m = (a_k \dots a_1)_b$ e $m' = (a'_\ell \dots a'_1)_b$, com a convenção $m = 0$ se $k = 0$ e $m' = 0$ se $\ell = 0$. Por definição,

$$n = bm + a_0 = bm' + a'_0.$$

Como $a_0, a'_0 \in \{0, \dots, b-1\}$, pela unicidade do quociente e do resto no algoritmo da divisão, segue que $m = m'$ e $a_0 = a'_0$. Se $m = 0$, então $k = \ell = 0$ e não há mais nada a provar. Se $m > 0$, então

$$n = bm + a_0 \geq bm > m;$$

pela hipótese de indução aplicada a m, temos $k = \ell$ e $a_i = a'_i$ para todo $i \geq 1$. □

Exemplo. $n = 34738$, $b = 5$.
Fazendo a divisão de 34738 por 5, vemos que

$$34738 = 5 \cdot 6947 + 3 \implies a_0 = 3.$$

Repetindo o processo, temos que

$$\begin{aligned} 6947 &= 5 \cdot 1389 + 2 \\ 1389 &= 5 \cdot 277 + 4 \\ 277 &= 5 \cdot 55 + 2 \\ 55 &= 5 \cdot 11 + 0 \\ 11 &= 5 \cdot 2 + 1 \\ 2 &= 5 \cdot 0 + 2. \end{aligned}$$

Substituindo as equações umas nas outras, obtemos que

$$\begin{aligned} 34738 &= 5^2 \cdot 1389 + 2 \cdot 5 + 3 \\ &= 5^3 \cdot 277 + 4 \cdot 5^2 + 2 \cdot 5 + 3 \\ &= 5^4 \cdot 55 + 2 \cdot 5^3 + 4 \cdot 5^2 + 2 \cdot 5 + 3 \\ &= 5^5 \cdot 11 + 2 \cdot 5^3 + 4 \cdot 5^2 + 2 \cdot 5 + 3 \\ &= 2 \cdot 5^6 + 5^5 + 2 \cdot 5^3 + 4 \cdot 5^2 + 2 \cdot 5 + 3. \end{aligned}$$

Ou seja, $n = (2102423)_5$.

1.10 Exercícios

Divisibilidade, mdc e mmc (Seção 1.2 de [NZM91])

3. (NZM, 1.2.18) Encontre os valores de (a, b) e $[a, b]$ se a e b são inteiros positivos tais que $a \mid b$.

4. (NZM, 1.2.21) Prove que se um inteiro é da forma $6k + 5$, então é necessariamente da forma $3k - 1$, mas não reciprocamente.

5. (NZM, 1.2.22) Prove que o quadrado de qualquer inteiro da forma $5k + 1$ é da mesma forma.

6. (NZM, 1.2.23) Prove que o quadrado de qualquer inteiro é da forma $3k$ ou $3k+1$, mas não da forma $3k+2$.

7. (NZM, 1.2.24) Prove que não existem inteiros x, y satisfazendo $x + y = 100$ e $(x, y) = 3$.

8. (NZM, 1.2.25) Prove que existem infinitos pares de inteiros x, y satisfazendo $x+y = 100$ e $(x, y) = 5$.

9. (NZM, 1.2.27) Encontre inteiros positivos a e b que satisfaçam simultaneamente as equações $(a, b) = 10$ e $[a, b] = 100$. Encontre todas as soluções.

10. (NZM, 1.2.28) Encontre todas as ternas de inteiros positivos a, b, c que satisfaçam simultaneamente $(a, b, c) = 10$ e $[a, b, c] = 100$.

11. (NZM, 1.2.33) Prove que $(a, b) = (a, b, a + b)$ e, mais geralmente, que $(a, b) = (a, b, ax + by)$ para todos os inteiros x, y.

12. (NZM, 1.2.34) Prove que $(a, a + k) \mid k$ para todos os inteiros a, k não ambos nulos.

13. (NZM, 1.2.35) Prove que $(a, a + 2) = 1$ ou 2 para todo inteiro a.

14. (NZM, 1.2.36) Prove que $(a, b, c) = ((a, b), c)$.

15. (NZM, 1.2.43) Prove que $a \mid bc$ se, e somente se, $\frac{a}{(a,b)} \Big| c$. (Versão do Lema de Euclides)

16. (NZM, 1.2.45) Prove que qualquer inteiro positivo a pode ser expresso de modo único na forma

$$a = 3^m + b_{m-1}3^{m-1} + b_{m-2}3^{m-2} + \cdots + b_0$$

onde cada $b_j = 0, 1$ ou -1.

17. (NZM, 1.2.49) Prove que se $m > n$, então $a^{2^n} + 1$ é um divisor de $a^{2^m} - 1$. Mostre que se a, m, n são positivos com $m \neq n$, então

$$\left(a^{2^m} + 1, a^{2^n} + 1\right) = \begin{cases} 1 \text{ se } a \text{ é par} \\ 2 \text{ se } a \text{ é ímpar} . \end{cases}$$

18. (NZM, 1.2.53) Mostre que $(n! + 1, (n + 1)! + 1) = 1$.

Números primos (Seção 1.3 de [NZM91])

19. (NZM, 1.3.6) Mostre que todo inteiro positivo n tem uma única expressão da forma $n = 2^r m, r \geq 0$, com m um inteiro positivo ímpar.

20. (NZM, 1.3.7) Mostre que todo inteiro positivo n pode ser escrito de modo único na forma $n = ab$, onde a é livre de quadrados e b é um quadrado. Mostre que b é, então, o maior quadrado que divide n.

21. (NZM, 1.3.9) Prove que qualquer primo da forma $3k + 1$ é da forma $6k + 1$.

22. (NZM, 1.3.10) Prove que qualquer inteiro positivo da forma $3k + 2$ tem um fator primo da mesma forma; analogamente para cada uma das formas $4k + 3$ e $6k + 5$.

23. (NZM, 1.3.11) Se x e y são ímpares, prove que $x^2 + y^2$ não pode ser um quadrado perfeito.

24. (NZM, 1.3.13) Se $(a, b) = p$, um primo, quais são os valores possíveis de (a^2, b)? De (a^3, b)? De (a^2, b^3)?

25. (NZM, 1.3.14) Calcule (ab, p^4) e $(a + b, p^4)$, sabendo que $(a, p^2) = p$ e $(b, p^3) = p^2$, onde p é primo.

26. (NZM, 1.3.16) Encontre um inteiro n tal que $n/2$ seja um quadrado, $n/3$ seja um cubo e $n/5$ seja uma quinta potência.

27. (NZM, 1.3.19) Sejam a e b inteiros positivos tais que $(a, b) = 1$ e ab é um quadrado perfeito. Prove que a e b são quadrados perfeitos.

28. (NZM, 1.3.20) Dado que $(a, b, c)[a, b, c] = abc$, prove que $(a, b) = (b, c) = (a, c) = 1$.

29. (NZM, 1.3.21) Prove que $[a, b, c](ab, bc, ca) = |abc|$.

30. (NZM, 1.3.23) Dados inteiros a, b, c, d, m, n, u, v satisfazendo $ad - bc = \pm 1, u = am + bn, v = cm + dn$, prove que $(m, n) = (u, v)$.

31. (NZM, 1.3.27) Mostre que $n \mid (n - 1)!$ para todo $n > 4$ composto.

32. (NZM, 1.3.32) Mostre que $n^4 + 4$ é composto para todo $n > 1$.

33. (NZM, 1.3.33) Mostre que $n^4 + n^2 + 1$ é composto se $n > 1$.

34. (NZM, 1.3.35) Mostre que existem inteiros não negativos x e y tais que $x^2 - y^2 = n$ se, e somente se, n é ímpar ou múltiplo de 4. Mostre que existe exatamente uma tal representação de n se, e somente se, $n = 1$, 4, um primo ímpar ou quatro vezes um primo.

35. (NZM, 1.3.36) Considere o conjunto $\mathscr{S}$ dos inteiros $1, 2, \ldots, n$. Seja 2^k o inteiro de $\mathscr{S}$ que é a maior potência de 2. Prove que 2^k não é divisor de nenhum outro inteiro de $\mathscr{S}$. Consequentemente, prove que $\sum_{j=1}^{n} 1/j$ não é inteiro se $n > 1$.

36. (NZM, 1.3.37) Prove que, em qualquer bloco de inteiros positivos consecutivos, existe um único inteiro divisível por uma potência de 2 maior do que a de qualquer um dos outros. Em seguida, use isso, ou qualquer outro método, para provar que não há nenhum inteiro entre os 2^{n+1} números

$$\pm\frac{1}{k} \pm \frac{1}{k+1} \pm \frac{1}{k+2} \pm \cdots \pm \frac{1}{k+n}$$

onde todas as combinações possíveis de sinais de mais e de menos são permitidas, e onde n e k são inteiros positivos quaisquer. (Observe que este resultado é uma ampla generalização do problema anterior.)

37. (NZM, 1.3.42) Se $2^n + 1$ é um primo ímpar para algum inteiro n, prove que n é uma potência de 2.

38. (NZM, 1.3.44) Se $2^n - 1$ é primo para algum inteiro n, prove que n é ele próprio primo. (Os números da forma $2^p - 1$, onde p é primo, são chamados números de Mersenne M_p, porque o francês Padre Marin Mersenne (1588-1648) afirmou que M_p é primo para $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, mas composto para todos os outros primos $p < 257$. Foram necessários cerca de 300 anos até que os detalhes dessa afirmação pudessem ser completamente verificados, com o seguinte resultado: M_p não é primo para $p = 67$ e $p = 257$, e M_p é primo para $p = 61$, $p = 89$ e $p = 107$. Assim, existem 12 primos $p < 257$ tais que M_p é primo. Até novembro de 2026, são conhecidos 52 primos de Mersenne. O maior deles, $M_{136279841}$, com 41 024 320 algarismos, foi encontrado em outubro de 2024 pelo projeto GIMPS (*Great Internet Mersenne Prime Search*) e é o maior número primo conhecido [Gre24]. Conjectura-se que infinitos números de Mersenne sejam primos.)

39. (NZM, 1.3.45) Sejam dados inteiros positivos g e l com $g \mid l$. Prove que o número de pares de inteiros positivos x, y satisfazendo $(x, y) = g$ e $[x, y] = l$ é 2^k, onde k é o número de fatores primos distintos de l/g. (Conte x_1, y_1 e x_2, y_2 como pares diferentes se $x_1 \neq x_2$ ou $y_1 \neq y_2$.)

40. (NZM, 1.3.46) Seja $k \geq 3$ um inteiro fixo. Encontre todos os conjuntos $a_1, a_2, \ldots, a_k$ de inteiros positivos tais que a soma de qualquer terna seja divisível por cada membro da terna.

41. (NZM, 1.3.48) Prove que existem infinitos primos considerando a sequência $2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1, 2^{2^4} + 1, \ldots$.

42. (NZM, 1.3.49) Se g é divisor de cada um dos números ab, cd e $ac + bd$, prove que também é divisor de ac e bd, onde a, b, c, d são inteiros.

43. (NZM, 1.3.50) Mostre que

$$(ab, cd) = (a, c)(b, d) \left(\frac{a}{(a, c)}, \frac{d}{(b, d)} \right) \left(\frac{c}{(a, c)}, \frac{b}{(b, d)} \right).$$

44. (NZM, 1.3.51) Mostre que 24 é o maior inteiro divisível por todos os inteiros menores que sua raiz quadrada.

Capítulo 2

Congruências

2.1 Definição e Propriedades Básicas

Definição. Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$. Dizemos que a é **congruente** a b módulo m se $m|(a-b)$. Notação: $a \equiv b \pmod{m}$.
Notações alternativas: $a \equiv b\ (m)$ **ou** $a \overset{m}{\equiv} b$.

Exemplo. Alguns exemplos de congruência:

- $11 \equiv 1 \pmod{2}$
- $7 \not\equiv 5 \pmod{3}$
- $12 \equiv 4 \pmod{8}$
- $105 \not\equiv 6 \pmod{7}$

Proposição 25 (Propriedades básicas da congruência)**.** *Sejam $a, b, c, m \in \mathbb{Z}, m > 0$. Então:*

1. $a \equiv a \pmod{m}$ *(Reflexiva)*
2. $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$ *(Simétrica)*
3. *Se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$*, então* $a \equiv c \pmod{m}$ *(Transitiva)*

Em outras palavras, dado $m > 0$, a relação de congruência módulo m é uma *relação de equivalência*.

Demonstração. 1. Segue pois $a - a = 0$ e $m \mid 0$.

2. Segue pois $m \mid a - b \iff m \mid b - a$.

3. Se $m \mid a - b$ e $m \mid b - c$, então $m \mid (a-b) + (b-c) \iff m \mid a - c$.

□

Teorema 26 (Congruência e Operações)**.** *Sejam $a, b, c, d, m \in \mathbb{Z}$ tais que $m > 0$, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Então:*

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$

Demonstração. 1. Como $m \mid a-b$ e $m \mid c-d$, segue que $m \mid (a-b)+(c-d) \iff m \mid (a+c)-(b+d)$. Ou seja, $a+c \equiv b+d \pmod{m}$.

2. É análogo.

3. Note que

$$\begin{aligned} ac-bd &= ac-bc+bc-bd \\ &= c(a-b)+b(c-d). \end{aligned}$$

Como $m \mid a-b$ e $m \mid c-d$, segue que $m \mid ac-bd$.

□

Exemplo. Note que se $a \equiv b \pmod{m}$, então para qualquer inteiro k:

- $a+k \equiv b+k \pmod{m}$
- $ak \equiv bk \pmod{m}$

Porém observe que a divisão não funciona da mesma forma: $12 \equiv 4 \pmod{8}$, mas $6 \not\equiv 2 \pmod{8}$. Vale apenas que $6 \equiv 2 \pmod{4}$.

Por outro lado, veja que se $2a \equiv 2b \pmod{7}$, isso significa que $7 \mid 2(a-b)$. Como $\text{mdc}(7,2)=1$, segue que $7 \mid a-b \iff a \equiv b \pmod{7}$.

Proposição 27. *Sejam a, b, c, m inteiros tais que $m > 0$ e $ac \equiv bc \pmod{m}$. Seja $d = \text{mdc}(c,m)$. Então $a \equiv b \pmod{m/d}$. Em particular, se $\text{mdc}(c,m)=1$, então $a \equiv b \pmod{m}$.*

Demonstração. Se $ac \equiv bc \pmod{m}$, então $m \mid ac-bc = c(a-b)$. Dividindo por d, obtemos

$$\frac{m}{d} \,\Big|\, \frac{c}{d}(a-b).$$

Pelo Corolário 8, $\text{mdc}\left(\frac{m}{d}, \frac{c}{d}\right) = 1$. Logo, pela versão geral do Lema de Euclides (Proposição 15), $\frac{m}{d} \mid a-b$, isto é, $a \equiv b \pmod{m/d}$. □

2.2 Sistema Completo de Restos (SCR)

Definição. Um conjunto $\mathcal{R}$ é um **Sistema Completo de Restos (SCR)** módulo m se:

1. Dados $r, s \in \mathcal{R}$ distintos, temos que $r \not\equiv s \pmod{m}$.
2. Para todo inteiro n, existe um $r \in \mathcal{R}$ tal que $n \equiv r \pmod{m}$.

Exemplo. O conjunto $\{0,1\}$ é um SCR módulo 2. Qualquer inteiro n é congruente a 0 (se for par) ou a 1 (se for ímpar) módulo 2.

Exemplo. Alguns SCRs notáveis:

- $\{0, 1, \ldots, m-1\}$ é um SCR módulo m.

1. Dados $r, s \in \{0, 1, \ldots, m-1\}$, a diferença entre eles satisfaz:

$$-(m-1) \leq r - s \leq m - 1.$$

O único múltiplo de m contido neste intervalo é 0. Portanto, se $r \neq s$, então $m \nmid (r-s)$, o que implica que $r \not\equiv s \pmod{m}$.

2. Pelo algoritmo da divisão, para qualquer inteiro n, existem q e r tais que:

$$n = mq + r, \quad \text{com } r \in \{0, 1, \ldots, m-1\}.$$

Esta igualdade implica que $m|(n-r)$, ou seja, $n \equiv r \pmod{m}$.

- Se m é ímpar, $\{-\frac{m-1}{2}, \ldots, 0, \ldots, \frac{m-1}{2}\}$ é um SCR.
- Se m é par, $\{-\frac{m}{2}+1, \ldots, 0, \ldots, \frac{m}{2}\}$ e $\{-\frac{m}{2}, \ldots, 0, \ldots, \frac{m}{2}-1\}$ são SCRs.

Estes dois últimos fatos podem ser provados de maneira análoga ao primeiro, mediante uma modificação do algoritmo da divisão mas também seguem de um resultado geral que veremos mais à frente.

Exemplo. $\{9, 12, 15, 18, 21\}$ é um SCR módulo 5. Verifique!

Teorema 28. *Se $\mathcal{R}$ e $\mathcal{R}'$ são SCRs módulo m, então $\#\mathcal{R} = \#\mathcal{R}'$.*

Demonstração. A estratégia é construir uma função bijetiva $f : \mathcal{R} \to \mathcal{R}'$. Dados $r \in \mathcal{R}$ e $r' \in \mathcal{R}'$, dizemos que r e r' estão associados se $r \equiv r' \pmod{m}$.

Como $\mathcal{R}'$ satisfaz a propriedade 2. de um SCR, segue que para todo $r \in \mathcal{R}$, existe $r' \in \mathcal{R}'$ tal que r e r' estão relacionados. Além disso se s' é um outro elemento de $\mathcal{R}'$ associado a r, teríamos que $r \equiv r' \pmod{m}$ e $r \equiv s' \pmod{m}$. Consequentemente, $r' \equiv s' \pmod{m}$. Como $\mathcal{R}'$ satisfaz a propriedade 1. de um SCR, segue que $r' = s'$. Ou seja, mostramos que todo $r \in \mathcal{R}$ está associado a *exatamente* um elemento de $\mathcal{R}'$. Isto é, construímos uma função $f : \mathcal{R} \to \mathcal{R}'$. Em seguida, provamos que f é bijetiva.

Injetividade: Suponha $f(r) = r' = f(s)$. Por construção, $r \equiv r' \pmod{m}$ e $s \equiv r' \pmod{m}$. Pela transitividade, $r \equiv s \pmod{m}$. Como $\mathcal{R}$ satisfaz a propriedade 1. de um SCR, segue que $r = s$.

Sobrejetividade: Seja $r' \in \mathcal{R}'$. Como $\mathcal{R}$ satisfaz a propriedade 2. de um SCR, existe $r \in \mathcal{R}$ tal que $r' \equiv r \pmod{m}$. Pela construção de f, isso significa que $f(r) = r'$. Portanto, como f é bijetiva, $\#\mathcal{R} = \#\mathcal{R}'$. □

Observação. A prova do teorema acima é bastante satisfatória do ponto de vista que dentre as hipóteses temos dois SCRs e, como a definição de um SCR envolve 2 propriedades, temos 4 propriedades no total e cada uma dessas propriedades é utilizada exatamente uma vez para construir uma associação entre os dois conjuntos, mostrar que essa associação é uma função, mostrar que essa função é injetiva e mostrar que ela é sobrejetiva.

Corolário 29. *Se $\mathcal{R}$ é um SCR módulo m, então $\#\mathcal{R} = m$.*

Demonstração. Segue do teorema acima e do fato que o conjunto $\{0, \ldots, m-1\}$ sempre é um SCR. □

Proposição 30. *Seja $m > 0$ e $\mathcal{R}$ um conjunto de inteiros. Então:*

a) Se $\mathcal{R}$ satisfaz a propriedade (1) da definição de SCR, então existe $\mathcal{R}'$ tal que $\mathcal{R} \subset \mathcal{R}'$ e $\mathcal{R}'$ é um SCR módulo m.

b) Se $\mathcal{R}$ satisfaz a propriedade (2) da definição de SCR, então existe $\mathcal{R}'$ tal que $\mathcal{R}' \subset \mathcal{R}$ e $\mathcal{R}'$ é um SCR módulo m.

Observação. Observe que esta proposição possui um paralelo claro com o resultado de álgebra linear que diz que um conjunto de vetores linearmente independentes pode ser estendido a uma base e um conjunto de vetores que geram um espaço vetorial pode ser reduzido a uma base.

Demonstração. a) Seja $\mathcal{R}'$ a união de $\mathcal{R}$ com o conjunto dos $i \in \{0, 1, \ldots, m-1\}$ que não são congruentes módulo m a nenhum elemento de $\mathcal{R}$. Vejamos que $\mathcal{R}'$ satisfaz a propriedade (1). Sejam $r, s \in \mathcal{R}'$ distintos. Se ambos estão em $\mathcal{R}$, então $r \not\equiv s \pmod{m}$ por hipótese. Se exatamente um deles foi acrescentado, então $r \not\equiv s \pmod{m}$ por construção. Se ambos foram acrescentados, então são elementos distintos de $\{0, 1, \ldots, m-1\}$ e, portanto, $r \not\equiv s \pmod{m}$. Quanto à propriedade (2), todo inteiro n é congruente módulo m a algum $i \in \{0, 1, \ldots, m-1\}$, e este i ou pertence a $\mathcal{R}'$ ou é congruente a um elemento de $\mathcal{R} \subset \mathcal{R}'$.

b) Para cada $i \in \{0, 1, \ldots, m-1\}$, a propriedade (2) fornece um $r_i \in \mathcal{R}$ tal que $r_i \equiv i \pmod{m}$. Seja $\mathcal{R}' = \{r_0, r_1, \ldots, r_{m-1}\}$. Se $r_i \equiv r_j \pmod{m}$, então $i \equiv j \pmod{m}$ e, portanto, $i = j$; logo $\mathcal{R}'$ satisfaz a propriedade (1). Além disso, todo inteiro n é congruente módulo m a algum $i \in \{0, 1, \ldots, m-1\}$ e, portanto, a r_i; logo $\mathcal{R}'$ satisfaz a propriedade (2). □

Corolário 31. *Se um conjunto $\mathcal{R}$ com m elementos satisfaz ou a propriedade (1) ou a propriedade (2) da definição de SCR módulo m, então ele é um SCR módulo m.*

Proposição 32. *Seja R um SCR módulo m e a, b inteiros tais que $(a, m) = 1$. Então o conjunto $\{ar + b : r \in R\}$ é um SCR.*

Demonstração. Seja $R' = \{ar + b : r \in R\}$. Claramente $\#R' = m$. Portanto, basta mostrar que satisfaz a propriedade (1) ou (2) de um SCR. Vamos mostrar que satisfaz (1). Sejam $r', s' \in R'$. Por definição, existem $r, s \in R$ tais que $r' = ar + b$ e $s' = as + b$. Suponha que $r' \equiv s' \pmod{m}$. Isso nos diz que:

$$ar + b \equiv as + b \pmod{m} \implies ar \equiv as \pmod{m} \implies r \equiv s \pmod{m},$$

onde na última implicação, utilizamos a Proposição 27. Como R é SCR e $r, s \in R$ e $r \equiv s \pmod{m}$, segue que $r = s$. Consequentemente, $r' = s'$. □

Exemplo. $m = 5$, $a = 2$, $b = 10$, $R = \{0, 1, 2, 3, 4\} \rightsquigarrow \{10, 12, 14, 16, 18\}$ é um SCR.

2.3 Congruências Lineares

Uma congruência linear é uma congruência da forma $ax \equiv b \pmod{m}$, onde a, b, m são inteiros e $m > 0$.

Exemplos.

- $2x \equiv 0 \pmod{4}$. Pela Proposição 27, isso é equivalente a

$$x \equiv 0 \pmod{2}.$$

- $3x \equiv 15 \pmod 8$. Aqui, como $(3, 8) = 1$, isso é equivalente a:

$$x \equiv 5 \pmod 8.$$

- $5x \equiv 2 \pmod 7$. Como $5 \nmid 2$, aqui não dá pra fazer a mesma coisa. A ideia para resolver essa congruência é substituir 2 por outro número b tal que $b \equiv 2 \pmod 7$ e $5|b$. Nesse caso, teríamos

$$5x \equiv 2 \pmod 7 \iff 5x \equiv b \pmod 7 \iff x \equiv \frac{b}{5} \pmod 7.$$

  Pergunta: Como fazemos para encontrar b? **Possível resposta:** Na marra.

  Veja que $b \equiv 2 \pmod 7$ significa $b = 2 + 7k$. Tentando $k = 0, 1, 2, 3, 4, \ldots$, temos $b = 2, 9, 16, 23, 30, \ldots$. Observe que 30 é um número com as propriedades desejadas. Assim, temos

$$5x \equiv 2 \pmod 7 \iff 5x \equiv 30 \pmod 7 \iff x \equiv 6 \pmod 7.$$

Observação. Note que no último exemplo, as escolhas $b = -5$ e $b = 65$ também satisfazem as propriedades desejadas. Com essas escolhas teríamos encontrado que

$$\begin{aligned} 5x \equiv 2 \pmod 7 &\iff x \equiv -1 \pmod 7 \\ 5x \equiv 2 \pmod 7 &\iff x \equiv 13 \pmod 7. \end{aligned}$$

O que não configura uma solução diferente. Visto que

$$6 \equiv -1 \equiv 13 \pmod 7.$$

Teorema 33. *Sejam a, b, m inteiros tais que $m > 0$ e $(a, m) = 1$. Então existe um inteiro c tal que:*

$$ax \equiv b \pmod m \iff x \equiv c \pmod m.$$

Demonstração. Inspirados pelo exemplo acima, vamos mostrar que existe um número inteiro b' tal que $b' \equiv b \pmod m$ e $a|b'$. Em outras palavras, queremos encontrar k tal que:

$$b + mk = ax \iff ax + m(-k) = b.$$

Ou seja, queremos mostrar que b é uma combinação linear de a e m.

Pelo teorema de Bézout, existem r, s tais que $ar + ms = 1$. Multiplicando por b, temos que:

$$abr + mbs = b.$$

Em particular, $abr \equiv b \pmod m$. De modo que

$$ax \equiv b \pmod m \iff ax \equiv abr \pmod m \iff x \equiv br \pmod m.$$

No último passo utilizamos mais uma vez a Proposição 27. Tomando $c = br$, concluímos. □

Observação. Quando $b = 1$, o teorema acima diz que dados a, m inteiros com $\text{mdc}(a, m) = 1$, existe $c \in \mathbb{Z}$ tal que:

$$ax \equiv 1 \pmod{m} \iff x \equiv c \pmod{m}.$$

Se c satisfaz a equivalência, dizemos que c é um **inverso multiplicativo** de a módulo m. Veja que se c é um inverso multiplicativo de a módulo m e $c' \equiv c \pmod{m}$, c' também é um inverso multiplicativo de a módulo m.

Exemplo. $5x \equiv 1 \pmod{7} \iff 5x \equiv 15 \pmod{7} \iff x \equiv 3 \pmod{7}$. Logo 3 é um inverso multiplicativo de 5 módulo 7. É fácil ver que -4 e 10 também são inversos multiplicativos módulo 7.

Corolário 34. *Sejam a, b, m inteiros, $m > 0$. Seja $d = \text{mdc}(a, m)$.*

- *Se $d \mid b$, então existe c tal que $ax \equiv b \pmod{m} \iff x \equiv c \pmod{m/d}$.*
- *Se $d \nmid b$, a congruência $ax \equiv b \pmod{m}$ não possui solução.*

Demonstração. Suponha primeiramente que $d|b$. Escreva $b = db_0$ e $a = da_0$.

$$ax \equiv b \pmod{m} \iff da_0x \equiv db_0 \pmod{m} \iff a_0x \equiv b_0 \pmod{m/d}.$$

Agora, temos $(a_0, m/d) = (a/d, m/d) = 1$. Então pelo teorema acima, existe c tal que:

$$a_0x \equiv b_0 \pmod{m/d} \iff x \equiv c \pmod{m/d}$$

(Para a segunda parte): Veja que $ax \equiv b \pmod{m}$ significa que existe $k \in \mathbb{Z}$ tal que:

$$ax - b = mk \iff b = ax - mk.$$

Como $d|a$ e $d|m$, devemos ter $d|b$. Isto é a contrapositiva da segunda parte do corolário. □

2.4 Outras Propriedades das Congruências

Proposição 35. *Sejam $a, b, m_1, \ldots, m_k$ tais que $m_1, \ldots, m_k > 0$. Então o sistema de congruências:*

$$\begin{cases} a \equiv b \pmod{m_1} \\ \quad \vdots \\ a \equiv b \pmod{m_k} \end{cases}$$

é equivalente à congruência $a \equiv b \pmod{[m_1, \ldots, m_k]}$.

Demonstração. Segue direto das definições de congruência e das propriedades do mmc. □

Proposição 36. *Sejam a, b, m inteiros, $m > 0$ tais que $a \equiv b \pmod{m}$. Então*

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

Demonstração. Pela definição de congruência, existe k inteiro tal que $b = a + mk$. Assim,

$$(b, m) = (a + mk, m) = (a, m)$$

onde na última igualdade utilizamos a Proposição 10 (ver também [San98, Teorema 1.5]). □

2.5 Teoremas de Fermat e Euler

Ideia: Sejam $a, m \in \mathbb{Z}$, com $m > 0$ e $(a, m) = 1$. Considere os números:

$$1, a, a^2, a^3, \ldots.$$

Como temos infinitos números, podemos encontrar i, j distintos tais que:

$$a^i \equiv a^j \pmod{m}.$$

De fato, se R é um SCR, para todo i, existe $r \in R$ tal que $a^i \equiv r \pmod{m}$. Pelo Princípio da Casa dos Pombos, existem $i > j$ e $r \in R$ tais que:

$$a^i \equiv r \equiv a^j \pmod{m}.$$

Suponha, sem perda de generalidade, que $i > j$. Temos:

$$a^j \cdot a^{i-j} \equiv a^j \pmod{m}.$$

Como $(a, m) = 1$, temos:

$$a^{i-j} \equiv 1 \pmod{m}.$$

Exemplo. $a = 2, m = 11$. $R = \{0, 1, \ldots, 10\}$.

$$2^0 \equiv 1 \pmod{11},\ 2^1 \equiv 2 \pmod{11},\ 2^2 \equiv 4 \pmod{11},\ 2^3 \equiv 8 \pmod{11},$$
$$2^4 \equiv 5 \pmod{11},\ 2^5 \equiv 10 \pmod{11},\ 2^6 \equiv 9 \pmod{11},\ 2^7 \equiv 7 \pmod{11},$$
$$2^8 \equiv 3 \pmod{11},\ 2^9 \equiv 6 \pmod{11},\ 2^{10} \equiv 1 \pmod{11}.$$

Para $a = 5, m = 11$:

$$5^0 \equiv 1 \pmod{11},\ 5^1 \equiv 5 \pmod{11},\ 5^2 \equiv 3 \pmod{11},$$
$$5^3 \equiv 4 \pmod{11},\ 5^4 \equiv 9 \pmod{11},\ 5^5 \equiv 1 \pmod{11}.$$

Teorema 37 (Fermat)**.** *Seja p um número primo e a um número inteiro tal que $p \nmid a$ (ou seja, $(a, p) = 1$). Então:*

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

Demonstração. Seja R um SCR módulo p (por exemplo, $R = \{0, 1, 2, \ldots, p-1\}$). Pelo que vimos, $R' = \{a \cdot r : r \in R\}$ também é um SCR. Considere os produtos:

$$X_R = \prod_{\substack{r \in R \\ r \not\equiv 0 \pmod{p}}} r, \qquad X_{R'} = \prod_{\substack{r' \in R' \\ r' \not\equiv 0 \pmod{p}}} r'.$$

Note que se $r' \in R'$, então existe $r \in R$ tal que $r' = ar$. Veja que:

$$r' \equiv 0 \pmod{p} \iff ar \equiv 0 \pmod{p} \iff r \equiv 0 \pmod{p}.$$

Em particular,

$$\begin{aligned} X_{R'} &= \prod_{\substack{r \in R \\ r \not\equiv 0 \pmod{p}}} ar \\ &= a^{\#R-1} \prod_{\substack{r \in R \\ r \not\equiv 0 \pmod{p}}} r \\ &= a^{p-1} X_R. \end{aligned}$$

Por outro lado, como R é um SCR, existem $r_0, \ldots, r_{p-1}$ distintos tais que $r_i \equiv i \pmod{p}$ e $R = \{r_0, \ldots, r_{p-1}\}$. Assim,

$$\begin{aligned} X_R &= \prod_{i=1}^{p-1} r_i \\ &\equiv \prod_{i=1}^{p-1} i = (p-1)! \pmod{p}. \end{aligned}$$

Como R' também é um SCR, o mesmo vale para $X_{R'}$. Juntando as duas igualdades acima, encontramos que

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

Já que p é um número primo, $(p, (p-1)!) = 1$ (contrariamente ao caso composto, ver o Exercício 31). Logo, cancelando o termo $(p-1)!$ de ambos os lados, encontramos que

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

□

Exemplo. $m = 12, a = 5$. $R = \{0, 1, \ldots, 11\}$. $R' = \{0, 5, 10, 15, \ldots, 55\}$. Módulo 12, analisamos os congruentes aos valores relativamente primos a 12 (que são 1, 5, 7, 11):

$$\begin{array}{lll} 5 \cdot 0 \equiv 0 \pmod{12}\text{✗}, & 5 \cdot 1 \equiv 5 \pmod{12}\text{✓}, & 5 \cdot 2 \equiv 10 \pmod{12}\text{✗}, \\ 5 \cdot 3 \equiv 3 \pmod{12}\text{✗}, & 5 \cdot 4 \equiv 8 \pmod{12}\text{✗}, & 5 \cdot 5 \equiv 1 \pmod{12}\text{✓}, \\ 5 \cdot 6 \equiv 6 \pmod{12}\text{✗}, & 5 \cdot 7 \equiv 11 \pmod{12}\text{✓}, & 5 \cdot 8 \equiv 4 \pmod{12}\text{✗}, \\ 5 \cdot 9 \equiv 9 \pmod{12}\text{✗}, & 5 \cdot 10 \equiv 2 \pmod{12}\text{✗}, & 5 \cdot 11 \equiv 7 \pmod{12}\text{✓}. \end{array}$$

Multiplicando as congruências com "✓":

$$\begin{aligned} & 5 \cdot 25 \cdot 35 \cdot 55 \equiv 5 \cdot 1 \cdot 11 \cdot 7 \pmod{12} \\ \iff & 5^4(1 \cdot 5 \cdot 7 \cdot 11) \equiv 1 \cdot 5 \cdot 7 \cdot 11 \pmod{12}. \end{aligned}$$

Como $(1 \cdot 5 \cdot 7 \cdot 11, 12) = 1$, cancelamos e obtemos:

$$5^4 \equiv 1 \pmod{12}.$$

Definição. A função ϕ de Euler associa a cada inteiro positivo m o número de inteiros $k \in \{1, 2, \ldots, m\}$ tais que $(k, m) = 1$.

Observação. Como $(0, m) = (m, m) = m$, é fácil ver que $\phi(m)$ também é o número de inteiros $k \in \{0, \ldots, m-1\}$ tais que $(k, m) = 1$.

Proposição 38. *Seja $m > 0$ e R um SCR módulo m. Então*

$$\#\{r \in R : (r, m) = 1\} = \phi(m).$$

Demonstração. Como vimos na demonstração do Teorema de Fermat, podemos escrever $R = \{r_1, \ldots, r_m\}$ de modo que $r_i \equiv i \pmod{m}$ para $i \in \{1, \ldots, m\}$. Por outro lado, segue da Proposição 10 que se $a \equiv b \pmod{m}$, então $(a, m) = (b, m)$. De fato, se $a = b + mk$ então $(a, m) = (b + mk, m) = (b, m)$. Portanto, $(r_i, m) = (i, m)$ para todo i, e

$$\#\{r \in R : (r, m) = 1\} = \#\{1 \leq i \leq m : (i, m) = 1\} = \phi(m).$$

□

Teorema 39 (Euler)**.** *Sejam $a, m \in \mathbb{Z}$ com $m > 0$ e $(a, m) = 1$. Então*

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

Demonstração. A ideia é copiar os passos da demonstração do Teorema de Fermat com as devidas adaptações. Seja R um SCR módulo m. Como já sabemos, $R' = \{ar : r \in R\}$ também é um SCR. Considere os produtos

$$Y_R = \prod_{\substack{r \in R \\ (r,m)=1}} r, \qquad Y_{R'} = \prod_{\substack{r' \in R' \\ (r',m)=1}} r'.$$

Seja $r' \in R'$, então existe $r \in R$ tal que $r' = ar$. Note que $(r', m) = (ar, m) = (r, m)$, pois $(a, m) = 1$. Portanto,

$$\begin{aligned} Y_{R'} &= \prod_{\substack{r \in R \\ (r,m)=1}} (ar) \\ &= a^{\phi(m)} Y_R. \end{aligned}$$

Escrevendo mais uma vez $R = \{r_1, \ldots, r_m\}$ com $r_i \equiv i \pmod{m}$. Como $(r_i, m) = (i, m)$, temos que

$$Y_R = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} r_i \equiv \prod_{\substack{i=1 \\ (i,m)=1}}^{m} i \pmod{m},$$

e, analogamente, para $Y_{R'}$. Ponha $Y = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} i$. Segue das identidades e congruências acima que

$$a^{\phi(m)} Y \equiv Y \pmod{m}.$$

O resultado segue, utilizando que $(Y, m) = 1$. □

2.6 Sistema Reduzido de Restos (SRR)

Subjacente à prova acima, está o conceito de Sistema Reduzido de Restos.

Definição. Seja $m > 0$. Um conjunto R de inteiros relativamente primos com m é um **Sistema Reduzido de Restos (SRR)** módulo m se satisfaz as seguintes propriedades:

1. Dados $r, s \in R$ distintos, $r \not\equiv s \pmod{m}$.
2. Para todo inteiro n tal que $(n, m) = 1$, existe $r \in R$ tal que $n \equiv r \pmod{m}$.

Proposição 40 (Propriedades básicas de SRRs)**.** *As seguintes afirmações sobre SRRs são válidas.*

1. *Seja R um SRR. Então existe um SCR $\widetilde{R}$ tal que $R = \{r \in \widetilde{R} : (r, m) = 1\}$.*
2. *Seja R um SRR. Então $\#R = \phi(m)$.*
3. *Seja R um conjunto de inteiros, todos eles primos com m, satisfazendo a propriedade 1 da definição de SRR. Então existe um SRR R' tal que $R \subset R'$.*

4. *Seja R um conjunto satisfazendo a propriedade 2 da definição de um SRR. Então existe um SRR R' tal que $R' \subset R$.*

5. *Seja R um conjunto com $\phi(m)$ elementos, todos relativamente primos com m, satisfazendo a propriedade (1) ou a (2) da definição de um SRR. Então R é um SRR.*

Demonstração. Exercício. Sugestões:

1. Segue da Proposição 30.

2. Segue do item 1.

5. Segue dos itens 3 e 4.

□

2.7 Teorema de Wilson

Completando a tríade de resultados clássicos sobre congruências, temos o Teorema de Wilson.

Teorema 41 (Wilson)**.** *Seja p um primo. Então:*

$$(p-1)! \equiv -1 \pmod{p}.$$

Exemplo. $p = 11$.

$$\begin{aligned} 2 \cdot 6 \equiv 6 \cdot 2 \equiv 1 \pmod{11} \\ 3 \cdot 4 \equiv 4 \cdot 3 \equiv 1 \pmod{11} \\ 5 \cdot 9 \equiv 9 \cdot 5 \equiv 1 \pmod{11} \\ 7 \cdot 8 \equiv 8 \cdot 7 \equiv 1 \pmod{11}. \end{aligned}$$

Assim, no fatorial de $p - 1 = 10$, temos:

$$\begin{aligned} 10! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 \pmod{11} \\ &\equiv 10 \equiv -1 \pmod{11}. \end{aligned}$$

Demonstração do Teorema de Wilson. Para $p = 2$ a afirmação é $1! \equiv -1 \pmod{2}$, que é verdadeira. Suponha então p ímpar. Dados a e b distintos em $\{1, \ldots, p-1\}$, vamos associar a e b se $a \cdot b \equiv 1 \pmod{p}$. No exemplo acima, com $p = 11$, associamos 2 e 6, 3 e 4, 5 e 9, 7 e 8. Pelo Teorema 33, para todo $a \in \{1, \ldots, p-1\}$, existe um inteiro x tal que $ax \equiv 1 \pmod{p}$. Como $\{0, \ldots, p-1\}$ é um SCR, podemos encontrar um único $a' \in \{0, \ldots, p-1\}$ tal que $a \cdot a' \equiv 1 \pmod{p}$.

Note que a' não pode ser 0, pois $a \cdot 0 = 0 \not\equiv 1 \pmod{p}$. Se $a' \neq a$, associamos a e a'. Se $a' = a$, a não está associado a ninguém. Isso ocorre exatamente quando:

$$a^2 \equiv 1 \pmod{p}.$$

Mas isso é equivalente a:

$$\begin{aligned} p|(a^2-1) &\iff p|(a-1)(a+1) \\ &\iff p|(a-1) \text{ ou } p|(a+1) \\ &\iff a \equiv 1 \pmod{p} \text{ ou } a \equiv -1 \pmod{p}. \end{aligned}$$

Ou seja, provamos que todo número diferente de 1 e $p-1$ em $\{1, \ldots, p-1\}$ está associado a um número $b \neq a$ no mesmo conjunto. Além disso, essa associação é simétrica. Em outras palavras, o conjunto $\{2, \ldots, p-2\}$ pode ser dividido em pares $(x_1, y_1),\ (x_2, y_2),\ \ldots (x_k, y_k)$ onde $k = \frac{p-3}{2}$ e x_i, y_i são tais que $x_i y_i \equiv 1 \pmod{p}$.

Assim,

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \ldots (p-2) \cdot (p-1) \\ &= 1 \cdot (x_1 y_1) \cdot (x_2 y_2) \ldots (x_k y_k) \cdot (p-1) \\ &\equiv 1 \cdot 1 \cdots 1 \cdot (p-1) \equiv -1 \pmod{p}. \end{aligned}$$

□

2.8 Teorema Chinês dos Restos

Vimos no Corolário 34 que uma congruência do tipo

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

é, quando possui solução, equivalente a uma congruência do tipo

$$x \equiv c \pmod{\frac{m}{d}}, \quad \text{onde } d = (a, m).$$

Teorema 42 (TCR)**.** *Sejam $m_1, \ldots, m_k$ inteiros positivos relativamente primos dois a dois e $a_1, \ldots, a_k$ inteiros. Então existe a inteiro tal que o sistema de congruências*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

é equivalente à congruência

$$x \equiv a \pmod{m_1 m_2 \ldots m_k}.$$

Exemplo. Vamos estudar o sistema:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 9 \pmod{5} \\ x \equiv -4 \pmod{7}. \end{cases}$$

Temos $x \equiv 2 \pmod{3} \iff x = 3k + 2$ para algum k. Substituindo nas outras,

$$\begin{cases} 3k+2 \equiv 9 \pmod{5} \\ 3k+2 \equiv -4 \pmod{7} \end{cases} \iff \begin{cases} 3k \equiv 7 \pmod{5} \\ 3k \equiv -6 \pmod{7}. \end{cases}$$

Notemos que $3 \cdot 2 = 6 \equiv 1 \pmod 5$. Assim,

$$3k \equiv 7 \pmod 5 \iff k \equiv 14 \equiv 4 \pmod 5.$$

Por outro lado:

$$3k \equiv -6 \pmod 7 \iff k \equiv -2 \pmod 7.$$

Ou seja, o sistema é equivalente a:

$$\begin{cases} k \equiv 4 \pmod 5 \\ k \equiv -2 \pmod 7. \end{cases}$$

Temos $k \equiv 4 \pmod 5 \iff k = 5l + 4$ para algum l. Substituindo, temos

$$5l + 4 \equiv -2 \pmod 7 \iff 5l \equiv -6 \pmod 7.$$

Como $5 \cdot 3 = 15 \equiv 1 \pmod 7$,

$$5l \equiv -6 \pmod 7 \iff l \equiv -18 \equiv 3 \pmod 7.$$

Por fim, $l \equiv 3 \pmod 7 \iff l = 7j + 3$ para algum j. Logo, x é solução do sistema se, e somente se,

$$\begin{aligned} x &= 3k + 2 = 3(5l + 4) + 2 \\ &= 15l + 14 \\ &= 15(7j + 3) + 14 \\ &= 105j + 59. \end{aligned}$$

Ou seja, provamos que o sistema é equivalente à congruência:

$$x \equiv 59 \pmod{105}.$$

Demonstração do TCR. Faremos por indução em k. A parte mais difícil é o caso inicial $k = 2$:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2}. \end{cases}$$

Como no exemplo, $x \equiv a_1 \pmod{m_1} \iff x = m_1 t + a_1$. Substituindo na segunda congruência:

$$m_1 t + a_1 \equiv a_2 \pmod{m_2} \implies m_1 t \equiv a_2 - a_1 \pmod{m_2}.$$

Como $(m_1, m_2) = 1$, sabemos que existe um c tal que a congruência acima é equivalente a $t \equiv c \pmod{m_2} \iff t = m_2 l + c$.

Portanto, o sistema é equivalente a:

$$\begin{aligned} x &= m_1 t + a_1 \\ &= m_1(m_2 l + c) + a_1 \\ &= m_1 m_2 l + (m_1 c + a_1) \end{aligned}$$

$$\iff x \equiv a \pmod{m_1 m_2},$$

onde $a = m_1 c + a_1$.

Hipótese de indução: Suponha que dá certo para sistemas com $2, \ldots, k-1$ congruências.

Passo indutivo: Considere o sistema

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ & \vdots \\ x & \equiv a_k \pmod{m_k}. \end{cases}$$

Pela hipótese de indução, as $k-1$ primeiras linhas do sistema são equivalentes a uma única congruência $x \equiv a' \pmod{m_1 \ldots m_{k-1}}$. Logo, o sistema original é equivalente a:

$$\begin{cases} x & \equiv a' \pmod{m_1 \ldots m_{k-1}} \\ x & \equiv a_k \pmod{m_k}. \end{cases}$$

Como $(m_1 \ldots m_{k-1}, m_k) = 1$, pelo caso $k = 2$ demonstrado acima, o resultado segue. □

A condição de que $(m_i, m_j) = 1$ é essencial. De fato, o sistema:

$$\begin{cases} x & \equiv 2 \pmod{4} \\ x & \equiv 3 \pmod{6} \end{cases}$$

não possui solução.

Apesar disto, o teorema admite a seguinte versão mais geral:

Proposição 43. *Sejam $m_1, \ldots, m_k$ inteiros positivos. Então o sistema:*

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ & \vdots \\ x & \equiv a_k \pmod{m_k} \end{cases}$$

possui solução se, e somente se, $(m_i, m_j) \mid a_i - a_j$ para todos os $i, j \in \{1, \ldots, k\}$. Neste caso, existe a inteiro tal que o sistema é equivalente à congruência

$$x \equiv a \pmod{[m_1, \ldots, m_k]}$$

onde $[m_1, \ldots, m_k]$ denota o mínimo múltiplo comum.

Demonstração. Exercício. □

Observe que os sistemas de congruência que estamos considerando se comportam de maneira linear. Se y e z são soluções dos sistemas

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad \text{e} \quad \begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

respectivamente. Então $y + z$ é solução do sistema

$$\begin{cases} x \equiv a_1 + b_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k + b_k \pmod{m_k} \end{cases}$$

e cy é solução de

$$\begin{cases} x \equiv c \cdot a_1 \pmod{m_1} \\ \vdots \\ x \equiv c \cdot a_k \pmod{m_k}. \end{cases}$$

Em particular, para resolver o sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

basta considerar os casos:

$$\begin{cases} x \equiv 0 \pmod{m_1} \\ \quad \vdots \\ x \equiv 0 \pmod{m_{j-1}} \\ x \equiv 1 \pmod{m_j} \\ x \equiv 0 \pmod{m_{j+1}} \\ \quad \vdots \\ x \equiv 0 \pmod{m_k}. \end{cases} \tag{2.1}$$

Suponha novamente que os m_i são relativamente primos dois a dois. Para resolver o sistema acima, veja que o sistema formado por todas as linhas exceto a j-ésima é equivalente a $x = M_j t$, onde

$$M_j = m_1 \dots m_{j-1} m_{j+1} \dots m_k = \prod_{i \neq j} m_i.$$

Assim, o sistema é equivalente a

$$\begin{cases} x = M_j t \\ M_j t \equiv 1 \pmod{m_j}. \end{cases}$$

Como $(M_j, m_j) = 1$, a congruência $M_j t \equiv 1 \pmod{m_j}$ possui solução. Seja N_j uma solução (Ou seja, N_j é um inverso multiplicativo de M_j módulo m_j). Assim,

$$M_j t \equiv 1 \pmod{m_j} \iff t \equiv N_j \pmod{m_j}.$$

Conclusão: $M_j N_j$ é uma solução do sistema (2.1).

Logo, pelas propriedades de soma e multiplicação por escalares de sistemas que vimos acima, o sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

possui a seguinte solução:

$$x = a_1 M_1 N_1 + \cdots + a_k M_k N_k.$$

onde $M_j = \prod_{\substack{i=1 \\ i \neq j}}^{k} m_i$ e N_j é um inverso multiplicativo de M_j módulo m_j.

Por conta do TCR, podemos, na verdade, dizer que o sistema é equivalente a

$$x \equiv a_1 M_1 N_1 + \cdots + a_k M_k N_k \pmod{m_1 \dots m_k}.$$

Exemplo.

$$\begin{cases} x \equiv 8 \pmod 5 \\ x \equiv 20 \pmod{11} \\ x \equiv 4 \pmod{13}. \end{cases}$$

Nesse caso, $m_1 = 5,\ m_2 = 11,\ m_3 = 13, a_1 = 8,\ a_2 = 20,\ a_3 = 4.$
Então $M_1 = 11 \cdot 13 = 143,\ M_2 = 5 \cdot 13 = 65,\ M_3 = 5 \cdot 11 = 55.$

- $M_1 = 143 \equiv 3 \pmod 5$. Assim, $N_1 = 2$ é um inverso multiplicativo de $M_1 \pmod{m_1}$.
- $M_2 = 65 \equiv 10 \equiv -1 \pmod{11}$. Assim, $N_2 = -1$ é um inverso multiplicativo de $M_2 \pmod{m_2}$.
- $M_3 = 55 \equiv 3 \pmod{13}$. Como $3 \cdot 9 = 27 = 2 \cdot 13 + 1$, segue que $N_3 = 9$ é um inverso multiplicativo de $M_3 \pmod{m_3}$.

Com isso chegamos ao valor

$$x = 8 \cdot 143 \cdot 2 + 20 \cdot 65 \cdot (-1) + 4 \cdot 55 \cdot 9 = 2968.$$

Ou seja, o sistema é equivalente a

$$X \equiv 2968 \pmod{715} \iff x \equiv 108 \pmod{715}.$$

2.9 Cálculo de $\phi(m)$

- Se $m = p$ é um número primo:

$$\begin{aligned} \phi(p) &= \#\{0 \leq i \leq p-1 \mid (i,p) = 1\} \\ &= \#\{1, \dots, p-1\} = p - 1. \end{aligned}$$

- Se $m = p^k$, com p primo:

$$\phi(p^k) = \#\{0 \leq i \leq p^k - 1 \mid (i, p^k) = 1\}.$$

Como $(i, p^k) = p^j$ para algum $j \leq k$. Temos que $j \geq 1 \iff p \mid i$. Ou seja:

$$\begin{aligned} \phi(p^k) &= \#\{0 \leq i \leq p^k - 1 \mid p \nmid i\} \\ &= \#\{0 \leq i \leq p^k - 1\} - \#\{0 \leq pj \leq p^k - 1\}. \end{aligned}$$

Claramente $\#\{0 \leq i \leq p^k - 1\} = p^k$. Por outro lado,

$$0 \leq pj \leq p^k - 1 \iff 0 \leq j \leq \lfloor \frac{p^k - 1}{p} \rfloor = p^{k-1} - 1$$

Assim,

$$\#\{0 \leq pj \leq p^k - 1\} = \#\{0 \leq j \leq p^{k-1} - 1\} = p^{k-1}.$$

Portanto,

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

Exemplo. $p = 3$, $k = 3$.

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

$$\phi(27) = 27 - 9.$$

O cálculo de $\phi(m)$ no caso geral se reduz ao caso das potências de primos graças ao seguinte resultado.

Proposição 44. *Sejam $m_1, m_2 > 0$ inteiros tais que $(m_1, m_2) = 1$. Então:*

$$\phi(m_1 m_2) = \phi(m_1)\phi(m_2).$$

Demonstração. Sejam S_1 um SCR módulo m_1, S_2 um SCR módulo m_2 e S um SCR módulo $m_1 m_2$. Vamos construir uma *bijeção*

$$S_1 \times S_2 \xrightarrow{f} S$$

com a seguinte propriedade:

$$f(a_1, a_2) \text{ é relativamente primo com } m_1 m_2 \iff (a_1, m_1) = 1 \text{ e } (a_2, m_2) = 1.$$

Dados $a_1 \in S_1$ e $a_2 \in S_2$, o TCR (Teorema Chinês dos Restos) diz que o sistema

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \end{cases}$$

é equivalente a $x \equiv a \pmod{m_1 m_2}$, para algum inteiro a. Assim, defina $f(a_1, a_2)$ como sendo o único elemento de S tal que $f(a_1, a_2) \equiv a \pmod{m_1 m_2}$. Como S é um SCR, o elemento $f(a_1, a_2)$ de fato existe e é único.

- f **é injetiva:** Suponha que $f(a_1, a_2) = f(a_1', a_2') = r$. Então

  $$r \equiv a_1 \pmod{m_1} \quad \text{e} \quad r \equiv a_1' \pmod{m_1}.$$

  Isso implica que $a_1 \equiv a_1' \pmod{m_1}$. Como a_1, a_1' pertencem ao mesmo SCR, segue que $a_1 = a_1'$. Da mesma maneira segue também que $a_2 = a_2'$.

- f **é sobrejetiva:** Dado $a \in S$, basta escolher $a_1 \in S_1$ tal que $a_1 \equiv a \pmod{m_1}$ e $a_2 \in S_2$ tal que $a_2 \equiv a \pmod{m_2}$. Segue do TCR e do fato que S é um SCR que $f(a_1, a_2) = a$.

Por fim, um inteiro n é relativamente primo com $m_1 m_2$ se, e somente se, $(n, m_1) = 1$ e $(n, m_2) = 1$. Como $f(a_1, a_2) \equiv a_1 \pmod{m_1}$,

$$(f(a_1, a_2), m_1) = 1 \iff (a_1, m_1) = 1.$$

Analogamente,

$$(f(a_1, a_2), m_2) = 1 \iff (a_2, m_2) = 1.$$

Portanto, f se restringe a uma bijeção entre o conjunto dos pares $(a_1, a_2) \in S_1 \times S_2$ tais que $(a_1, m_1) = 1$ e $(a_2, m_2) = 1$ e o conjunto dos $a \in S$ tais que $(a, m_1 m_2) = 1$. Pela Proposição 38, o primeiro conjunto tem $\phi(m_1)\phi(m_2)$ elementos e o segundo tem $\phi(m_1 m_2)$. Logo $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$. □

Teorema 45. *Seja $m > 0$ um número inteiro e seja $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sua fatoração em números primos. Então:*

$$\begin{aligned}\phi(m) &= \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\ &= m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

Demonstração. Como p_k não divide $p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}}$, temos $(p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}}, p_k^{\alpha_k}) = 1$. Aplicando repetidamente a Proposição 44, obtemos

$$\begin{aligned}\phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \phi(p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}})\phi(p_k^{\alpha_k}) \\ &= \phi(p_1^{\alpha_1} \cdots p_{k-2}^{\alpha_{k-2}})\phi(p_{k-1}^{\alpha_{k-1}})\phi(p_k^{\alpha_k}) \\ &= \cdots = \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}).\end{aligned}$$

As outras duas igualdades seguem da fórmula $\phi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right)$, obtida no início desta seção. □

2.10 Congruências Módulo Potência de Primo

2.10.1 Motivação

Suponha que saibamos resolver uma congruência do tipo $f(x) \equiv 0 \pmod{p}$, onde $f(x)$ é um polinômio. Queremos resolver $f(x) \equiv 0 \pmod{p^2}$ ou, mais geralmente, $f(x) \equiv 0 \pmod{p^k}$.

Considere $f(x) = x^2 - 2$. Note que $3^2 - 2 = 7 \equiv 0 \pmod 7$, ou seja, $f(3) \equiv 0 \pmod 7$.

Objetivo: Construir uma solução módulo $7^2 = 49$. O número 3 não funciona diretamente: $3^2 - 2 = 7 \not\equiv 0 \pmod{49}$.

Observação: Se $f(x) \equiv 0 \pmod{49}$, então $f(x) \equiv 0 \pmod 7 \iff x^2 \equiv 2 \pmod 7$. Testando as possibilidades módulo 7:

$$x^2 \equiv 2 \pmod 7 \iff x \equiv 3 \pmod 7 \quad \text{ou} \quad x \equiv 4 \pmod 7.$$

Vamos tentar encontrar uma solução da forma $x \equiv 3 \pmod 7$, isto é, $x = 7k + 3$. Substituindo em $x^2 - 2 \equiv 0 \pmod{49}$:

$$\begin{aligned}(7k+3)^2 - 2 &\equiv 0 \pmod{49}\\ 49k^2 + 42k + 9 - 2 &\equiv 0 \pmod{49}\\ 42k + 7 &\equiv 0 \pmod{49}\\ 6k + 1 &\equiv 0 \pmod 7\\ k &\equiv 1 \pmod 7.\end{aligned}$$

Em particular, $k = 1$ é uma solução, o que gera $x = 7(1) + 3 = 10$. **Verificando:** $10^2 - 2 = 98 = 2 \cdot 49 \equiv 0 \pmod{49}$.

Porém, $10^2 - 2 = 98 \not\equiv 0 \pmod{7^3 = 343}$.

Para encontrar uma solução módulo 7^3, procuramos uma solução da forma $x = 49k + 10$:

$$\begin{aligned}(49k+10)^2 - 2 &\equiv 0 \pmod{7^3}\\ 7^4k^2 + 980k + 98 &\equiv 0 \pmod{7^3}\\ 980k + 98 &\equiv 0 \pmod{343}\\ 20k + 2 \equiv 0 \pmod 7 &\iff 6k + 2 \equiv 0 \pmod 7 \iff k \equiv 2 \pmod 7.\end{aligned}$$

Em particular, para $k = 2$, temos $x = 49(2) + 10 = 108$. Verificando: $108^2 - 2 = 11662 = 34 \cdot 343 \equiv 0 \pmod{7^3}$.

2.10.2 Derivada de um Polinômio

Definição. Se $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ é um polinômio, sua **derivada** é o polinômio:

$$f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2x + a_1.$$

Observação. Se os coeficientes de f são inteiros, os coeficientes de f' também são inteiros.

Exemplos.

- $f(x) = x^2 - 2 \implies f'(x) = 2x$
- $f(x) = x^3 + 3x + 9 \implies f'(x) = 3x^2 + 3$

2.10.3 O Lema de Hensel

Teorema 46 (Lema de Hensel)**.** *Seja p um número primo, $j \geq 1$ e $f(x)$ um polinômio com coeficientes inteiros. Seja $a \in \mathbb{Z}$ tal que:*

$$f(a) \equiv 0 \pmod{p^j} \quad e \quad f'(a) \not\equiv 0 \pmod p.$$

Então, o sistema

$$\begin{cases} f(x) \equiv 0 \pmod{p^{j+1}} \\ x \equiv a \pmod{p^j} \end{cases}$$

possui uma única solução módulo p^{j+1}.

Para provar este teorema, utilizamos o seguinte lema auxiliar:

Lema 47. *Para quaisquer $a, t \in \mathbb{Z}$ e $j \geq 1$, vale a congruência:*

$$f(a + tp^j) \equiv f(a) + f'(a) \cdot tp^j \pmod{p^{2j}}.$$

Demonstração do Lema. Por linearidade, basta demonstrar o resultado para monômios da forma $f(x) = x^n$. Ou seja, queremos mostrar que:

$$(a + tp^j)^n \equiv a^n + na^{n-1}tp^j \pmod{p^{2j}}.$$

Pelo Binômio de Newton:

$$(a + tp^j)^n = a^n + na^{n-1}tp^j + \binom{n}{2}a^{n-2}(tp^j)^2 + \cdots + (tp^j)^n.$$

Como $j \geq 1$, todos os termos a partir de $\binom{n}{2}a^{n-2}(tp^j)^2$ possuem potências de p maiores ou iguais a p^{2j}, sendo portanto divisíveis por p^{2j}. Logo:

$$(a + tp^j)^n \equiv a^n + na^{n-1}tp^j \pmod{p^{2j}}. \qquad \square$$

Demonstração do Lema de Hensel. O sistema

$$\begin{cases} f(x) \equiv 0 \pmod{p^{j+1}} \\ x \equiv a \pmod{p^j} \end{cases}$$

é equivalente a procurar soluções da forma $x = a + tp^j$ tais que $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Pelo Lema, como $2j \geq j + 1$ para $j \geq 1$, a congruência reduz-se a:

$$f(a) + f'(a)tp^j \equiv 0 \pmod{p^{j+1}}.$$

Como $f(a) \equiv 0 \pmod{p^j}$, podemos dividir toda a congruência por p^j:

$$\frac{f(a)}{p^j} + f'(a)t \equiv 0 \pmod{p}.$$

Como $\text{mdc}(f'(a), p) = 1$ (já que $f'(a) \not\equiv 0 \pmod{p}$), esta congruência linear em t possui uma única solução módulo p, digamos $t \equiv a_0 \pmod{p}$.

Escrevendo $t = a_0 + pk$, obtemos:

$$x = a + p^j(a_0 + pk) = a + a_0p^j + p^{j+1}k \iff x \equiv a + a_0p^j \pmod{p^{j+1}}$$

que é a única solução módulo p^{j+1}. $\square$

2.10.4 Exemplo: $x^3 + 3x + 1 \equiv 0 \pmod{7^3}$

Exemplo. Resolva a congruência $x^3 + 3x + 1 \equiv 0 \pmod{7^3}$.

1º Passo: Resolver módulo 7. Testando os resíduos de 0 a 6:

$$\begin{aligned} 0^3 + 3(0) + 1 &\equiv 1 \pmod{7} \\ 1^3 + 3(1) + 1 &\equiv 5 \pmod{7} \\ 2^3 + 3(2) + 1 &\equiv 1 \pmod{7} \\ 3^3 + 3(3) + 1 &\equiv 2 \pmod{7} \\ 4^3 + 3(4) + 1 = 77 &\equiv 0 \pmod{7} \quad \checkmark \\ 5^3 + 3(5) + 1 &\equiv 1 \pmod{7} \\ 6^3 + 3(6) + 1 &\equiv 4 \pmod{7}. \end{aligned}$$

Portanto, a única solução módulo 7 é $x \equiv 4 \pmod 7$.

Calculando a derivada $f'(x) = 3x^2 + 3$:

$$f'(4) = 3(4^2) + 3 = 51 \equiv 2 \not\equiv 0 \pmod 7$$

2º Passo: Resolver módulo $49 = 7^2$. Escrevemos $x = 7k + 4$. Aplicando o desenvolvimento do Lema de Hensel:

$$f(7k + 4) \equiv f(4) + f'(4) \cdot 7k \pmod{49}.$$

Queremos $f(7k + 4) \equiv 0 \pmod{49}$:

$$\begin{aligned} 77 + 51 \cdot 7k &\equiv 0 \pmod{49} \\ 11 + 51k &\equiv 0 \pmod 7 \quad \text{(dividindo por 7)} \\ 4 + 2k \equiv 0 \pmod 7 &\iff 2k \equiv 3 \pmod 7 \\ k &\equiv 5 \pmod 7. \end{aligned}$$

Assim, a única solução módulo 49 é $x \equiv 7(5) + 4 = 39 \equiv -10 \pmod{49}$.

3º Passo: Resolver módulo $343 = 7^3$. Escrevemos $x = -10 + 49k$.

$$f(-10 + 49k) \equiv f(-10) + f'(-10) \cdot 49k \pmod{343}.$$

Calculando $f(-10)$:

$$f(-10) = (-10)^3 + 3(-10) + 1 = -1029 = -3 \cdot 343 \equiv 0 \pmod{343}.$$

Logo:

$$f'(-10) \cdot 49k \equiv 0 \pmod{343} \iff f'(-10) \cdot k \equiv 0 \pmod 7.$$

Como $-10 \equiv 4 \pmod 7$, temos $f'(-10) \equiv f'(4) = 51 \not\equiv 0 \pmod 7$. Portanto:

$$f'(-10)k \equiv 0 \pmod 7 \iff k \equiv 0 \pmod 7.$$

Assim, a única solução módulo 343 é $x \equiv -10 \equiv 333 \pmod{343}$.

2.10.5 Variações do Lema de Hensel

Lembre que, pelo Teorema 46 (**Lema de Hensel**), se $f(a) \equiv 0 \pmod{p^j}$ e $f'(a) \not\equiv 0 \pmod p$, então a solução a se levanta de modo único a uma solução módulo p^{j+1}.

Este resultado pode ser usado como passo indutivo para provar a seguinte versão:

Corolário 48. *Seja p um primo, $f(x)$ um polinômio com coeficientes inteiros e $a \in \mathbb{Z}$ tal que $f(a) \equiv 0 \pmod p$ e $f'(a) \not\equiv 0 \pmod p$. Então, para todo $j \geq 1$, o sistema:*

$$\begin{cases} f(x) \equiv 0 \pmod{p^j} \\ x \equiv a \pmod p \end{cases}$$

possui uma única solução módulo p^j.

Temos ainda uma outra versão mais forte (porém menos usada), cuja demonstração segue por uma pequena modificação do argumento original (exercício):

Teorema 49. *Seja p primo e $f(x)$ um polinômio com coeficientes inteiros. Se $a \in \mathbb{Z}$ é tal que $f(a) \equiv 0 \pmod{p^j}$ e $p^t \parallel f'(a)$, com $j \geq 2t+1$. Então, para todo $b \equiv a \pmod{p^{j-t}}$, temos $f(b) \equiv f(a) \pmod{p^j}$ e $p^t \parallel f'(b)$. Além disso, o sistema:*

$$\begin{cases} f(x) \equiv 0 \pmod{p^{j+1}} \\ x \equiv a \pmod{p^{j-t}} \end{cases}$$

possui uma única solução módulo p^{j-t+1}.

Observação. A notação $p^t \parallel m$ significa que $p^t \mid m$, mas $p^{t+1} \nmid m$.

Exemplo. $3^2 \parallel 36$, pois $9 \mid 36$, mas $27 \nmid 36$.

2.10.6 Exemplo: $x^2 + x + 223 \equiv 0 \pmod{3^j}$

Exemplo. Estudar as soluções de $x^2 + x + 223 \equiv 0 \pmod{3^j}$.

Caso $j = 1$:

$$x^2 + x + 223 \equiv 0 \pmod 3 \iff x^2 + x + 1 \equiv 0 \pmod 3.$$

Testando os resíduos módulo 3:

- $0^2 + 0 + 1 = 1 \not\equiv 0 \pmod 3$
- $1^2 + 1 + 1 = 3 \equiv 0 \pmod 3$ ✓
- $2^2 + 2 + 1 = 7 \equiv 1 \not\equiv 0 \pmod 3$

A única solução módulo 3 é $x \equiv 1 \pmod 3 \implies x = 1 + 3k$.

Caso $j = 2$ (Módulo 9): Não usaremos o Lema de Hensel em si, mas a estratégia de sua prova. Queremos encontrar k tal que $f(1 + 3k) \equiv 0 \pmod 9$. Pela expansão:

$$f(1 + 3k) \equiv f(1) + 3k \cdot f'(1) \pmod 9.$$

Como $f(1) = 1^2 + 1 + 223 = 225 \equiv 0 \pmod 9$ e $f'(x) = 2x + 1 \implies f'(1) = 3$:

$$f(1 + 3k) \equiv 225 + 9k \equiv 0 \pmod 9.$$

Portanto, para **qualquer** $k \in \mathbb{Z}$, $x = 1 + 3k$ é solução módulo 9. As soluções módulo 9 são: $1, 4, 7 \pmod 9$.

Caso $j = 3$ (Módulo 27): Analisamos cada família de soluções módulo 9:

(i) $f(1 + 9k) \equiv f(1) + 9kf'(1) \pmod{27} \equiv 225 + 27k \equiv 225 \equiv 9 \not\equiv 0 \pmod{27}$. Logo, não há soluções dessa forma.

(ii) $f(4 + 9k) \equiv f(4) + 9kf'(4) \pmod{27}$. Calculando: $f(4) = 4^2 + 4 + 223 = 243 = 27 \times 9 \equiv 0 \pmod{27}$ e $f'(4) = 2(4) + 1 = 9$. Assim: $f(4 + 9k) \equiv 0 + 81k \equiv 0 \pmod{27}$. Logo, para qualquer $k \in \mathbb{Z}$, $x = 4 + 9k$ é solução módulo 27.

(iii) Como em (i): $f(7) = 279 \equiv 9 \pmod{27}$ e $f'(7) = 15$, de modo que $f(7 + 9k) \equiv 9 + 135k \equiv 9 \not\equiv 0 \pmod{27}$. Logo, não há soluções dessa forma.

Conclusão: as soluções módulo 27 são os $x \equiv 4 \pmod 9$.

2.11 Congruências Polinomiais Módulo p

Lembre que, pelo Teorema de Fermat, $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$. Em outras palavras, o polinômio $f(x) = x^p - x$ possui p soluções módulo p.

Assim, por exemplo, o polinômio $f(x) = x^{p+2} - 3x^{p+1} + 3x + 2$ tem as mesmas soluções módulo p que o polinômio $x^3 - 3x^2 + 3x + 2$.

Definição. Um polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, com $a_n \neq 0$, é dito **mônico** se $a_n = 1$.

Teorema 50. *Seja p um número primo e f um polinômio de grau $n \geq p$ com coeficientes inteiros. Então, ou $f(x) \equiv 0 \pmod{p}$ para todo $x \in \mathbb{Z}$, ou existe um polinômio g com coeficientes inteiros, mônico e com $\deg(g) < p$ tal que:*

$$f(x) \equiv 0 \pmod{p} \iff g(x) \equiv 0 \pmod{p}.$$

Demonstração. Pelo Teorema de Fermat, $x^p \equiv x \pmod{p}$. Consequentemente:

$$x^{p+1} \equiv x^2 \pmod{p}, \quad x^{p+2} \equiv x^3 \pmod{p}, \quad \ldots, \quad x^{2p-2} \equiv x^{p-1} \pmod{p}.$$

De modo geral:

$$(\star) \quad x^{t+(p-1)k} \equiv x^t \pmod{p} \quad (t \geq 1).$$

Escrevendo $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, se $n \geq p$, podemos usar $(\star)$ para substituir potências x^m (com $m \geq p$) por potências de grau menor que p, obtendo um polinômio $g(x)$ com $\deg(g) < p$ tal que:

$$f(x) \equiv g(x) \pmod{p} \quad \forall x \in \mathbb{Z}.$$

Escreva $g(x) = b_{p-1}x^{p-1} + \cdots + b_1 x + b_0$.

- Se $p \mid b_i$ para todo $i = 0, 1, \ldots, p-1$, então $f(x) \equiv 0 \pmod{p}$ para todo $x \in \mathbb{Z}$.
- Caso contrário, seja k o maior índice para o qual $p \nmid b_k$. Assim, $g(x) \equiv b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0 \pmod{p}$. Como $\text{mdc}(b_k, p) = 1$, existe $c_k \in \mathbb{Z}$ tal que $b_k c_k \equiv 1 \pmod{p}$. Logo, $g(x) \equiv 0 \pmod{p} \iff c_k g(x) \equiv 0 \pmod{p}$. O polinômio desejado é $\tilde{g}(x) = x^k + c_k b_{k-1}x^{k-1} + \cdots + c_k b_0$.

□

Exemplo. Reduzir $f(x) = 3x^{10} + x^5 + 7x^2 + x + 3 \pmod{5}$.

Pelo Teorema de Fermat ($p = 5$), $x^5 \equiv x \pmod{5}$ e $x^{10} \equiv x^2 \pmod{5}$ para todo $x \in \mathbb{Z}$. Substituindo em $f(x)$:

$$f(x) \equiv 3x^2 + x + 7x^2 + x + 3 \equiv 10x^2 + 2x + 3 \equiv 2x + 3 \pmod{5}.$$

Como $2 \cdot 3 \equiv 1 \pmod{5}$, multiplicamos por 3:

$$\begin{aligned} 2x + 3 \equiv 0 \pmod{5} &\iff x + 9 \equiv 0 \pmod{5}, \\ &\iff x + 4 \equiv 0 \pmod{5}. \end{aligned}$$

Assim, o polinômio mônico equivalente é $\tilde{g}(x) = x + 4$ (ou $x - 1$).

Definição. Seja $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, com algum coeficiente não divisível por p. O **grau módulo** p de f é o maior inteiro k tal que $p \nmid a_k$. Notação: $\deg_p(f)$ ou $\partial_p(f)$.

Observação. $\deg_p(f) \leq \deg(f)$.

Pelo Teorema 50, para qualquer polinômio $f(x)$ módulo um primo p, podemos encontrar um polinômio $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ com $m \leq p - 1$ (ou $g = 0$) tal que $f(x) \equiv 0 \pmod{p} \iff g(x) \equiv 0 \pmod{p}$, preservando as mesmas raízes.

2.11.1 Número de Soluções de $f(x) \equiv 0 \pmod{p}$

Teorema 51. *Seja f um polinômio com grau módulo p dado por $\deg_p(f) = m$. A congruência*

$$f(x) \equiv 0 \pmod{p}$$

possui no máximo m soluções incongruentes módulo p.

Análise dos Casos Iniciais:

- **Caso $\deg_p(f) = 0$:** Significa que existe $a \in \mathbb{Z}$ tal que $a \not\equiv 0 \pmod{p}$ e $f(x) \equiv a \pmod{p}$. Em particular, $f(x) \not\equiv 0 \pmod{p}$ para todo $x \in \mathbb{Z}$, logo possui 0 soluções.
- **Caso $\deg_p(f) = 1$:** Temos $f(x) \equiv ax + b \pmod{p}$ com $a \not\equiv 0 \pmod{p}$. A congruência $ax + b \equiv 0 \pmod{p}$ possui exatamente 1 solução módulo p.
- **Caso $\deg_p(f) = 2$:** Temos $f(x) \equiv ax^2 + bx + c \pmod{p}$ com $a \not\equiv 0 \pmod{p}$. Suponha que possua pelo menos 2 soluções, digamos a_1 e a_2. Considere o polinômio:

  $$g(x) = f(x) - a(x - a_1)(x - a_2).$$

  Por construção, $g(a_1) \equiv g(a_2) \equiv 0 \pmod{p}$. Além disso, o termo de grau 2 cancela-se, logo $\deg_p(g) \leq 1$.

  - Se $\deg_p(g) = 1$, pelo caso anterior $g(x) \equiv 0 \pmod{p}$ teria exatamente 1 solução, uma contradição pois a_1 e a_2 são soluções.
  - Se $\deg_p(g) = 0$, pelo caso anterior não teria soluções, contradição.
  - Logo, $g(x) \equiv 0 \pmod{p}$ para todo x, o que implica:

    $$f(x) \equiv a(x - a_1)(x - a_2) \pmod{p}.$$

    Neste caso, $f(x) \equiv 0 \pmod{p}$ se, e somente se, $x \equiv a_1 \pmod{p}$ ou $x \equiv a_2 \pmod{p}$, possuindo exatamente 2 soluções.

Demonstração Geral (por Indução em $m = \deg_p(f)$). **Hipótese de Indução:** Se $f \not\equiv 0 \pmod{p}$ e $\deg_p(f) \leq m$, então $f(x) \equiv 0 \pmod{p}$ possui no máximo m soluções.

Passo Indutivo: Seja $f(x)$ tal que $\deg_p(f) = m+1$. Escrevemos $f(x) = ax^{m+1} + \ldots$ com $a \not\equiv 0 \pmod{p}$.

Se $f(x) \equiv 0 \pmod{p}$ possui até $m + 1$ soluções, o resultado é válido. Caso contrário, suponha que possua mais de $m + 1$ soluções. Escolha $m + 1$ dessas soluções distintas módulo p, digamos $a_1, a_2, \ldots, a_{m+1}$. Considere o polinômio:

$$g(x) = f(x) - a(x - a_1)(x - a_2)\ldots(x - a_{m+1}).$$

Por construção, $g(a_1) \equiv g(a_2) \equiv \cdots \equiv g(a_{m+1}) \equiv 0 \pmod{p}$. O termo x^{m+1} cancela-se, logo $\deg_p(g) \leq m$.

Se $g \not\equiv 0 \pmod{p}$, pela hipótese de indução $g(x) \equiv 0 \pmod{p}$ deveria ter no máximo m soluções, o que contradiz o fato de ter $m + 1$ soluções.

Portanto, devemos ter $g(x) \equiv 0 \pmod{p}$, o que implica:

$$f(x) \equiv a(x - a_1)(x - a_2)\ldots(x - a_{m+1}) \pmod{p} \quad \forall x \in \mathbb{Z}.$$

Assim, $f(x) \equiv 0 \pmod{p} \iff x \equiv a_i \pmod{p}$ para algum $i \in \{1, \ldots, m + 1\}$, o que significa que $f(x) \equiv 0 \pmod{p}$ possui exatamente $m + 1$ soluções. □

Corolário 52. *Se $f(x)$ é um polinômio de grau $\deg(f) = n \geq 0$ e a congruência $f(x) \equiv 0 \pmod{p}$ possui mais de n soluções incongruentes módulo p, então todos os coeficientes de f são divisíveis por p (ou seja, $f(x) \equiv 0 \pmod{p}$).*

Corolário 53 (Fatoração de Polinômios Módulo p)**.** *Se $\deg_p(f) = m \geq 0$ e $f(x) \equiv 0 \pmod{p}$ possui exatamente m soluções $a_1, a_2, \ldots, a_m$ incongruentes módulo p, com coeficiente líder $a \not\equiv 0 \pmod{p}$, então:*

$$f(x) \equiv a(x - a_1)(x - a_2)\ldots(x - a_m) \pmod{p}.$$

Exemplo. Para o polinômio $f(x) = x^p - x$, sabemos pelo Teorema de Fermat que todos os resíduos $0, 1, 2, \ldots, p-1$ são soluções módulo p. Como $\deg_p(f) = p$, temos:

$$x^p - x \equiv x(x-1)(x-2)\ldots(x-(p-1)) \pmod{p}.$$

2.11.2 Fatoração de $x^p - x$ e Algoritmo da Divisão

Nosso objetivo é mostrar que, se $f(x)$ é mônico com $\deg_p(f) = m > 0$, então $f(x) \equiv 0 \pmod{p}$ possui exatamente m soluções se, e somente se, $f(x)$ é um fator módulo p do polinômio $x^p - x$. Para isso precisamos do algoritmo da divisão para polinômios.

Teorema 54 (Algoritmo da Divisão para Polinômios com Coeficientes Inteiros)**.** *Sejam $f(x)$ e $g(x)$ polinômios com coeficientes inteiros tais que $g(x)$ é mônico. Existem únicos polinômios $q(x)$ e $r(x)$ com coeficientes inteiros tais que:*

$$f(x) = g(x)q(x) + r(x)$$

onde $r(x) = 0$ ou $\deg(r) < \deg(g)$.

Demonstração do Algoritmo da Divisão. Indução no grau de $f(x)$:

- Se $f = 0$ ou $\deg(f) < \deg(g)$, tomamos $q(x) = 0$ e $r(x) = f(x)$.
- Seja $\deg(f) = n \geq m = \deg(g)$, com $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$. Se $f(x) = ax^n + \ldots$, consideramos o polinômio $f_1(x) = f(x) - ax^{n-m}g(x)$, cujo grau é estritamente menor que n. Pela hipótese de indução, $f_1(x) = g(x)q_1(x) + r(x)$ com $r = 0$ ou $\deg(r) < \deg(g)$. Substituindo, obtemos $f(x) = g(x)(ax^{n-m} + q_1(x)) + r(x)$.

A unicidade segue comparando graus: se $gq + r = gq' + r'$, então $g(q - q') = r' - r$ tem grau menor que o de g, logo $q = q'$ e $r = r'$. □

Exemplo. Efetuar a divisão polinomial de $f(x) = 3x^4 + 8x^2 + 9$ por $g(x) = x^2 + 3x + 5$:

$$\begin{aligned} f(x) - 3x^2 g(x) &= -9x^3 - 7x^2 + 9 \\ f(x) - 3x^2 g(x) + 9x g(x) &= 20x^2 + 45x + 9 \\ f(x) - g(x)(3x^2 - 9x + 20) &= -15x - 91. \end{aligned}$$

Portanto, $q(x) = 3x^2 - 9x + 20$ e o resto é $r(x) = -15x - 91$.

2.11.3 Caracterização do Número Máximo de Soluções

Teorema 55. *Seja $f(x)$ um polinômio mônico com $\deg_p(f) = m > 0$. A congruência $f(x) \equiv 0 \pmod{p}$ tem exatamente m soluções módulo p se, e somente se, existem polinômios $q(x)$ e $r(x)$ tais que:*

$$x^p - x = f(x)q(x) + r(x)$$

onde $q(x)$ é mônico de grau $\deg(q) = p - m$, e $r(x) \equiv 0 \pmod{p}$ (ou seja, todos os coeficientes de $r(x)$ são divisíveis por p).

Demonstração. ($\implies$) Suponha primeiro que $f(x) \equiv 0 \pmod{p}$ tem exatamente m soluções módulo p. Como $m \leq p$, pelo algoritmo da divisão, existem $q(x)$ e $r(x)$ tais que:

$$x^p - x = f(x)q(x) + r(x)$$

onde $r = 0$ ou $\deg(r) < m$.

Se a é uma solução de $f(a) \equiv 0 \pmod{p}$, pelo Teorema de Fermat temos $a^p - a \equiv 0 \pmod{p}$. Substituindo na equação:

$$0 \equiv f(a)q(a) + r(a) \equiv r(a) \pmod{p} \implies r(a) \equiv 0 \pmod{p}.$$

Logo, todas as m soluções de $f(x) \equiv 0 \pmod{p}$ também são raízes de $r(x) \equiv 0 \pmod{p}$. Se $r(x) \not\equiv 0 \pmod{p}$, como $\deg_p(r) < m$, o número de soluções de $r(x) \equiv 0 \pmod{p}$ seria no máximo $\deg_p(r) < m$, o que é uma contradição. Portanto, $r(x) \equiv 0 \pmod{p}$.

Para o grau e coeficiente líder de $q(x)$: como $r(x) \equiv 0 \pmod{p}$, o termo de maior grau de $x^p - x - r(x)$ é x^p. Escrevendo $q(x) = ax^k + \ldots$, temos $f(x)q(x) = ax^{m+k} + \cdots = x^p + \ldots$, o que implica $a = 1$ e $m + k = p \implies \deg(q) = p - m$. Logo $q(x)$ é mônico.

($\impliedby$) Suponha agora que $x^p - x = f(x)q(x) + r(x)$ com $q(x)$ mônico de grau $p - m$ e $r(x) \equiv 0 \pmod{p}$. Para todo $x \in \mathbb{Z}$, pelo Teorema de Fermat temos:

$$f(x)q(x) \equiv x^p - x \equiv 0 \pmod{p}.$$

Como f e q são mônicos de graus m e $p - m$, temos $\deg_p(f) = m$ e $\deg_p(q) = p - m$. Assim, $f(x) \equiv 0 \pmod{p}$ tem no máximo m soluções e $q(x) \equiv 0 \pmod{p}$ tem no máximo $p - m$ soluções. Como o produto $f(x)q(x) \equiv 0 \pmod{p}$ possui p soluções (todo resíduo módulo p), a única maneira disso ocorrer é se $f(x) \equiv 0 \pmod{p}$ tiver exatamente m soluções e $q(x) \equiv 0 \pmod{p}$ tiver exatamente $p - m$ soluções disjuntas. □

Exemplo. Para $p = 5$ e $f(x) = x^2 - 2x$, testando os resíduos módulo 5:

$$\begin{aligned}
&f(0) = 0 \equiv 0 \pmod{5} \quad \checkmark \\
&f(1) = -1 \equiv 4 \pmod{5} \\
&f(2) = 0 \equiv 0 \pmod{5} \quad \checkmark \\
&f(3) = 3 \pmod{5} \\
&f(4) = 8 \equiv 3 \pmod{5}.
\end{aligned}$$

Dividindo $x^5 - x$ por $x^2 - 2x$:

$$x^5 - x = (x^2 - 2x)(x^3 + 2x^2 + 4x + 8) + 15x.$$

Como o resto é $r(x) = 15x \equiv 0 \pmod{5}$ e $q(x) = x^3 + 2x^2 + 4x + 8$ é mônico de grau $5 - 2 = 3$, $f(x)$ tem exatamente 2 soluções. As soluções de $q(x) \equiv 0 \pmod{5}$ são $x \equiv 1, 3, 4 \pmod{5}$ (disjuntas das soluções de f).

2.11.4 Resumo dos Resultados sobre Congruências Polinomiais

Seja $f(x)$ um polinômio com coeficientes inteiros:

- Se todos os coeficientes de f são múltiplos de p ($f \equiv 0 \pmod{p}$), $\deg_p(f)$ não está definido e $f(x) \equiv 0 \pmod{p}$ possui p soluções.
- Se $f \not\equiv 0 \pmod{p}$, então $\deg_p(f)$ está definido e $f(x) \equiv 0 \pmod{p}$ tem no máximo $\deg_p(f)$ soluções.
- Se f é mônico, $f(x) \equiv 0 \pmod{p}$ tem exatamente $\deg_p(f)$ soluções se, e somente se, $f(x)$ divide $x^p - x \pmod{p}$.

2.11.5 Aplicação: Soluções de $x^d - 1 \equiv 0 \pmod{p}$

Corolário 56. *Se $d \mid (p-1)$, então a congruência*

$$x^d - 1 \equiv 0 \pmod{p}$$

possui exatamente d soluções módulo p.

Demonstração. Como $d \mid (p-1)$, escrevemos $p - 1 = dk$. Utilizando a identidade $y^k - 1 = (y-1)(y^{k-1} + \cdots + 1)$ para $y = x^d$:

$$x^{p-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1).$$

Multiplicando por x, obtemos:

$$x^p - x = (x^d - 1) \cdot x(x^{d(k-1)} + \cdots + 1).$$

Portanto, $x^d - 1$ é um fator de $x^p - x$ com resto $r(x) = 0$. Como $x^d - 1$ é mônico de grau d, pelo teorema anterior $x^d - 1 \equiv 0 \pmod{p}$ tem exatamente d soluções. □

Exemplo. Se $p = 3k+1$, então $3 \mid (p-1)$. Pelo corolário, $x^3 \equiv 1 \pmod{p}$ tem exatamente 3 soluções módulo p. Para $p = 13$ ($13 = 3(4) + 1$), calculando os cubos módulo 13:

$$0^3 \equiv 0, \quad 1^3 \equiv 1, \quad 2^3 \equiv 8, \quad 3^3 \equiv 1, \quad 4^3 \equiv 12, \quad 5^3 \equiv 8, \quad 6^3 \equiv 8$$

$$7^3 \equiv 5, \quad 8^3 \equiv 5, \quad 9^3 \equiv 1, \quad 10^3 \equiv 12, \quad 11^3 \equiv 5, \quad 12^3 \equiv 12 \pmod{13}.$$

As 3 soluções de $x^3 \equiv 1 \pmod{13}$ são $x \equiv 1, 3, 9 \pmod{13}$.

2.11.6 Propriedades dos Coeficientes e Teorema de Wolstenholme

Considere o polinômio cujas raízes são todos os resíduos módulo p:

$$f(x) = x(x-1)(x-2)\ldots(x-(p-1)) = x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0.$$

Como $f(x)$ é mônico de grau p e tem p raízes distintas módulo p, temos $f(x) \equiv x^p - x \pmod{p}$. Comparando os coeficientes:

- $a_0 = 0$ (pois $x \mid f(x)$).

- $a_1 = (-1)^{p-1}(p-1)! = (p-1)!$ (para p ímpar). Como $a_1 \equiv -1 \pmod{p}$, obtemos o **Teorema de Wilson**:

$$(p-1)! \equiv -1 \pmod{p}.$$

- $a_{p-1} = -(1+2+\cdots+(p-1)) = -\frac{p(p-1)}{2}$. Como $p \mid \frac{p(p-1)}{2}$ para $p > 2$, temos:

$$a_{p-1} \equiv 0 \pmod{p}.$$

- De modo geral, $a_i \equiv 0 \pmod{p}$ para todo $2 \leq i \leq p-1$.

Teorema 57 (Teorema de Wolstenholme)**.** *Para todo primo $p \geq 5$, o coeficiente a_2 satisfaz:*

$$a_2 \equiv 0 \pmod{p^2}.$$

Ideia da Demonstração. Avaliando o polinômio $f(x)$ em $x = p$:

$$f(p) = p(p-1)(p-2)\ldots(p-(p-1)) = p^p + a_{p-1}p^{p-1} + \cdots + a_2p^2 + a_1p.$$

Como $f(p) = p!$, podemos analisar a expansão termo a termo em potências de p para deduzir que os termos de menor ordem requerem $a_2 \equiv 0 \pmod{p^2}$. □

2.12 Exercícios

Congruências e sistemas de restos (Seção 2.1 de [NZM91])

45. (NZM, 2.1.11) Encontre o menor inteiro positivo x tal que $13 \mid (x^2+1)$.

46. (NZM, 2.1.12) Prove que 19 não é divisor de $4n^2+4$ para nenhum inteiro n.

47. (NZM, 2.1.17) Mostre que $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$.

48. (NZM, 2.1.29) Qual é o último dígito da representação decimal usual de 2^{400}?

49. (NZM, 2.1.30) Quais são os dois últimos dígitos da representação decimal usual de 3^{400}?

50. (NZM, 2.1.33) Mostre que $1^2, 2^2, \ldots, m^2$ não é um sistema completo de restos módulo m se $m > 2$.

51. (NZM, 2.1.43) Se p é um primo ímpar, prove que:

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

e

$$2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

52. (NZM, 2.1.44) Mostre que se p é primo, então $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ para $0 \leq k \leq p-1$.

53. (NZM, 2.1.48) Se $r_1, r_2, \ldots, r_p$ e $r'_1, r'_2, \ldots, r'_p$ são dois sistemas completos de restos quaisquer módulo um primo $p > 2$, prove que o conjunto $r_1r'_1, r_2r'_2, \ldots, r_pr'_p$ não pode ser um sistema completo de restos módulo p.

54. (NZM, 2.1.49) Se p é qualquer primo diferente de 2 e 5, prove que p divide infinitos dos inteiros 9, 99, 999, 9999, $\cdots$. Se p é qualquer primo diferente de 2 e 5, prove que p divide infinitos dos inteiros $1, 11, 111, 1111, \ldots$.

Soluções de congruências (Seção 2.2 de [NZM91])

55. (NZM, 2.2.1) Se $f(x) \equiv 0 \pmod{p}$ tem exatamente j soluções, com p primo, e $g(x) \equiv 0 \pmod{p}$ não tem solução, prove que $f(x)g(x) \equiv 0 \pmod{p}$ tem exatamente j soluções.

56. (NZM, 2.2.2) Denotando por $N(k)$ o número de soluções de $f(x) \equiv k \pmod{m}$, prove que $\sum_{k=1}^{m} N(k) = m$.

57. (NZM, 2.2.3) Se uma congruência polinomial $f(x) \equiv 0 \pmod{m}$ tem m soluções, prove que qualquer inteiro é uma solução.

58. (NZM, 2.2.4) O fato de que o produto de quaisquer três inteiros consecutivos é divisível por 3 leva à congruência identidade $x(x+1)(x+2) \equiv 0 \pmod{3}$. Generalize isso e escreva uma congruência identidade módulo m.

59. (NZM, 2.2.5) Encontre todas as soluções das congruências
(a) $20x \equiv 4 \pmod{30}$;
(b) $20x \equiv 30 \pmod{4}$;
(c) $353x \equiv 254 \pmod{400}$;
(d) $57x \equiv 87 \pmod{105}$;
(e) $64x \equiv 83 \pmod{105}$:
(f) $589x \equiv 209 \pmod{817}$;
(g) $49x \equiv 5000 \pmod{999}$.

60. (NZM, 2.2.6) Quantas soluções existem para cada uma das seguintes congruências:

(a) $15x \equiv 25 \pmod{35}$;

(b) $15x \equiv 24 \pmod{35}$;

(c) $15x \equiv 0 \pmod{35}$?

61. (NZM, 2.2.7) Se a é escolhido ao acaso entre $1, 2, 3, \ldots, 14$, e b é escolhido ao acaso entre $1, 2, 3, \ldots, 15$, qual é a probabilidade de que $ax \equiv b \pmod{15}$ tenha pelo menos uma solução? Exatamente uma solução?

62. (NZM, 2.2.8) Mostre que se p é um primo ímpar, então a congruência $x^2 \equiv 1 \pmod{p^\alpha}$ tem apenas as duas soluções $x \equiv 1, x \equiv -1 \pmod{p^\alpha}$.

63. (NZM, 2.2.9) Mostre que a congruência $x^2 \equiv 1 \pmod{2^\alpha}$ tem uma solução quando $\alpha = 1$, duas soluções quando $\alpha = 2$, e precisamente as quatro soluções $1, 2^{\alpha-1} - 1, 2^{\alpha-1} + 1, -1$ quando $\alpha \geq 3$.

64. (NZM, 2.2.10) Mostre que se p é um primo ímpar, então o número de soluções (pares ordenados) da congruência $x^2 - y^2 \equiv a \pmod{p}$ é $p - 1$, a menos que $a \equiv 0 \pmod{p}$, caso em que o número de soluções é $2p - 1$.

65. (NZM, 2.2.11) Suponha $(a, m) = 1$, e denote por x_1 uma solução de $ax \equiv 1 \pmod{m}$. Para $s = 1, 2, \ldots,$ seja $x_s = 1/a - (1/a)(1 - ax_1)^s$. Prove que x_s é um inteiro e que é uma solução de $ax \equiv 1 \pmod{m^s}$.

66. (NZM, 2.2.12) Suponha que $(a, m) = 1$. Se $a = \pm 1$, a solução de $ax \equiv 1 \pmod{m^s}$ é obviamente $x \equiv a \pmod{m^s}$. Se $a = \pm 2$, então m é ímpar e $x \equiv \frac{1}{2}(1 - m^s)\frac{1}{2}a \pmod{m^s}$ é a solução de $ax \equiv 1 \pmod{m^s}$. Para todos os outros a, use o Exercício 65 para mostrar que a solução de $ax \equiv 1 \pmod{m^s}$ é $x \equiv k \pmod{m^s}$, onde k é o inteiro mais próximo de $-(1/a)(1 - ax_1)^s$.

67. (NZM, 2.2.13) Resolva $3x \equiv 1 \pmod{125}$ pelo Exercício 66, tomando $x_1 = 2$.

68. (NZM, 2.2.14) Mostre que $\binom{p^\alpha}{k} \equiv 0 \pmod{p}$ para $0 < k < p^\alpha$.

69. (NZM, 2.2.15) Mostre que $\binom{p^\alpha - 1}{k} \equiv (-1)^k \pmod{p}$ para $0 \leq k \leq p^\alpha - 1$.

70. (NZM, 2.2.16) Mostre que se r é um inteiro não negativo, então todos os coeficientes do polinômio $(1 + x)^{2^r} - \left(1 + x^{2^r}\right)$ são pares. Escreva um inteiro positivo n em binário, $n = \sum_{r \in \mathscr{R}} 2^r$. Mostre que todos os coeficientes do polinômio $(1 + x)^n - \prod_{r \in \mathscr{R}} \left(1 + x^{2^r}\right)$ são pares. Escreva $k = \sum_{s \in \mathscr{S}} 2^s$ em binário. Mostre que $\binom{n}{k}$ é ímpar se, e somente se, $\mathscr{S} \subseteq \mathscr{R}$. Conclua que, dado n, $\binom{n}{k}$ é ímpar para precisamente $2^{w(n)}$ valores de k, onde $w(n)$, chamado peso binário de n, é o número de algarismos 1 na expansão binária de n. Em símbolos, $w(n) = \text{card}(\mathscr{R})$.
Nota: Este é um caso particular de um resultado de E. Lucas, provado em 1891. Veja N. J. Fine, "Binomial coefficients modulo a prime," Amer. Math. Monthly, 54 (1947), 589-592.

71. (NZM, 2.2.17) Sejam os números c_i definidos pela identidade de séries de potências

$$\left(1 + x + \cdots + x^{p-1}\right)/(1 - x)^{p-1} = 1 + c_1 x + c_2 x^2 + \cdots .$$

Mostre que $c_i \equiv 0 \pmod{p}$ para todo $i \geq 1$.

Teorema Chinês dos Restos e função ϕ (Seção 2.3 de [NZM91])

72. (NZM, 2.3.4) Encontre todos os inteiros que deixam restos 1, 2, 3 quando divididos por 3, 4, 5, respectivamente.

73. (NZM, 2.3.5) Resolva o Exemplo 2 de [NZM91, Seção 2.3] usando a técnica que foi aplicada ao Exemplo 4 da mesma seção.

74. (NZM, 2.3.6) Resolva o Exemplo 1 de [NZM91, Seção 2.3] pelo método usado na segunda solução do Exemplo 3 da mesma seção.

75. (NZM, 2.3.7) Determine se as congruências $5x \equiv 1 \pmod{6}, 4x \equiv 13 \pmod{15}$ têm uma solução comum e, caso exista, encontre-a.

76. (NZM, 2.3.8) Encontre o menor inteiro positivo que deixa restos 1, 2, 3, 4 e 5 quando dividido por 3, 5, 7, 9 e 11, respectivamente.

77. (NZM, 2.3.9) Para quais valores de n o número $\phi(n)$ é ímpar?

78. (NZM, 2.3.10) Encontre a quantidade de inteiros positivos ≤ 3600 que são primos com 3600.

79. (NZM, 2.3.11) Encontre a quantidade de inteiros positivos ≤ 3600 que têm um fator maior que 1 em comum com 3600.

80. (NZM, 2.3.12) Encontre a quantidade de inteiros positivos ≤ 7200 que são primos com 3600.

81. (NZM, 2.3.13) Encontre a quantidade de inteiros positivos ≤ 25200 que são primos com 3600. (Observe que $25200 = 7 \times 3600$.)

82. (NZM, 2.3.14) Resolva as congruências:

$$\begin{aligned} x^3 + 2x - 3 &\equiv 0 \pmod 9 \\ x^3 + 2x - 3 &\equiv 0 \pmod 5 \\ x^3 + 2x - 3 &\equiv 0 \pmod{45}. \end{aligned}$$

83. (NZM, 2.3.15) Resolva a congruência $x^3 + 4x + 8 \equiv 0 \pmod{15}$.

84. (NZM, 2.3.16) Resolva a congruência $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{503}$ observando que 503 é primo e que o polinômio se fatora como $(x-1)(x-3)(x-5)$.

85. (NZM, 2.3.17) Resolva a congruência $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$.

86. (NZM, 2.3.18) Dado qualquer inteiro positivo k, prove que existem k inteiros consecutivos, cada um divisível por um quadrado > 1.

87. (NZM, 2.3.19) Sejam $m_1, m_2, \ldots, m_r$ primos entre si dois a dois. Supondo que cada uma das congruências $b_i x \equiv a_i \pmod{m_i}, i = 1, 2, \ldots, r$, seja solúvel, prove que as congruências têm uma solução simultânea.

88. (NZM, 2.3.20) Sejam m_1 e m_2 inteiros positivos arbitrários, e sejam a_1 e a_2 inteiros arbitrários. Mostre que existe uma solução simultânea das congruências $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ se, e somente se, $a_1 \equiv a_2 \pmod{g}$, onde $g = (m_1, m_2)$. Mostre que, se essa condição for satisfeita, então a solução é única módulo $[m_1, m_2]$.

89. (NZM, 2.3.21) Seja p um número primo, e suponha que $m_j = p^{\alpha_j}$ no sistema $x \equiv a_j \pmod{m_j}$, $j = 1, 2, \ldots, r$, onde $1 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_r$. Mostre que o sistema tem uma solução simultânea se, e somente se, $a_i \equiv a_r \pmod{p^{\alpha_i}}$ para $i = 1, 2, \ldots, r$.

90. (NZM, 2.3.22) Sejam os m_j como no problema anterior. Mostre que o sistema $x \equiv a_j \pmod{m_j}$, $j = 1, 2, \ldots, r$, tem uma solução simultânea se, e somente se, $a_i \equiv a_j \pmod{p^{\alpha_i}}$ para todos os pares de índices i, j com $1 \leq i < j \leq r$.

91. (NZM, 2.3.23) Sejam os m_j inteiros positivos arbitrários no sistema $x \equiv a_j \pmod{m_j}$, $j = 1, 2, \ldots, r$. Mostre que existe uma solução simultânea deste sistema se, e somente se, $a_i \equiv a_j \pmod{(m_i, m_j)}$ para todos os pares de índices i, j com $1 \leq i < j \leq r$.

92. (NZM, 2.3.24) Suponha que $m_1, m_2, \ldots, m_r$ sejam inteiros positivos primos entre si dois a dois. Para cada j, denote por $\mathscr{C}(m_j)$ um sistema completo de restos módulo m_j. Mostre que os números $c_1 + c_2 m_1 + c_3 m_1 m_2 + \cdots + c_r m_1 m_2 \cdots m_{r-1}, c_j \in \mathscr{C}(m_j)$, formam um sistema completo de restos módulo $m = m_1 m_2 \cdots m_r$.

93. (NZM, 2.3.25) Se m e k são inteiros positivos, prove que a quantidade de inteiros positivos $\leq mk$ que são primos com m é $k\phi(m)$.

94. (NZM, 2.3.26) Mostre que $\phi(nm) = n\phi(m)$ se todo primo que divide n também divide m.

95. (NZM, 2.3.27) Se P denota o produto dos primos comuns a m e n, prove que $\phi(mn) = P\phi(m)\phi(n)/\phi(P)$. Consequentemente, se $(m, n) > 1$, prove que $\phi(mn) > \phi(m)\phi(n)$.

96. (NZM, 2.3.28) Se $\phi(m) = \phi(mn)$ e $n > 1$, prove que $n = 2$ e m é ímpar.

97. (NZM, 2.3.29) Caracterize o conjunto dos inteiros positivos n que satisfazem $\phi(2n) = \phi(n)$.

98. (NZM, 2.3.30) Caracterize o conjunto dos inteiros positivos que satisfazem $\phi(2n) > \phi(n)$.

99. (NZM, 2.3.31) Prove que existem infinitos inteiros n tais que $3 \nmid \phi(n)$.

100. (NZM, 2.3.32) Encontre todas as soluções x de $\phi(x) = 24$.

101. (NZM, 2.3.33) Encontre o menor inteiro positivo n tal que $\phi(x) = n$ não tenha solução; tenha exatamente duas soluções; exatamente três soluções; exatamente quatro soluções. (Conjectura-se que não existe inteiro n tal que $\phi(x) = n$ tenha exatamente uma solução, mas este é um problema em aberto.)

102. (NZM, 2.3.34) Prove que a equação $\phi(x) = 14$ não tem solução e que 14 é o menor inteiro positivo par com essa propriedade. Além de 14, qual é o próximo menor inteiro positivo par n tal que $\phi(x) = n$ não tem solução?

103. (NZM, 2.3.35) Se n tem k fatores primos ímpares distintos, prove que $2^k \mid \phi(n)$.

104. (NZM, 2.3.36) Quais são os dois últimos dígitos, isto é, os dígitos das dezenas e das unidades, de 2^{1000}? E de 3^{1000}?

105. (NZM, 2.3.37) Seja $a_1 = 3, a_{i+1} = 3^{a_i}$. Descreva esta sequência $\pmod{100}$.

106. (NZM, 2.3.38) Sejam $(a, b) = 1$ e $c > 0$. Prove que existe um inteiro x tal que $(a + bx, c) = 1$.

107. (NZM, 2.3.39) Prove que, para um inteiro fixo n, a equação $\phi(x) = n$ tem apenas um número finito de soluções.

Congruências módulo potência de primo (Seção 2.6 de [NZM91])

108. (NZM, 2.6.1) Resolva a congruência $x^2 + x + 7 \equiv 0 \pmod{27}$ usando o método de completar o quadrado da álgebra elementar, assim: $4x^2 + 4x + 28 = (2x + 1)^2 + 27$. Resolva esta congruência $\pmod{81}$ pelo mesmo método.

109. (NZM, 2.6.2) Resolva $x^5 + x^4 + 1 \equiv 0 \pmod{3^4}$.

110. (NZM, 2.6.3) Resolva $x^3 + x + 57 \equiv 0 \pmod{5^3}$.

111. (NZM, 2.6.4) Resolva $x^2 + 5x + 24 \equiv 0 \pmod{36}$.

112. (NZM, 2.6.5) Resolva $x^3 + 10x^2 + x + 3 \equiv 0 \pmod{3^3}$.

113. (NZM, 2.6.6) Resolva $x^3 + x^2 - 4 \equiv 0 \pmod{7^3}$.

114. (NZM, 2.6.7) Resolva $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$.

115. (NZM, 2.6.8) Aplique a teoria desta seção para resolver $1000x \equiv 1 \pmod{101^3}$, usando uma calculadora.

116. (NZM, 2.6.9) Suponha que $f(a) \equiv 0 \pmod{p^j}$ e que $f'(a) \not\equiv 0 \pmod{p}$. Seja $\overline{f'(a)}$ um inteiro escolhido de modo que $f'(a)\overline{f'(a)} \equiv 1 \pmod{p^{2j}}$, e ponha $b = a - f(a)\overline{f'(a)}$. Mostre que $f(b) \equiv 0 \pmod{p^{2j}}$.

117. (NZM, 2.6.10) Seja p um primo ímpar, e suponha que $a \not\equiv 0 \pmod{p}$. Mostre que se a congruência $x^2 \equiv a \pmod{p^j}$ tem solução quando $j = 1$, então tem solução para todo j.

118. (NZM, 2.6.11) Seja $f(x)$ um polinômio com coeficientes inteiros nas n variáveis $x_1, x_2, \ldots, x_n$. Suponha que $f(\mathbf{a}) \equiv 0 \pmod{p}$, onde $\mathbf{a} = (a_1, a_2, \ldots, a_n)$, e que $\frac{\partial}{\partial x_i} f(\mathbf{a}) \not\equiv 0 \pmod{p}$ para pelo menos um i. Mostre que a congruência $f(x) \equiv 0 \pmod{p^j}$ tem solução para todo j.

Congruências módulo primo (Seção 2.7 de [NZM91])

119. (NZM, 2.7.1) Reduza as seguintes congruências a congruências equivalentes de grau ≤ 6:

(a) $x^{11} + x^8 + 5 \equiv 0 \pmod{7}$;

(b) $x^{20} + x^{13} + x^7 + x \equiv 2 \pmod{7}$;

(c) $x^{15} - x^{10} + 4x - 3 \equiv 0 \pmod{7}$.

120. (NZM, 2.7.2) Prove que $2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod{7}$ tem três soluções usando o Teorema 55.

121. (NZM, 2.7.3) Prove que $x^{14} + 12x^2 \equiv 0 \pmod{13}$ tem 13 soluções e, portanto, é uma congruência identidade.

122. (NZM, 2.7.4) Prove que se $f(x) \equiv 0 \pmod{p}$ tem j soluções $x \equiv a_1, x \equiv a_2, \ldots, x \equiv a_j \pmod{p}$, então existe um polinômio $q(x)$ tal que

$$f(x) \equiv (x - a_1)(x - a_2) \cdots (x - a_j)\, q(x) \pmod{p}.$$

123. (NZM, 2.7.5) Com as hipóteses e a notação do problema anterior, prove que se o grau de $f(x)$ é j, então $q(x)$ é uma constante e pode ser tomado como o coeficiente líder de $f(x)$.

124. (NZM, 2.7.6) Seja m composto. Prove que o Teorema 51 é falso se "mod$p$" for substituído por "mod$m$".

125. (NZM, 2.7.7) Mostre que, se o número primo p em [NZM91, Teorema 2.28] for substituído por um número composto m, o enunciado se torna falso.

126. (NZM, 2.7.8) Explique por que a demonstração da congruência de Wolstenholme falha quando $p = 3$.

127. (NZM, 2.7.9) Para $p = 5$, calcule os valores dos números $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ em [NZM91, equação (2.7)].

128. (NZM, 2.7.10) Escreva $1/1 + 1/2 + \cdots + 1/(p-1) = a/b$ com $(a, b) = 1$. Mostre que $p^2 \mid a$ se $p \geq 5$.

129. (NZM, 2.7.11) Seja p um primo, $p \geq 5$, e suponha que os números σ_j sejam como em [NZM91, equação (2.7)]. Mostre que $\sigma_{p-2} \equiv p\sigma_{p-3} \pmod{p^3}$.

130. (NZM, 2.7.12) Mostre que se $p \geq 5$ e m é um inteiro positivo, então $\binom{mp-1}{p-1} \equiv 1 \pmod{p^3}$.

131. (NZM, 2.7.13) Mostre que se $p \geq 5$, então $(mp)! \equiv m!p!^m \pmod{p^{m+3}}$.

132. (NZM, 2.7.14) Suponha que p seja um primo ímpar, e escreva $1/1 - 1/2 + 1/3 - \cdots - 1/(p-1) = a/(p-1)!$. Mostre que $a \equiv (2 - 2^p)/p \pmod{p}$.

Capítulo 3

Raízes Primitivas

3.1 Ordem de um Elemento

Vimos no Corolário 56 que se $d \mid (p-1)$, então a congruência

$$x^d \equiv 1 \pmod{p}$$

tem exatamente d soluções módulo p.

Exemplo ($p = 11$)**.**

- $1^k \equiv 1 \pmod{11}$, $\forall k$.
- Potências de 2 módulo 11:

  $$1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, 2, \ldots$$

  (10 valores distintos mod 11. Todo resíduo não nulo aparece).
- Potências de 3 módulo 11:

  $$1, 3, 9, 5, 4, 1, 3, \ldots \quad \text{(5 valores distintos)}.$$

- Potências de 4 módulo 11:

  $$1, 4, 5, 9, 3, 1, 4, \ldots \quad \text{(5 valores distintos)}.$$

- Potências de 5 módulo 11:

  $$1, 5, 3, 4, 9, 1, 5, \ldots \quad \text{(5 valores distintos)}.$$

- Potências de 6 módulo 11:

  $$1, 6, 3, 7, 9, 10, 5, 8, 4, 2, 1, 6, \ldots \quad \text{(10 valores distintos)}.$$

- Potências de 7 módulo 11:

  $$1, 7, 5, 2, 3, 10, 4, 6, 9, 8, 1, 7, \ldots \quad \text{(10 valores distintos)}.$$

- Potências de 8 módulo 11:

$$1, 8, 9, 6, 4, 10, 3, 2, 5, 7, 1, 8, \ldots \quad \text{(10 valores distintos)}.$$

- Potências de 9 módulo 11:

$$1, 9, 4, 3, 5, 1, 9, \ldots \quad \text{(5 valores distintos)}.$$

- Potências de 10 módulo 11:

$$1, 10, 1, 10, \ldots \quad \text{(2 valores distintos)}.$$

Sobre o Corolário 56: $p - 1 = 10$, divisores $d \in \{1, 2, 5, 10\}$.

- $x^1 \equiv 1 \pmod{11}$ tem 1 solução: $\{1\}$.
- $x^2 \equiv 1 \pmod{11}$ tem 2 soluções: $\{1, 10\}$.
- $x^5 \equiv 1 \pmod{11}$ tem 5 soluções: $\{1, 3, 4, 5, 9\}$.
- $x^{10} \equiv 1 \pmod{11}$ tem 10 soluções (Teorema de Fermat).

Definição. Sejam a, m inteiros tais que $m > 0$ e $\text{mdc}(a, m) = 1$. Seja h o menor expoente positivo tal que $a^h \equiv 1 \pmod{m}$. Dizemos que h é a *ordem* de a módulo m.

$$\text{Notação: } h = \text{ord}_m(a).$$

Observação. A existência de h segue do Princípio da Boa Ordenação, visto que o conjunto $\{k > 0 : a^k \equiv 1 \pmod{m}\}$ é não vazio pelo Teorema de Euler.

Lema 58. *Se* $\text{ord}_m(a) = h$*, então* $a^k \equiv 1 \pmod{m} \iff h \mid k$.

Demonstração. ($\Leftarrow$) Se $h \mid k$, escrevendo $k = hq$, temos:

$$a^k = (a^h)^q \equiv 1^q \equiv 1 \pmod{m}$$

($\Rightarrow$) Pelo algoritmo da divisão, escreva $k = hq + r$, com $0 \leq r < h$. Então:

$$a^k \equiv 1 \pmod{m} \iff (a^h)^q \cdot a^r \equiv 1 \pmod{m} \implies a^r \equiv 1 \pmod{m}.$$

Como $r < h$ e h é o menor inteiro positivo com essa propriedade, devemos ter $r = 0$. Portanto, $h \mid k$. □

Corolário 59. *Para* $m > 0$ *e* $\text{mdc}(a, m) = 1$*, temos* $\text{ord}_m(a) \mid \phi(m)$.

Lema 60. *Se* $\text{ord}_m(a) = h$*, então*

$$\text{ord}_m(a^k) = \frac{h}{\text{mdc}(h, k)}.$$

Demonstração. $\text{ord}_m(a^k)$ é o menor elemento positivo do conjunto $\{t > 0 : (a^k)^t \equiv 1 \pmod{m}\}$.

$$(a^k)^t \equiv 1 \pmod{m} \iff a^{kt} \equiv 1 \pmod{m} \iff h \mid kt \iff \frac{h}{\text{mdc}(h, k)} \,\Big|\, t.$$

Assim, $\text{ord}_m(a^k)$ é o menor inteiro positivo múltiplo de $\frac{h}{\text{mdc}(h,k)}$, ou seja, é igual a $\frac{h}{\text{mdc}(h,k)}$. □

Voltando ao exemplo com $m = 11$, temos

- $\text{ord}_{11}(2) = 10$.
- $\text{ord}_{11}(4) = \text{ord}_{11}(2^2) = \frac{10}{\text{mdc}(10,2)} = 5$
- $\text{ord}_{11}(8) = \text{ord}_{11}(2^3) = \frac{10}{\text{mdc}(10,3)} = 10$

Lema 61. *Se* $\text{ord}_m(a) = h$, $\text{ord}_m(b) = k$ *e* $\text{mdc}(h,k) = 1$, *então* $\text{ord}_m(ab) = hk$.

Demonstração. Primeiramente, note que:

$$(ab)^{hk} = a^{hk} \cdot b^{hk} = (a^h)^k (b^k)^h \equiv 1^k \cdot 1^h \equiv 1 \pmod{m}.$$

Seja agora $t > 0$ tal que $(ab)^t \equiv 1 \pmod{m}$. Então:

$$a^t b^t \equiv 1 \pmod{m} \implies (a^t b^t)^h \equiv 1 \pmod{m} \implies b^{ht} \equiv 1 \pmod{m}.$$

Como $\text{ord}_m(b) = k$, temos $k \mid ht$. Sendo $\text{mdc}(h,k) = 1$, segue que $k \mid t$. De maneira completamente análoga, $h \mid t$. Como $\text{mdc}(h,k) = 1$, segue que $hk \mid t$. Em particular, $t \geq hk \implies hk$ é o menor expoente positivo. Logo, $\text{ord}_m(ab) = hk$. □

Exercício 133. Prove ou dê um contraexemplo: se $\text{ord}_m(a) = h$ e $\text{ord}_m(b) = k$, então $\text{ord}_m(ab) = \frac{hk}{\text{mdc}(h,k)} = \text{mmc}(h,k)$.

3.2 Raízes Primitivas

Definição. Dizemos que a é uma **raiz primitiva** módulo m se $\text{ord}_m(a) = \phi(m)$.

No exemplo com $m = 11$, obtemos que $2, 6, 7, 8$ são raízes primitivas módulo 11.

Teorema 62. *Seja* p *primo. Se* $d \mid (p-1)$, *então existem exatamente* $\phi(d)$ *resíduos módulo* p *cuja ordem é igual a* d.

Corolário 63. *Existem* $\phi(p-1)$ *raízes primitivas módulo* p.

Lema 64. *Seja* n *um inteiro positivo. Então*

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

Demonstração. Seja $X = \{1, 2, \ldots, n\}$, de modo que $\#X = n$. Para cada divisor d de n, seja X_d o subconjunto de X definido por:

$$X_d = \{k \in X : \text{mdc}(k,n) = d\}.$$

Claramente, os conjuntos X_d são disjuntos e $X = \bigcup_{d \mid n} X_d$. Vamos mostrar que $\#X_d = \phi(n/d)$.

Se $k \in X_d$, então $d \mid k$ e $\text{mdc}(k,n) = d \iff \text{mdc}\left(\frac{k}{d}, \frac{n}{d}\right) = 1$. Ou seja, $k = dk'$ onde $k' \in \{1, \ldots, n/d\}$ e $\text{mdc}(k', n/d) = 1$. Reciprocamente, todo número da forma dk' com $1 \leq k' \leq n/d$ e $\text{mdc}(k', n/d) = 1$ pertence a X_d. Logo, $\#X_d = \phi(n/d)$.

Portanto:

$$n = \#X = \sum_{d \mid n} \#X_d = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$

visto que $\frac{n}{d}$ percorre os mesmos divisores de n em ordem inversa. □

Demonstração do Teorema 62. A prova é por indução em $d \mid (p-1)$.

- Para $d = 1$: A única solução de $\text{ord}_p(a) = 1$ é $a \equiv 1 \pmod{p}$, totalizando $1 = \phi(1)$ solução.
- Assuma verdadeiro para todos os divisores $e < d$.

Já sabemos que a congruência $x^d \equiv 1 \pmod{p}$ possui exatamente d soluções módulo p. Além disso, se $a^d \equiv 1 \pmod{p}$, então $\text{ord}_p(a) = e$ para algum divisor e de d. Assim:

$$d = \#\{a : a^d \equiv 1 \pmod{p}\} = \sum_{e \mid d} \#\{a : \text{ord}_p(a) = e\}.$$

Isolando o termo para $e = d$:

$$\#\{a : \text{ord}_p(a) = d\} = d - \sum_{\substack{e \mid d \\ e < d}} \#\{a : \text{ord}_p(a) = e\}.$$

Pela hipótese de indução, para $e < d$, o número de elementos de ordem e é $\phi(e)$. Logo:

$$\#\{a : \text{ord}_p(a) = d\} = d - \sum_{\substack{e \mid d \\ e < d}} \phi(e) = \phi(d)$$

pelo Lema anterior. □

Exercício 134. Calcule $\text{ord}_{13}(a)$ para $a = 1, 2, \ldots, 12$.

Sabemos que se $d \mid (p-1)$, existem exatamente $\phi(d)$ resíduos incongruentes módulo p que possuem ordem d. Em particular, para $d = p-1$, existem exatamente $\phi(p-1)$ resíduos com ordem $p-1$, chamados de **raízes primitivas** módulo p.

3.3 Resíduos Potência n-ésima

Definição. Seja m um inteiro positivo e a tal que $\text{mdc}(a, m) = 1$. Dizemos que a é um *resíduo potência n-ésima módulo m* se a congruência

$$x^n \equiv a \pmod{m}$$

admite solução.

- Se $n = 2$, a é chamado de *resíduo quadrático* módulo m.
- Se $n = 3$, a é chamado de *resíduo cúbico* módulo m.

Exemplo.
- -1 é resíduo quadrático módulo 2 ($1^2 \equiv -1 \pmod{2}$).
- -1 sempre é um resíduo cúbico para qualquer m, pois $(-1)^3 = -1 \equiv -1 \pmod{m}$.

Teorema 65. *Seja p um número primo e a um inteiro tal que* $\text{mdc}(a, p) = 1$. *A congruência*

$$x^n \equiv a \pmod{p}$$

possui exatamente $\text{mdc}(n, p-1)$ *soluções incongruentes se*

$$a^{\frac{p-1}{\text{mdc}(n,p-1)}} \equiv 1 \pmod{p}$$

e não possui nenhuma solução caso contrário.

Demonstração. Seja g uma raiz primitiva módulo p. Se $x^n \equiv a \pmod{p}$, então $p \nmid x$, pois $p \nmid a$. Como $\text{mdc}(a,p) = 1$ e $\text{mdc}(x,p) = 1$, podemos expressar a e x como potências de g:

$$a \equiv g^k \pmod{p} \quad \text{e} \quad x \equiv g^l \pmod{p}.$$

Substituindo na congruência original:

$$(g^l)^n \equiv g^k \pmod{p} \iff g^{ln} \equiv g^k \pmod{p}.$$

Como g é uma raiz primitiva módulo p, a igualdade de potências de g módulo p é equivalente à congruência linear nos expoentes módulo $p-1$:

$$n \cdot l \equiv k \pmod{p-1}.$$

Seja $d = \text{mdc}(n, p-1)$. A congruência linear acima tem solução em l se, e somente se, $d \mid k$.

Existência de solução: Se $d \mid k$, podemos escrever $k = d \cdot t$ para algum $t \in \mathbb{Z}$. Então:

$$a^{\frac{p-1}{d}} \equiv (g^k)^{\frac{p-1}{d}} \equiv (g^{d\cdot t})^{\frac{p-1}{d}} \equiv (g^{p-1})^t \equiv 1^t \equiv 1 \pmod{p}.$$

Reciprocamente, se $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, temos $(g^k)^{\frac{p-1}{d}} \equiv g^{\frac{k(p-1)}{d}} \equiv 1 \pmod{p}$. Como $\text{ord}_p(g) = p-1$, isso implica que $(p-1) \mid \frac{k(p-1)}{d}$, logo $d \mid k$.

Número de soluções: Quando $d \mid k$, a congruência $n \cdot l \equiv k \pmod{p-1}$ possui exatamente $d = \text{mdc}(n, p-1)$ soluções incongruentes para $l \pmod{p-1}$. Como cada valor de $l \pmod{p-1}$ produz um valor distinto para $x \equiv g^l \pmod{p}$, a congruência $x^n \equiv a \pmod{p}$ possui exatamente $\text{mdc}(n, p-1)$ soluções. □

Corolário 66 (Critério de Euler)**.** *Se p é um primo ímpar e $\text{mdc}(a,p) = 1$, então a é um resíduo quadrático módulo p se, e somente se:*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Se a for resíduo quadrático, a congruência $x^2 \equiv a \pmod{p}$ possui exatamente 2 soluções; caso contrário, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ e a congruência $x^2 \equiv a \pmod{p}$ não possui soluções.

Definição. Se $\text{mdc}(x,m) = 1$, x^{-1} é o inverso multiplicativo de x e $x^{-k} := (x^{-1})^k$.

Outra maneira de definir: dado $k > 0$, $x^{-k} := x^{\ell\phi(m)-k}$ para algum ℓ suficientemente grande

Na prática temos três opções:

- Opção 1: Resolver o seguinte exercício: mostrar que essas definições coincidem e que todas as propriedades de exponenciação continuam válidas, por exemplo:

$$x^{a+b} \equiv x^a \cdot x^b \pmod{m}, \quad (x^a)^b \equiv x^{ab} \pmod{m}.$$

- Opção 2: Confiar no professor e acreditar que tudo dá certo.
- Opção 3: Sempre manipular as potências para não ter expoentes negativos.

Observação. Expoente negativo só faz sentido quando $\text{mdc}(a,m) = 1$.

Filosoficamente,

$$(g^l)^n = x^n \equiv a = g^k \pmod{p} \iff nl \equiv k \pmod{p-1}$$

é equivalente a

$$x^n = a \iff n \log x = \log a.$$

3.3.1 Exemplo: $x^6 \equiv 5 \pmod{11}$

Exemplo. Resolver a congruência $x^6 \equiv 5 \pmod{11}$.

Passo 1: Verificar a existência de soluções. Temos $n = 6$, $p = 11$, $a = 5$. O divisor comum é $d = \text{mdc}(6, 11-1) = \text{mdc}(6, 10) = 2$. Testamos a condição de solubilidade $a^{\frac{p-1}{d}} \equiv 5^5 \pmod{11}$:

$$\begin{aligned} 5^1 &\equiv 5 \pmod{11} \\ 5^2 &\equiv 25 \equiv 3 \pmod{11} \\ 5^3 &\equiv 15 \equiv 4 \pmod{11} \\ 5^4 &\equiv 20 \equiv 9 \pmod{11} \\ 5^5 &\equiv 45 \equiv 1 \pmod{11}. \end{aligned}$$

Como $5^5 \equiv 1 \pmod{11}$, a congruência tem solução e possui exatamente $\text{mdc}(6, 10) = 2$ soluções incongruentes módulo 11.

Passo 2: Encontrar as soluções usando uma raiz primitiva. Tomando $g = 2$ como raiz primitiva módulo 11:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16 \equiv 5 \pmod{11}.$$

Logo, $5 \equiv 2^4 \pmod{11}$. Escrevendo $x \equiv 2^l \pmod{11}$:

$$(2^l)^6 \equiv 2^4 \pmod{11} \iff 2^{6l} \equiv 2^4 \pmod{11} \iff 6l \equiv 4 \pmod{10}.$$

Simplificando a congruência linear dividindo por $\text{mdc}(6, 10) = 2$:

$$3l \equiv 2 \pmod{5} \iff l \equiv 4 \pmod{5}.$$

Os valores de $l \pmod{10}$ são $l = 4$ e $l = 4 + 5 = 9$.

Passo 3: Obter os valores de x.

- Para $l = 4$: $x \equiv 2^4 = 16 \equiv 5 \pmod{11}$
- Para $l = 9$: $x \equiv 2^9 = 512 \equiv 6 \pmod{11}$

As soluções da congruência são $x \equiv 5 \pmod{11}$ e $x \equiv 6 \pmod{11}$.

3.4 Cálculo da Ordem de Elementos

Para determinar a ordem de todos os elementos módulo um primo p (por exemplo, $p = 31$):

1. Encontra-se uma raiz primitiva g módulo p.
2. Expressam-se todos os elementos como potências de g: $a \equiv g^k \pmod{p}$.
3. Utiliza-se a fórmula para a ordem de potências:

$$\text{ord}_p(a) = \text{ord}_p(g^k) = \frac{\text{ord}_p(g)}{\text{mdc}(k, \text{ord}_p(g))} = \frac{p-1}{\text{mdc}(k, p-1)}.$$

Já sabemos que se p é um primo ímpar, existem raízes primitivas módulo p. Isto é, existe g tal que $\{g^1, g^2, \ldots, g^{p-1}\}$ é um Sistema Reduzido de Restos (SRR) módulo p; em particular,

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

Mais precisamente, existem exatamente $\phi(\phi(p)) = \phi(p-1)$ raízes primitivas para cada p.

Exemplo ($p = 31$)**.** Quantas raízes primitivas existem?

$$\phi(\phi(31)) = \phi(30) = 8 \quad \text{(Faça a conta!)}$$

$$\operatorname{ord}_{31}(3^k) = \frac{30}{\operatorname{mdc}(k, 30)}$$

$$\operatorname{ord}_{31}(3^k) = 30 \iff \operatorname{mdc}(k, 30) = 1 \implies k \in \{1, 7, 11, 13, 17, 19, 23, 29\}.$$

Assim, $3^1, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}$ são as raízes primitivas módulo 31.
Calculando as potências de 3 módulo 31:

$$\begin{aligned}
3^1 &= 3 \\
3^2 &= 9 \\
3^3 &= 27 \equiv -4 \pmod{31} \\
3^4 &\equiv 19 \pmod{31} \\
3^5 &= 243 \equiv -5 \pmod{31} \\
3^7 &\equiv 17 \pmod{31} \\
3^{11} &\equiv (-5)(-5) \cdot 3 = 75 \equiv 13 \pmod{31} \\
3^{13} &\equiv (-5)(-5)(-4) = -100 \equiv 24 \pmod{31} \\
3^{15} &= (3^5)^3 \equiv (-5)^3 = -125 \equiv -1 \pmod{31} \\
3^{17} &= 3^{15} \cdot 3^2 \equiv -9 \equiv 22 \pmod{31} \\
3^{19} &\equiv 3^{15} \cdot 3^4 \equiv -19 \equiv 12 \pmod{31} \\
3^{23} &\equiv 11 \pmod{31} \\
3^{29} &\equiv 21 \pmod{31}.
\end{aligned}$$

Conclusão: As raízes primitivas módulo 31 são $3, 11, 12, 13, 17, 21, 22, 24$.

3.5 Raízes Primitivas Módulo p^2

Teorema 67. *Seja p um primo. Existem exatamente $\phi(\phi(p^2)) = (p-1)\phi(p-1)$ raízes primitivas módulo p^2.*

Observação. Isto quer dizer que para cada raiz primitiva módulo p, existem $p-1$ raízes primitivas módulo p^2 congruentes a ela módulo p.

Demonstração. Primeiramente observe que se g é raiz primitiva módulo p^2, então g é raiz primitiva módulo p. Caso contrário, teríamos $g^k \equiv 1 \pmod{p}$ para algum $k < p-1$. Vamos mostrar que isto implicaria que $g^{kp} \equiv 1 \pmod{p^2}$. De fato, seja $g^k = 1 + pt$.

$$g^{kp} = (1 + pt)^p = 1 + p \cdot pt + \cdots \equiv 1 \pmod{p^2}.$$

Como $kp < p(p-1) = \phi(p^2)$, isso contradiz o fato de g ser raiz primitiva módulo p^2.

Seja agora g_0 uma raiz primitiva módulo p. Queremos encontrar todas as raízes primitivas módulo p^2 congruentes a g_0 módulo p. Em outras palavras, queremos encontrar g da forma $g = g_0 + pt$ tal que g é raiz primitiva.

Observe que

$$\begin{aligned} g^k \equiv 1 \pmod{p^2} &\implies g^k \equiv 1 \pmod{p} \\ &\implies g_0^k \equiv 1 \pmod{p} \\ &\implies (p-1) \mid k. \end{aligned}$$

Assim, se $g = g_0 + pt$, temos $(p-1) \mid \mathrm{ord}_{p^2}(g)$

Como, pelo Teorema de Euler, $\mathrm{ord}_{p^2}(g) \mid \phi(p^2) = p(p-1)$, temos que $\mathrm{ord}_{p^2}(g) = p-1$ ou $p(p-1)$. Logo, g é raiz primitiva sse $g^{p-1} \not\equiv 1 \pmod{p^2}$.

Escrevendo $g = g_0 + pt$:

$$(g_0 + pt)^{p-1} \equiv g_0^{p-1} + (p-1)g_0^{p-2}pt \pmod{p^2}.$$

Assim, $g^{p-1} \equiv 1 \pmod{p^2} \iff g_0^{p-1} + (p-1)g_0^{p-2}pt \equiv 1 \pmod{p^2}$. Pelo Teorema de Fermat, $p \mid (1 - g_0^{p-1})$, logo:

$$(p-1)g_0^{p-2}t \equiv \frac{1 - g_0^{p-1}}{p} \pmod{p}.$$

A congruência acima tem exatamente 1 solução módulo p.

Ou seja, dentre $\{g_0, g_0 + p, g_0 + 2p, \ldots, g_0 + p(p-1)\}$, um deles terá ordem $p-1$ e os outros $p-1$ terão ordem $p(p-1)$. Ou seja, serão raízes primitivas. Assim o total de raízes primitivas módulo p^2 é $(p-1)\phi(p-1)$. □

Exemplo (Raízes primitivas módulo 25)**.** Módulo 25, temos $\phi(25) = 20$. Todo resto módulo 25 se escreve de modo único como $a + 5b$, com $0 \le a, b \le 4$.

	$a=0$	$a=1$	$a=2$	$a=3$	$a=4$
$b=0$	0	1	2	3	4
$b=1$	5	6	~~7~~	8	9
$b=2$	10	11	12	13	14
$b=3$	15	16	17	18	19
$b=4$	20	21	22	23	24

Seja $x = 2 + 5b$. Já sabemos que 2 é raiz primitiva módulo 5. Se $(2+5b)^k \equiv 1 \pmod{25}$, então $2^k \equiv 1 \pmod{5} \implies 4 \mid k$. Em particular, $4 \mid \mathrm{ord}_{25}(2+5b)$. Por outro lado, pelo Teorema de Euler, $\mathrm{ord}_{25}(2+5b) \mid 20 \implies \mathrm{ord}_{25}(2+5b) = 4$ ou 20.

$$\implies \mathrm{ord}_{25}(2+5b) = 4 \iff (2+5b)^4 \equiv 1 \pmod{25}.$$

Agora $(2+5b)^4 \equiv 16 + 160b \pmod{25}$.

$$16 + 160b \equiv 1 \pmod{25} \iff 10b \equiv 10 \pmod{25} \iff b \equiv 1 \pmod{5}$$

$\implies 7 = 2 + 5(1)$ não é raiz primitiva módulo 25 (sua ordem é 4). Os outros números da forma $2 + 5b$ $(2, 12, 17, 22)$ são raízes primitivas módulo 25.

Exercício 135. Encontre o número da forma $3 + 5b$, com $0 \le b \le 4$, que não é raiz primitiva módulo 25.

3.6 Raízes Primitivas Módulo p^k

Teorema 68. *Seja p um primo ímpar e $k \geq 2$. Se g é raiz primitiva módulo p^k, então g é raiz primitiva módulo p^{k+1}.*

Demonstração. Seja $d = \text{ord}_{p^{k+1}}(g)$. Então $g^d \equiv 1 \pmod{p^{k+1}}$. Logo, $g^d \equiv 1 \pmod{p^k}$. Como g é raiz primitiva módulo p^k, segue que $\phi(p^k) \mid d$. Por outro lado, pelo Teorema de Euler, $d \mid \phi(p^{k+1})$.

Como $\phi(p^k) = p^{k-1}(p-1)$ e $\phi(p^{k+1}) = p^k(p-1)$, segue que $d = \phi(p^k)$ ou $d = \phi(p^{k+1})$.

Portanto, para mostrar que g é raiz primitiva módulo p^{k+1}, basta mostrar que:

$$g^{\phi(p^k)} \not\equiv 1 \pmod{p^{k+1}} \iff g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$$

Como g é raiz primitiva módulo p^k, pelo Teorema de Euler temos $g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$.

Isto quer dizer que:

$$g^{p^{k-2}(p-1)} = 1 + p^{k-1}t \quad \text{com } \text{mdc}(t,p) = 1.$$

Mas isto significa:

$$g^{p^{k-1}(p-1)} = (1+p^{k-1}t)^p = 1 + p \cdot p^{k-1}t + \binom{p}{2}(p^{k-1}t)^2 + \cdots \equiv 1 + p^k t \not\equiv 1 \pmod{p^{k+1}}.$$

Logo, $d = \phi(p^{k+1})$, ou seja, g é raiz primitiva módulo p^{k+1}. □

3.7 Raízes Primitivas Módulo Potências de 2

Vimos nos Teoremas 67 e 68 que p^k possui raízes primitivas para p primo ímpar.

- $m = 2 \implies \text{SRR} = \{1\}$.
- $m = 4 \implies \text{SRR} = \{1, 3\}$, $\phi(4) = 2$.

  $$\text{ord}_4(3) = 2 \quad (3 \not\equiv 1 \pmod 4, \text{ mas } 3^2 \equiv 1 \pmod 4).$$

  Logo, 3 é raiz primitiva módulo 4. Quantidade de raízes primitivas: $\phi(\phi(4)) = \phi(2) = 1$.

- $m = 8 \implies \text{SRR} = \{1, 3, 5, 7\}$, $\phi(8) = 4$.

  $$3^2 = 9 \equiv 1 \pmod 8$$
  $$5^2 = 25 \equiv 1 \pmod 8$$
  $$7^2 = 49 \equiv 1 \pmod 8.$$

  Assim, $\text{ord}_8(1) = 1$ e $\text{ord}_8(3) = \text{ord}_8(5) = \text{ord}_8(7) = 2$. **Não existem raízes primitivas módulo 8.**

- $m = 16 \implies \text{SRR} = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $\phi(16) = 8$.
  - Potências de 3: $3, 9, 11, 1 \implies \text{ord}_{16}(3) = 4$

– Potências de 5: $5, 9, 13, 1 \implies \text{ord}_{16}(5) = 4$
– Potências de 7: $7, 1 \implies \text{ord}_{16}(7) = 2$
– Potências de 9: $9, 1 \implies \text{ord}_{16}(9) = 2$
– Potências de 11: $11, 9, 3, 1 \implies \text{ord}_{16}(11) = 4$
– Potências de 13: $13, 9, 5, 1 \implies \text{ord}_{16}(13) = 4$
– Potências de 15: $15, 1 \implies \text{ord}_{16}(15) = 2$

Também não existem raízes primitivas módulo 16.

Teorema 69. *Seja a ímpar e $n \geq 3$. Então*

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

A demonstração deste teorema vem depois do corolário abaixo.

Observação. Isto é um resultado mais forte do que o Teorema de Euler, que garante apenas $a^{\phi(2^n)} = a^{2^{n-1}} \equiv 1 \pmod{2^n}$.

Corolário 70. *Não existem raízes primitivas módulo 2^n para $n \geq 3$.*

Demonstração. Por indução em $n \geq 3$.

- **Caso inicial ($n = 3$):** Para $n = 3$ a afirmação é $a^2 \equiv 1 \pmod{8}$, que vale para todo a ímpar.
- **Passo indutivo:** Suponha válido para n, ou seja, $a^{2^{n-2}} \equiv 1 \pmod{2^n}$. Isso significa que existe $t \in \mathbb{Z}$ tal que
$$a^{2^{n-2}} = 1 + 2^n t.$$
Elevando ambos os lados ao quadrado:
$$a^{2^{n-1}} = (1 + 2^n t)^2 = 1 + 2 \cdot 2^n t + 2^{2n} t^2 = 1 + 2^{n+1} t + 2^{2n} t^2.$$
Como $n \geq 3 \implies 2n \geq n + 1$, temos $2^{n+1} \mid 2^{2n} t^2$. Portanto:
$$a^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}.$$

□

3.8 Módulos Gerais

Teorema 71. *Seja $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\text{mdc}(a, m) = 1$. Então*

$$a^M \equiv 1 \pmod{m}$$

onde $M = \text{mmc}(\phi(p_1^{\alpha_1}), \dots, \phi(p_k^{\alpha_k}))$.

Demonstração. Pelo Teorema de Euler, para cada $i \in \{1, \dots, k\}$, temos $a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$. Como $\phi(p_i^{\alpha_i}) \mid M$, segue que $a^M \equiv 1 \pmod{p_i^{\alpha_i}}$ para todo i. Como os módulos $p_i^{\alpha_i}$ são primos entre si dois a dois, concluímos que:

$$a^M \equiv 1 \pmod{m}.$$

□

Análise do valor de M: Se $\phi(p_1^{\alpha_1}), \ldots, \phi(p_k^{\alpha_k})$ não forem primos entre si, teremos $M < \phi(m)$, de modo que nenhum elemento terá ordem $\phi(m)$. Assim, m não admitirá raiz primitiva.

- Se p é um primo ímpar, $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ é sempre um número par.
- Portanto, se m possui pelo menos dois fatores primos ímpares distintos,

$$\text{mmc}(\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2})) < \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}),$$

  o que implica $M < \phi(m)$. Logo, m não admite raiz primitiva.
- Se $m = 2^\alpha p^\beta$ com $\alpha \geq 2$ e p primo ímpar, como $\phi(2^\alpha) = 2^{\alpha-1}$ é par para $\alpha \geq 2$, pelo mesmo motivo $2^\alpha p^\beta$ não possui raiz primitiva.

Conclusão: Sobraram apenas os seguintes módulos que podem admitir raízes primitivas:

$$m = 1, 2, 4, p^\alpha, 2p^\alpha \quad (p \text{ primo ímpar}, \alpha \geq 1).$$

Exercício 136. Mostre que a é raiz primitiva módulo $2p^\alpha$ se, e somente se, a é raiz primitiva módulo p^α e a é ímpar. Em particular, se a é raiz primitiva módulo p^α, então a ou $a + p^\alpha$ é raiz primitiva módulo $2p^\alpha$.

Exemplo: 22 é raiz primitiva mod 25. Como $22 + 25 = 47$ é ímpar, 47 é raiz primitiva mod 50.

Teorema 72. *Seja $m = 1, 2, 4, p^\alpha$ ou $2p^\alpha$ ($\alpha \geq 1$, p primo ímpar) e $\text{mdc}(a, m) = 1$. A congruência*

$$x^n \equiv a \pmod{m}$$

tem $\text{mdc}(n, \phi(m))$ soluções se $a^{\frac{\phi(m)}{\text{mdc}(n,\phi(m))}} \equiv 1 \pmod{m}$ e tem 0 soluções caso contrário.

Demonstração. Seja g uma raiz primitiva módulo m. Como $\text{mdc}(a, m) = 1$, existe k tal que $a \equiv g^k \pmod{m}$. Como $\{g^0, g^1, g^2, \ldots, g^{\phi(m)-1}\}$ forma um Sistema Reduzido de Restos (SRR) módulo m, a quantidade de soluções da congruência $x^n \equiv a \pmod{m}$ é igual ao número de $j \in \{0, 1, \ldots, \phi(m) - 1\}$ tais que:

$$g^{jn} \equiv g^k \pmod{m}.$$

Sendo g raiz primitiva módulo m, essa congruência de potências é equivalente à congruência linear:

$$j \cdot n \equiv k \pmod{\phi(m)}.$$

Esta congruência linear possui solução se, e somente se, $\text{mdc}(n, \phi(m)) \mid k$, hipótese que equivale a $a^{\frac{\phi(m)}{\text{mdc}(n,\phi(m))}} \equiv 1 \pmod{m}$. Quando satisfeita, o número de soluções incongruentes para $j \pmod{\phi(m)}$ (e consequentemente para $x \pmod{m}$) é exatamente $\text{mdc}(n, \phi(m))$. □

3.9 Exercícios

Raízes primitivas e resíduos de potência (Seção 2.8 de [NZM91])

137. (NZM, 2.8.1) Encontre uma raiz primitiva do primo 3; do primo 5; do primo 7; do primo 11; do primo 13.

138. (NZM, 2.8.2) Encontre uma raiz primitiva de 23.

139. (NZM, 2.8.3) Quantas raízes primitivas tem o primo 13?

140. (NZM, 2.8.4) Qual é a ordem de cada um dos números 1, 2, 3, 4, 5, 6 módulo 7? E módulo 11?

141. (NZM, 2.8.5) Seja p um primo ímpar. Prove que a tem ordem 2 módulo p se, e somente se, $a \equiv -1 \pmod{p}$.

142. (NZM, 2.8.6) Se a tem ordem h módulo m, prove que não há dois entre a, a^2, a^3, $\cdots$, a^h que sejam congruentes módulo m.

143. (NZM, 2.8.7) Se p é um primo ímpar, quantas soluções existem para $x^{p-1} \equiv 1 \pmod{p}$? E para $x^{p-1} \equiv 2 \pmod{p}$?

144. (NZM, 2.8.8) Use o Teorema 65 para determinar quantas soluções tem cada uma das seguintes congruências:
(a) $x^{12} \equiv 16 \pmod{17}$
(b) $x^{48} \equiv 9 \pmod{17}$
(c) $x^{20} \equiv 13 \pmod{17}$
(d) $x^{11} \equiv 9 \pmod{17}$.

145. (NZM, 2.8.9) Mostre que $3^8 \equiv -1 \pmod{17}$. Explique por que isso implica que 3 é uma raiz primitiva de 17.

146. (NZM, 2.8.10) Mostre que as potências de 3 (mod 17) são 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1. Use essa informação para encontrar as soluções das congruências do Exercício 144.

147. (NZM, 2.8.11) Usando os dados do problema anterior, decida quais das congruências $x^2 \equiv 1, x^2 \equiv 2, x^2 \equiv 3, \ldots, x^2 \equiv 16 \pmod{17}$ têm solução.

148. (NZM, 2.8.12) Prove que se p é primo, $(a, p) = 1$ e $(n, p-1) = 1$, então $x^n \equiv a \pmod{p}$ tem exatamente uma solução.

149. (NZM, 2.8.13) Mostre que os números $1^k, 2^k, \ldots, (p-1)^k$ formam um sistema reduzido de restos $\pmod{p}$ se, e somente se, $(k, p-1) = 1$.

150. (NZM, 2.8.14) Suponha que a tenha ordem $h \pmod{p}$ e que $a\bar{a} \equiv 1 \pmod{p}$. Mostre que $\bar{a}$ também tem ordem h. Suponha que g seja uma raiz primitiva $\pmod{p}$ e que $a \equiv g^i \pmod{p}, 0 \leq i < p-1$. Mostre que $\bar{a} \equiv g^{p-1-i} \pmod{p}$.

151. (NZM, 2.8.15) Prove que se a tem ordem h módulo um primo p, e se h é par, então $a^{h/2} \equiv -1 \pmod{p}$.

152. (NZM, 2.8.16) Sejam m e n inteiros positivos. Mostre que $(2^m - 1, 2^n + 1) = 1$ se m é ímpar.

153. (NZM, 2.8.17) Mostre que se $a^k + 1$ é primo e $a > 1$, então k é uma potência de 2. Mostre que se $p \mid \left(a^{2^n} + 1\right)$, então $p = 2$ ou $p \equiv 1 \pmod{2^{n+1}}$.

154. (NZM, 2.8.18) Mostre que se g e g' são raízes primitivas módulo um primo ímpar p, então gg' não é raiz primitiva de p.

155. (NZM, 2.8.19) Mostre que se $a^h \equiv 1 \pmod{p}$, então $a^{ph} \equiv 1 \pmod{p^2}$. Mostre que se g é uma raiz primitiva $\pmod{p^2}$, então é uma raiz primitiva $\pmod{p}$.

156. (NZM, 2.8.20) Dos 101 inteiros de um sistema completo de restos $\pmod{101^2}$ que são $\equiv 2 \pmod{101}$, qual deles não é raiz primitiva $\pmod{101^2}$?

157. (NZM, 2.8.21) Seja g uma raiz primitiva do primo ímpar p. Mostre que $-g$ é raiz primitiva, ou não, conforme $p \equiv 1 \pmod{4}$ ou $p \equiv 3 \pmod{4}$.

158. (NZM, 2.8.22) Seja g uma raiz primitiva $\pmod{p}$. Mostre que $(p-1)! \equiv g \cdot g^2 \cdots g^{p-1} \equiv g^{p(p-1)/2} \pmod{p}$. Use isso para dar outra demonstração da congruência de Wilson (Teorema 41).

159. (NZM, 2.8.23) Prove que se a tem ordem 3 módulo um primo p, então $1+a+a^2 \equiv 0 \pmod{p}$, e $1 + a$ tem ordem 6.

160. (NZM, 2.8.24) Sejam a e $n > 1$ inteiros quaisquer tais que $a^{n-1} \equiv 1 \pmod{n}$, mas $a^d \not\equiv 1 \pmod{n}$ para todo divisor próprio d de $n - 1$. Prove que n é primo.

161. (NZM, 2.8.25) Mostre que o número de resíduos reduzidos $a \pmod{m}$ tais que $a^{m-1} \equiv 1 \pmod{m}$ é exatamente $\prod_{p|m}(p - 1, m - 1)$.

162. (NZM, 2.8.26) (Lembre que m é um número de Carmichael se $a^{m-1} \equiv 1 \pmod{m}$ para todos os resíduos reduzidos $a \pmod{m}$.) Mostre que m é um número de Carmichael se, e somente se, m é livre de quadrados e $(p - 1) \mid (m - 1)$ para todos os primos p que dividem m. Deduza que $2821 = 7 \cdot 13 \cdot 31$ é um número de Carmichael.

163. (NZM, 2.8.27) Mostre que m é um número de Carmichael se, e somente se, $a^m \equiv a \pmod{m}$ para todos os inteiros a.

164. (NZM, 2.8.28) Mostre que as seguintes afirmações sobre o inteiro positivo n são equivalentes:

(i) n é livre de quadrados e $(p - 1) \mid n$ para todos os primos p que dividem n;

(ii) Se j e k são inteiros positivos tais que $j \equiv k \pmod{n}$, então

$$a^j \equiv a^k \pmod{n} \text{ para todos os inteiros } a.$$

(Os números 1, 2, 6, 42, 1806 têm essa propriedade, mas não há outros. Veja J. Dyer-Bennet, "A theorem on partitions of the set of positive integers," Amer. Math. Monthly, 47 (1940), 152-154.)

165. (NZM, 2.8.29) Mostre que a sequência $1^1, 2^2, 3^3, \ldots$, considerada $\pmod p$, é periódica com período mínimo $p(p-1)$.

166. (NZM, 2.8.30) Suponha que $(10a, q) = 1$ e que k seja a ordem de 10 $\pmod q$. Mostre que a expansão decimal do número racional a/q é periódica com período mínimo k.

167. (NZM, 2.8.31) Mostre que a expansão decimal de $1/p$ tem período $p-1$ se, e somente se, 10 é uma raiz primitiva de p. (Conjectura-se que, se g não é um quadrado e $g \neq -1$, então existem infinitos primos dos quais g é raiz primitiva.)

168. (NZM, 2.8.32) Seja $r_1, r_2, \ldots, r_n$ um sistema reduzido de restos módulo $m (n = \phi(m))$. Mostre que os números $r_1^k, r_2^k, \ldots, r_n^k$ formam um sistema reduzido de restos $(\text{mod } m)$ se, e somente se, $(k, \phi(m)) = 1$.

169. (NZM, 2.8.33) Sejam k e a inteiros positivos, com $a \geq 2$. Mostre que $k \mid \phi\left(a^k - 1\right)$.

170. (NZM, 2.8.34) Mostre que se $p \mid \phi(m)$ e $p \nmid m$, então existe pelo menos um fator primo q de m tal que $q \equiv 1 \pmod p$.

171. (NZM, 2.8.35) Seja p um número primo dado. Prove que existem infinitos números primos $q \equiv 1 \pmod p$.

172. (NZM, 2.8.37) Mostre que se $n > 1$, então $n \nmid (2^n - 1)$.

173. (NZM, 2.8.38) Seja m dado; suponha que q seja um número primo, $q^\alpha \| (m-1), \alpha > 0$, e que exista um número a tal que $a^{m-1} \equiv 1 \pmod m$, mas $\left(a^{(m-1)/q} - 1, m\right) = 1$. Mostre que $p \equiv 1 \pmod{q^\alpha}$ para todos os fatores primos p de m.

Capítulo 4

Resíduos Quadráticos

4.1 Definição e Primeiros Exemplos

Definição. Seja $m \in \mathbb{Z}$, $m > 0$ e $\text{mdc}(a, m) = 1$. Dizemos que a é um **resíduo quadrático** módulo m se a congruência

$$x^2 \equiv a \pmod{m}$$

tem solução.

Exemplos.

- -1 é um resíduo quadrático módulo 5, pois $2^2 = 4 \equiv -1 \pmod{5}$.
- 3 não é resíduo quadrático módulo 8.
  - Se x é par, x^2 é par $\implies x^2 \not\equiv 3 \pmod{8}$.
  - Se x é ímpar, testando os casos vemos que $x^2 \equiv 1 \pmod{8}$.

Nosso foco será no caso em que $m = p$ é um número primo ímpar. Lembre, pelo Teorema 65 com $n = 2$, que a congruência $x^2 \equiv a \pmod{p}$ tem $\text{mdc}(2, p-1) = 2$ soluções se $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, e 0 soluções caso contrário.

Segue automaticamente o seguinte:

Lema 73. *Seja p um primo ímpar e* $\text{mdc}(a, p) = 1$. *Então a é resíduo quadrático módulo p se, e somente se, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Caso contrário, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Demonstração. A equivalência é o Teorema 65 com $n = 2$. Como $(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p}$ pelo Teorema de Fermat, segue que $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Se a não é resíduo quadrático, então $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Definição. a é um **resíduo não-quadrático** módulo p se $x^2 \equiv a \pmod{p}$ não tem solução (com $\text{mdc}(a, p) = 1$).

Exemplo ($p = 7$)**.** Temos $\frac{p-1}{2} = 3$.

$$\begin{aligned}
1^3 &= 1 \equiv 1 \pmod{7} \\
2^3 &= 8 \equiv 1 \pmod{7} \\
3^3 &= 27 \equiv 6 \equiv -1 \pmod{7} \\
4^3 &= 64 \equiv 1 \pmod{7} \\
5^3 &= 125 \equiv 6 \equiv -1 \pmod{7} \\
6^3 &= (-1)^3 = -1 \equiv 6 \pmod{7}.
\end{aligned}$$

Conclusão: $1, 2, 4$ são resíduos quadráticos mod 7 e $3, 5, 6$ são resíduos não-quadráticos.

4.2 Símbolo de Legendre

Definição. Seja p um número primo ímpar. Para cada $a \in \mathbb{Z}$, definimos o **Símbolo de Legendre** de a mod p, denotado por $\left(\frac{a}{p}\right)$, da seguinte forma:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é resíduo quadrático mod } p, \\ -1, & \text{se } a \text{ é resíduo não-quadrático mod } p, \\ 0, & \text{se } a \equiv 0 \pmod{p}. \end{cases}$$

Exemplo ($p = 7$)**.**

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1, \quad \left(\frac{0}{7}\right) = 0.$$

Proposição 74. *Seja p um primo ímpar.*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
4. $\text{mdc}(a, p) = 1 \implies \left(\frac{a^2}{p}\right) = 1 \quad e \quad \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right), \forall b$
5. $\left(\frac{1}{p}\right) = 1 \quad e \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Demonstração. 1. Já vimos no Lema 73.

2. Segue do item (1):

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

   Como $p \geq 3$, o único múltiplo de p no intervalo $[-2, 2]$ para a diferença $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)$ é 0. Conclusão: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

3. Se $a \equiv b \pmod{p}$, então $x^2 \equiv a \pmod{p} \iff x^2 \equiv b \pmod{p}$.

4. Segue do item (2) que $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2$. Como $\left(\frac{a}{p}\right) = \pm 1$, temos $(\pm 1)^2 = 1$. A outra parte segue diretamente de (2).

5. $\left(\frac{1}{p}\right) = 1$ pois $1^2 \equiv 1 \pmod{p}$. Por outro lado, do item (1) temos $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Como feito em (2), conclui-se que a igualdade é exata: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

□

Seja g uma raiz primitiva mod p. Isto quer dizer que $\{g^1, g^2, \ldots, g^{p-1}\}$ é um SRR mod p. É evidente que os números $g^2, g^4, \ldots, g^{p-1}$ são resíduos quadráticos, pois $(g^j)^2 \equiv g^{2j} \pmod{p}$. Ou seja, em um SRR mod p, há pelo menos $\frac{p-1}{2}$ resíduos quadráticos.

Afirmação: Estes são os únicos.

$$(g^{2j+1})^{\frac{p-1}{2}} = (g^{2j})^{\frac{p-1}{2}} \cdot g^{\frac{p-1}{2}} = (g^{p-1})^j \cdot (-1) \equiv 1 \cdot (-1) = -1 \pmod{p}.$$

Conclusão: Em um SRR mod p, exatamente metade dos termos são resíduos quadráticos e a outra metade são resíduos não-quadráticos.

4.3 Lema de Gauss

Lema 75 (Lema de Gauss)**.** *Seja p um primo ímpar e $\mathrm{mdc}(a,p) = 1$. Considere os inteiros*

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a$$

e seus restos quando divididos por p. Se n denota o número destes restos que pertencem ao conjunto

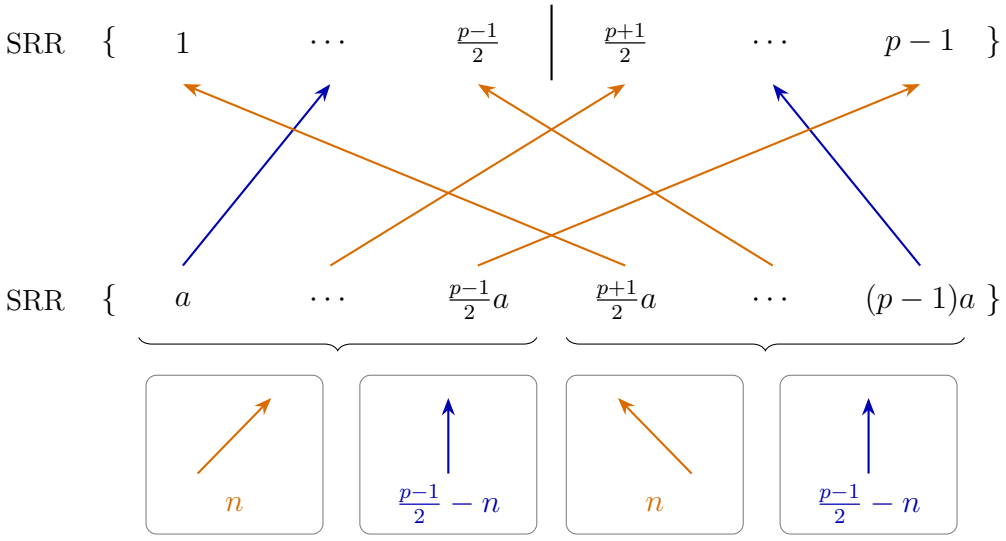
$$\left\{\frac{p+1}{2}, \ldots, p-1\right\}$$

então:

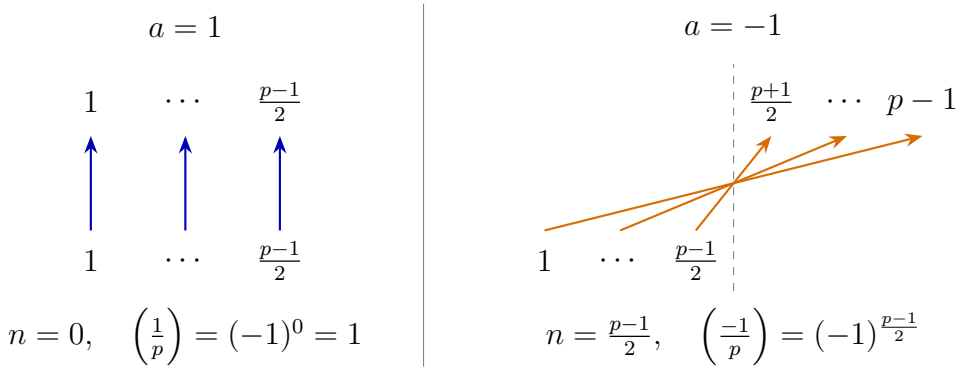
$$\left(\frac{a}{p}\right) = (-1)^n.$$

Exemplos.

- Para $a = 1$: Os restos de $1, 2, \ldots, \frac{p-1}{2}$ pertencem todos ao conjunto $\{1, \ldots, \frac{p-1}{2}\}$. Logo $n = 0 \implies \left(\frac{1}{p}\right) = (-1)^0 = 1$.
- Para $a = -1$: Os restos de $-1, -2, \ldots, -\frac{p-1}{2} \equiv p-1, p-2, \ldots, \frac{p+1}{2}$ estão todos na segunda metade. Logo $n = \frac{p-1}{2} \implies \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.



Cada seta liga um número x ao número $ax \pmod{p}$: sai de ax, na linha de baixo, e chega ao seu resto módulo p, na linha de cima. Em azul, as setas que ficam na mesma metade; em laranja, as que trocam de metade.



Demonstração. Vamos definir a função $f : \{1, \ldots, \frac{p-1}{2}\} \to \{1, \ldots, \frac{p-1}{2}\}$ da seguinte forma: Dado $i \in \{1, \ldots, \frac{p-1}{2}\}$, seja r_i o resto da divisão de ai por p. Definimos:

$$f(i) = \begin{cases} r_i, & \text{se } r_i \in \left\{1, \ldots, \frac{p-1}{2}\right\}, \\ p - r_i, & \text{se } r_i \in \left\{\frac{p+1}{2}, \ldots, p-1\right\}. \end{cases}$$

Afirmação: $\left\{f(1), \ldots, f\left(\frac{p-1}{2}\right)\right\} = \left\{1, \ldots, \frac{p-1}{2}\right\}$.

Para mostrar a afirmação, basta mostrar que se $i \neq j$, então $f(i) \neq f(j)$. Suponha por absurdo que $f(i) \equiv f(j) \pmod p$ para $i, j \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ distintos. Sabemos que $f(i) \equiv \pm r_i \equiv \pm ai \pmod p$ e $f(j) \equiv \pm r_j \equiv \pm aj \pmod p$. Portanto:

$$f(i) \equiv f(j) \pmod p \implies ai \equiv \pm aj \pmod p.$$

Como $\text{mdc}(a, p) = 1$, isso implicaria $i \equiv \pm j \pmod p$.

- 1º caso: $i \equiv j \pmod p$. Absurdo, pois $i, j \in \left\{1, \ldots, \frac{p-1}{2}\right\} \subset \{1, \ldots, p-1\}$ e são distintos.
- 2º caso: $i \equiv -j \pmod p \implies i \equiv p - j \pmod p$. Absurdo, pois $i \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ e $p - j \in \left\{\frac{p+1}{2}, \ldots, p-1\right\}$, logo são elementos distintos de um SRR e portanto incongruentes.

Isso conclui a prova da afirmação.

Utilizando a afirmação que acabamos de provar:

$$\prod_{i=1}^{\frac{p-1}{2}} f(i) = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)!$$

Por outro lado:

$$\prod_{i=1}^{\frac{p-1}{2}} f(i) \equiv \prod_{r_i \leq \frac{p-1}{2}} (r_i) \cdot \prod_{r_i > \frac{p-1}{2}} (-r_i) \equiv (-1)^n \prod_{i=1}^{\frac{p-1}{2}} (ai) = (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

Juntando as duas informações:

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

Como $\text{mdc}\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$, podemos cancelar o fatorial:

$$1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod p \implies (-1)^n \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Como $(-1)^n - \left(\frac{a}{p}\right) \in [-2, 2]$, a diferença deve ser 0, ou seja, $\left(\frac{a}{p}\right) = (-1)^n$. □

4.4 Lema de Eisenstein

Lembrando que para $x \in \mathbb{R}$, $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a x (função piso).

$$\lfloor 4{,}97 \rfloor = 4,\ \lfloor \pi \rfloor = 3,\ \lfloor -1{,}5 \rfloor = -2.$$

Proposição 76 (Lema de Eisenstein)**.** *Se p é um primo ímpar e* $\mathrm{mdc}(a, p) = 1$*:*

1. *Se a é ímpar, então:*

$$\left(\frac{a}{p}\right) = (-1)^t, \quad \textit{onde } t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor.$$

2. *Para $a = 2$:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Demonstração. Para cada $i = 1, 2, \ldots, \frac{p-1}{2}$, pela divisão euclidiana de ai por p:

$$ai = p \left\lfloor \frac{ai}{p} \right\rfloor + r_i, \quad \text{com } 0 \leq r_i < p.$$

Considere a função do Lema de Gauss $f(i)$:

$$f(i) = \begin{cases} r_i, & \text{se } r_i < \frac{p}{2} \\ p - r_i, & \text{se } r_i > \frac{p}{2}. \end{cases}$$

Assim, podemos escrever:

$$ai = \begin{cases} p \left\lfloor \frac{ai}{p} \right\rfloor + f(i), & \text{se } r_i < \frac{p}{2} \\ p \left\lfloor \frac{ai}{p} \right\rfloor + p - f(i), & \text{se } r_i > \frac{p}{2}. \end{cases}$$

Somando essas equações para $i = 1, \ldots, \frac{p-1}{2}$:

$$\sum_{i=1}^{\frac{p-1}{2}} ai = p \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor + \sum_{r_i < \frac{p}{2}} f(i) + \sum_{r_i > \frac{p}{2}} (p - f(i)).$$

Seja n o número de restos $r_i > \frac{p}{2}$. Então:

$$a \sum_{i=1}^{\frac{p-1}{2}} i = p \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor + n \cdot p + \sum_{r_i < \frac{p}{2}} f(i) - \sum_{r_i > \frac{p}{2}} f(i).$$

Como $\{f(1), \ldots, f(\frac{p-1}{2})\} = \{1, \ldots, \frac{p-1}{2}\}$, a soma de todos os $f(i)$ é igual a $\sum_{i=1}^{\frac{p-1}{2}} i = \frac{p^2-1}{8}$. Analisando a igualdade módulo 2 (usando $p \equiv 1 \pmod 2$):

$$a \left(\frac{p^2-1}{8}\right) \equiv \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor + n + \frac{p^2-1}{8} \pmod 2.$$

- **1º Caso (a ímpar):** Como $a \equiv 1 \pmod 2$, temos:

$$\frac{p^2-1}{8} \equiv \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor + n + \frac{p^2-1}{8} \pmod 2 \implies n \equiv \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor = t \pmod 2.$$

  Logo, $(-1)^t = (-1)^n = \left(\frac{a}{p}\right)$.

- **2º Caso ($a = 2$):** Para todo $i \in \{1, \ldots, \frac{p-1}{2}\}$, temos $2i < p$, portanto $\left\lfloor \frac{2i}{p} \right\rfloor = 0$. Substituindo $a = 2$:

$$2\left(\frac{p^2-1}{8}\right) \equiv 0 \equiv 0 + n + \frac{p^2-1}{8} \pmod 2 \implies n \equiv \frac{p^2-1}{8} \pmod 2.$$

  Logo, $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$.

□

Exemplo ($a = 9$, $p = 11$)**.** Temos $\frac{p-1}{2} = 5$. Restos da divisão de $9i$ por 11:

$$\begin{aligned}
i = 1: &\quad 9 = 11 \cdot 0 + 9 \implies r_1 = 9, \quad \lfloor 9/11 \rfloor = 0 \\
i = 2: &\quad 18 = 11 \cdot 1 + 7 \implies r_2 = 7, \quad \lfloor 18/11 \rfloor = 1 \\
i = 3: &\quad 27 = 11 \cdot 2 + 5 \implies r_3 = 5, \quad \lfloor 27/11 \rfloor = 2 \\
i = 4: &\quad 36 = 11 \cdot 3 + 3 \implies r_4 = 3, \quad \lfloor 36/11 \rfloor = 3 \\
i = 5: &\quad 45 = 11 \cdot 4 + 1 \implies r_5 = 1, \quad \lfloor 45/11 \rfloor = 4.
\end{aligned}$$

Os restos maiores que $11/2 = 5.5$ são $r_1 = 9, r_2 = 7$, logo $n = 2$. Por outro lado, $t = \sum \left\lfloor \frac{9i}{11} \right\rfloor = 0 + 1 + 2 + 3 + 4 = 10$. Note que $t \equiv n \pmod 2$ ($10 \equiv 2 \pmod 2$).

4.5 Lei da Reciprocidade Quadrática

Sejam p e q primos ímpares. A priori não existe qualquer relação entre o fato de p ser ou não resíduo quadrático módulo q e o fato de q ser ou não resíduo quadrático módulo p. O teorema da reciprocidade quadrática que demonstraremos a seguir diz que na verdade existe sim.

Teorema 77 (Lei da Reciprocidade Quadrática de Gauss)**.** *Sejam p e q primos ímpares distintos. Então:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Exemplo. Calcular $\left(\frac{7}{101}\right)$. Note que 101 é primo e $101 \equiv 1 \pmod 4$, enquanto $7 \equiv 3 \pmod 4$.

$$\left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

Pela Reciprocidade Quadrática:

$$\left(\frac{7}{101}\right)\left(\frac{101}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{101-1}{2}} = (-1)^{3\cdot 50} = 1$$

$$\implies \left(\frac{7}{101}\right)\cdot(-1) = 1 \implies \left(\frac{7}{101}\right) = -1.$$

Exemplo. Calcular $\left(\frac{47}{131}\right)$.

1. $\left(\frac{47}{131}\right)\left(\frac{131}{47}\right) = (-1)^{23\cdot 65} = -1 \implies \left(\frac{47}{131}\right) = -\left(\frac{131}{47}\right)$
2. $\left(\frac{131}{47}\right) = \left(\frac{37}{47}\right)$
3. $\left(\frac{37}{47}\right)\left(\frac{47}{37}\right) = (-1)^{18\cdot 23} = 1 \implies \left(\frac{37}{47}\right) = \left(\frac{47}{37}\right)$
4. $\left(\frac{47}{37}\right) = \left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right)$
5. $\left(\frac{2}{37}\right) = (-1)^{\frac{37^2-1}{8}} = (-1)^{171} = -1$
6. $\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1$

Juntando tudo:

$$\left(\frac{47}{131}\right) = -\left(\frac{131}{47}\right) = -\left(\frac{37}{47}\right) = -\left(\frac{10}{37}\right) = -\left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -(-1)(-1) = -1.$$

Demonstração do teorema. Pelo Lema de Eisenstein (Proposição 76):

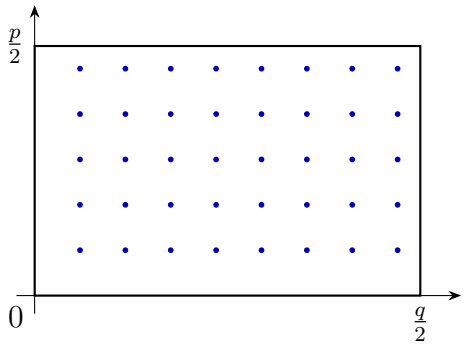
$$\left(\frac{p}{q}\right) = (-1)^{\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{pi}{q} \right\rfloor} \quad \text{e} \quad \left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor}.$$

Considere o retângulo no plano cartesiano definido por $1 \leq x \leq \frac{q-1}{2}$ e $1 \leq y \leq \frac{p-1}{2}$. O número total de pontos com coordenadas inteiras (x, y) neste retângulo é:

$$N = \left(\frac{q-1}{2}\right) \cdot \left(\frac{p-1}{2}\right).$$

A reta $y = \frac{p}{q}x$ conecta a origem ao ponto $(q/2, p/2)$. Nenhum ponto de coordenadas inteiras (x, y) com $1 \leq x \leq \frac{q-1}{2}$ está sobre a reta, pois p e q são primos entre si ($\text{mdc}(p, q) = 1$).

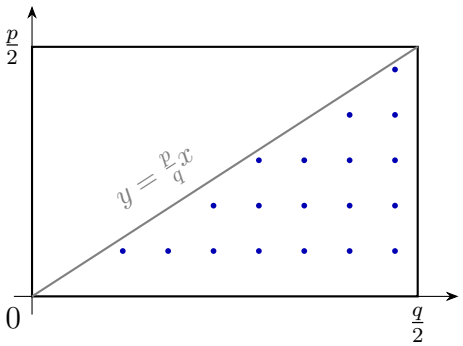
Nas figuras abaixo, $p = 11$ e $q = 17$: são 40 pontos, 19 abaixo da reta e 21 acima.

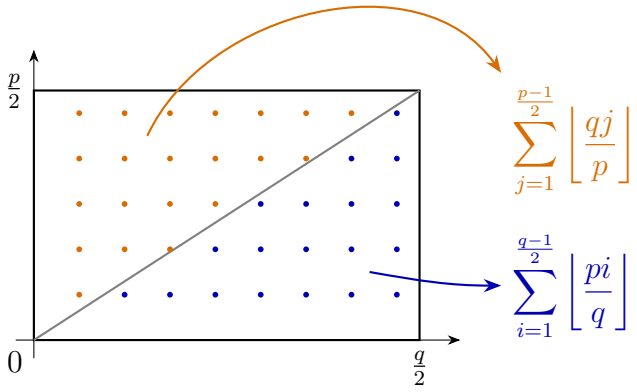


$\frac{q-1}{2}$ possibilidades para x

$\frac{p-1}{2}$ possibilidades para y

Total: $\frac{p-1}{2} \cdot \frac{q-1}{2}$

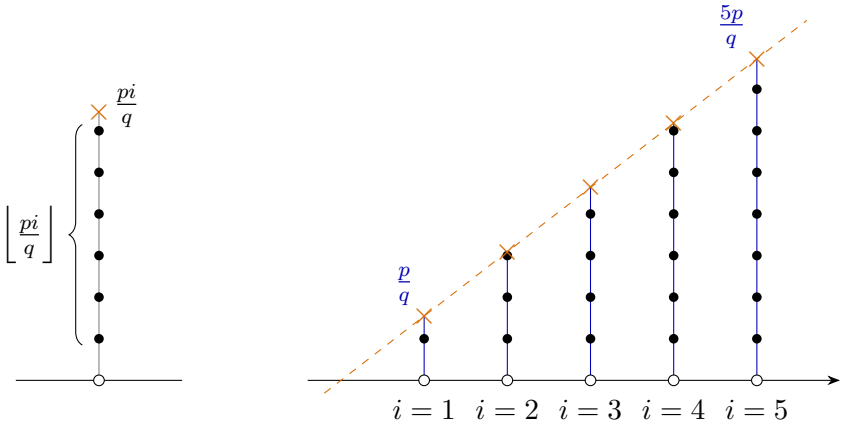




Para interpretar geometricamente cada parcela, note que

$$\left\lfloor \frac{pi}{q} \right\rfloor = \#\left\{k \in \mathbb{Z} : 1 \leq k \leq \frac{pi}{q}\right\}.$$

Na figura abaixo, trocamos os papéis: $p = 17$ e $q = 11$.



- O número de pontos de grade abaixo da reta para um $x = i$ fixo é $\left\lfloor \frac{pi}{q} \right\rfloor$. Somando para todos os $x \in \{1, \ldots, \frac{q-1}{2}\}$, o número de pontos abaixo da reta é $\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{pi}{q} \right\rfloor$.
- Invertendo os eixos, o número de pontos de grade acima da reta é dado por $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor$.

Como todo ponto do retângulo está estritamente acima ou abaixo da reta:

$$\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{pi}{q} \right\rfloor + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor = \left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right).$$

Portanto:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\Sigma\left\lfloor \frac{pi}{q} \right\rfloor + \Sigma\left\lfloor \frac{qj}{p} \right\rfloor} = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

□

4.6 Formas Equivalentes e Valores Pequenos

Reescrevendo a Lei da Reciprocidade Quadrática:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{se } q \equiv 1 \pmod 4 \text{ ou } p \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right) = \left(\frac{-q}{p}\right), & \text{se } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

4.6.1 Símbolo para $a = 2, 3, 5, 7$

Em cada fórmula abaixo, p é um primo ímpar diferente de a.

1. Para $a = 2$: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

- $p \equiv 1 \pmod 8 \implies \frac{(8k+1)^2-1}{8} = 8k^2 + 2k$ (par) $\implies \left(\frac{2}{p}\right) = 1$
- $p \equiv 3 \pmod 8 \implies \frac{(8k+3)^2-1}{8} = 8k^2 + 6k + 1$ (ímpar) $\implies \left(\frac{2}{p}\right) = -1$
- $p \equiv 5 \pmod 8 \implies \frac{(8k+5)^2-1}{8} = 8k^2 + 10k + 3$ (ímpar) $\implies \left(\frac{2}{p}\right) = -1$
- $p \equiv 7 \pmod 8 \implies \frac{(8k+7)^2-1}{8} = 8k^2 + 14k + 6$ (par) $\implies \left(\frac{2}{p}\right) = 1$

Conclusão:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 8, \\ -1, & \text{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

2. Para $a = 3$: $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1, 11 \pmod{12}, \\ -1, & \text{se } p \equiv 5, 7 \pmod{12}. \end{cases}$$

3. Para $a = 5$: Como $5 \equiv 1 \pmod 4$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1, 4 \pmod 5, \\ -1, & \text{se } p \equiv 2, 3 \pmod 5. \end{cases}$$

4. Para $a = 7$: $\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right)$

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 1, 2 \text{ ou } 4 \pmod 7, \\ 1, & \text{se } p \equiv -1 \pmod 4 \text{ e } p \equiv 3, 5 \text{ ou } 6 \pmod 7, \\ -1, & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 3, 5 \text{ ou } 6 \pmod 7, \\ -1, & \text{se } p \equiv -1 \pmod 4 \text{ e } p \equiv 1, 2 \text{ ou } 4 \pmod 7. \end{cases}$$

São $\phi(28) = 12$ classes no total. Por exemplo, $13 \equiv 1 \pmod 4$ e $13 \equiv 6 \pmod 7$, logo $\left(\frac{7}{13}\right) = -1$. Em classes módulo 28:

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}, \\ -1, & \text{se } p \equiv 5, 11, 13, 15, 17, 23 \pmod{28}. \end{cases}$$

4.7 Símbolo de Jacobi

O símbolo de Jacobi é uma generalização do símbolo de Legendre para módulos ímpares não necessariamente primos.

Definição. Seja Q um número ímpar positivo com fatoração em primos dada por

$$Q = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}.$$

Dado $N \in \mathbb{Z}$ qualquer, o **símbolo de Jacobi** $\left(\frac{N}{Q}\right)$ é definido por:

$$\left(\frac{N}{Q}\right) := \prod_{i=1}^{k} \left(\frac{N}{q_i}\right)^{\alpha_i} \in \{-1, 0, 1\}$$

onde $\left(\frac{N}{q_i}\right)$ denota o símbolo de Legendre.

Observação.

- $\left(\frac{N}{Q}\right) \in \{-1, 1\} \iff \text{mdc}(N, Q) = 1.$
- **NÃO É VERDADE** que $\left(\frac{N}{Q}\right) = 1 \implies N$ é resíduo quadrático módulo Q.

  Exemplo: Para $Q = 15 = 3 \cdot 5$ e $N = 2$:

  $$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$$

  porém não existe $x \in \mathbb{Z}$ tal que $x^2 \equiv 2 \pmod{15}$, pois $x^2 \equiv 2 \pmod 3$ não tem solução.

Teorema 78 (Relação entre o Símbolo de Jacobi e Soluções Quadráticas)**.** *Seja $Q = \prod_{i=1}^{k} p_i^{\alpha_i}$ um número ímpar.*

a) Se $\left(\frac{N}{Q}\right) = -1$, então N não é resíduo quadrático módulo Q.

b) N é resíduo quadrático módulo Q se, e somente se, N é resíduo quadrático módulo p_i para todo $i = 1, 2, \ldots, k$, ou seja, $\left(\frac{N}{p_i}\right) = 1$ para todo i.

Demonstração. a) Se $\left(\frac{N}{Q}\right) = -1$, então necessariamente existe algum fator p_i tal que $\left(\frac{N}{p_i}\right) = -1$. Se existisse x tal que $x^2 \equiv N \pmod Q$, reduzindo módulo p_i teríamos $x^2 \equiv N \pmod{p_i}$, o que é um absurdo pois $\left(\frac{N}{p_i}\right) = -1$.

b) A congruência $x^2 \equiv N \pmod Q$ é equivalente ao sistema de congruências:

$$\begin{cases} x^2 \equiv N \pmod{p_1^{\alpha_1}} \\ \quad \vdots \\ x^2 \equiv N \pmod{p_k^{\alpha_k}}. \end{cases}$$

Se $\left(\frac{N}{p_i}\right) = 1$, existe x_i tal que $x_i^2 \equiv N \pmod{p_i}$ com $\text{mdc}(x_i, p_i) = 1$. Seja $f(x) = x^2 - N$. Como $f'(x_i) = 2x_i \not\equiv 0 \pmod{p_i}$ (pois p_i é ímpar e $\text{mdc}(x_i, p_i) = 1$), pelo Lema de Hensel cada congruência $x^2 \equiv N \pmod{p_i^{\alpha_i}}$ possui solução y_i. Pelo Teorema Chinês dos Restos, existe x tal que $x \equiv y_i \pmod{p_i^{\alpha_i}}$ para todo i, o que fornece a solução de $x^2 \equiv N \pmod{Q}$.

□

Corolário 79. *Seja p um primo ímpar e $\alpha \geq 1$. Então a é resíduo quadrático mod p^α se, e somente se, $\left(\frac{a}{p}\right) = 1$.*

4.7.1 Propriedades do Símbolo de Jacobi

Teorema 80 (Propriedades Operatórias)**.** *Sejam Q, Q' inteiros ímpares positivos.*

a) $\left(\frac{N}{Q}\right)\left(\frac{N}{Q'}\right) = \left(\frac{N}{QQ'}\right)$

b) $\left(\frac{N}{Q}\right)\left(\frac{N'}{Q}\right) = \left(\frac{NN'}{Q}\right)$

c) Se $\text{mdc}(N, Q) = 1$*, então* $\left(\frac{N^2}{Q}\right) = \left(\frac{N}{Q^2}\right) = 1$.

d) Se $\text{mdc}(NN', QQ') = 1$*, então* $\left(\frac{N^2N'}{Q^2Q'}\right) = \left(\frac{N'}{Q'}\right)$.

e) Se $N' \equiv N \pmod{Q}$*, então* $\left(\frac{N'}{Q}\right) = \left(\frac{N}{Q}\right)$.

Demonstração. a) Escrevendo $Q = \prod p_i^{\alpha_i}$ e $Q' = \prod p_i^{\beta_i}$ (com a convenção $\left(\frac{N}{p_i}\right)^0 = 1$), temos:

$$\left(\frac{N}{Q}\right)\left(\frac{N}{Q'}\right) = \prod \left(\frac{N}{p_i}\right)^{\alpha_i} \prod \left(\frac{N}{p_i}\right)^{\beta_i} = \prod \left(\frac{N}{p_i}\right)^{\alpha_i+\beta_i} = \left(\frac{N}{QQ'}\right).$$

b) Segue diretamente da multiplicatividade do símbolo de Legendre:

$$\left(\frac{NN'}{Q}\right) = \prod \left(\frac{NN'}{p_i}\right)^{\alpha_i} = \prod \left[\left(\frac{N}{p_i}\right)\left(\frac{N'}{p_i}\right)\right]^{\alpha_i} = \left(\frac{N}{Q}\right)\left(\frac{N'}{Q}\right).$$

c) Segue de (a) e (b).

d) Segue dos itens (a), (b) e (c).

e) Se $N' \equiv N \pmod{Q}$, então $N' \equiv N \pmod{p_i}$ para cada fator $p_i \mid Q$. Logo $\left(\frac{N'}{p_i}\right) = \left(\frac{N}{p_i}\right)$ para todo i, implicando $\left(\frac{N'}{Q}\right) = \left(\frac{N}{Q}\right)$.

□

Lema 81. *Sejam a, b números ímpares.*

a) $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2$

b) $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} \pmod 2$

Demonstração. a) A congruência equivale a $\frac{a-1}{2} + \frac{b-1}{2} - \frac{ab-1}{2} \equiv 0 \pmod 2 \iff \frac{(a-1)(b-1)}{2} \equiv 0 \pmod 2 \iff (a-1)(b-1) \equiv 0 \pmod 4$, o que é verdade pois $a-1$ e $b-1$ são múltiplos de 2.

b) De maneira semelhante, precisamos que $(a^2-1)(b^2-1) \equiv 0 \pmod{16}$, o que vale pois $x^2 \equiv 1 \pmod 8$ para todo x ímpar.

□

Proposição 82. *Se Q é um inteiro ímpar positivo:*

a) $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$

b) $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$

Demonstração. Aplica-se indução na quantidade de fatores primos de Q usando os resultados do lema anterior.

$$\left(\frac{-1}{Q}\right) = \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)^{\alpha_i} = (-1)^{\sum \alpha_i \frac{p_i-1}{2}} = (-1)^{\frac{Q-1}{2}}.$$

O item (b) segue de forma análoga. □

4.7.2 Lei da Reciprocidade Quadrática para o Símbolo de Jacobi

Teorema 83. *Sejam N, Q inteiros ímpares positivos com* $\text{mdc}(N,Q) = 1$. *Então:*

$$\left(\frac{N}{Q}\right)\left(\frac{Q}{N}\right) = (-1)^{\frac{N-1}{2}\cdot\frac{Q-1}{2}}.$$

Demonstração. Escreva $N = \prod_{i=1}^{k} p_i^{\alpha_i}$ e $Q = \prod_{j=1}^{l} q_j^{\beta_j}$.

$$\left(\frac{N}{Q}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}, \quad \left(\frac{Q}{N}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}$$

$$\implies \left(\frac{N}{Q}\right)\left(\frac{Q}{N}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right]^{\alpha_i\beta_j} = (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{l}\alpha_i\beta_j\frac{p_i-1}{2}\frac{q_j-1}{2}}.$$

Como $\sum \alpha_i \frac{p_i-1}{2} \equiv \frac{N-1}{2} \pmod 2$ e $\sum \beta_j \frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2$, concluímos que:

$$\left(\frac{N}{Q}\right)\left(\frac{Q}{N}\right) = (-1)^{\frac{N-1}{2}\cdot\frac{Q-1}{2}}.$$

□

Exemplo. Calcular $\left(\frac{105}{317}\right)$.

- **Apenas com Legendre:**

$$\left(\frac{105}{317}\right) = \left(\frac{3}{317}\right)\left(\frac{5}{317}\right)\left(\frac{7}{317}\right)$$

$\left(\frac{3}{317}\right) = \left(\frac{317}{3}\right) = \left(\frac{2}{3}\right) = -1$
$\left(\frac{5}{317}\right) = \left(\frac{317}{5}\right) = \left(\frac{2}{5}\right) = -1$
$\left(\frac{7}{317}\right) = \left(\frac{317}{7}\right) = \left(\frac{2}{7}\right) = 1$
Logo, $\left(\frac{105}{317}\right) = (-1)(-1)(1) = 1$.

- **Usando o Símbolo de Jacobi:** Como $317 \equiv 1 \pmod 4$:

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right).$$

Como $105 \equiv 1 \pmod 8$, temos $\left(\frac{2}{105}\right) = 1$.

4.8 O Menor Resíduo Não-Quadrático

Pergunta: Ao considerar a sequência $1, 2, 3, \ldots, p-1$, "quanto tempo" demora para aparecer o primeiro resíduo não-quadrático módulo um primo p?

Teorema 84. *Seja p um primo ímpar e n_p o menor inteiro positivo que é resíduo não-quadrático módulo p. Então:*

$$n_p < 1 + \sqrt{p}.$$

Nota Histórica: Resultados mais avançados (Burgess, 1957) mostram que, para todo $\theta > \frac{1}{4\sqrt{e}} \approx 0{,}1516$, existe $C = C(\theta) > 0$ tal que $n_p < C \cdot p^\theta$.

Demonstração do Teorema. Seja $n = n_p$ o menor resíduo não-quadrático módulo p. Seja m o menor inteiro tal que $mn > p$.

Por construção, $(m-1)n \leq p$; como p é primo e $1 < n < p$, $(m-1)n \neq p$. Logo:

$$(m-1)n < p < mn \implies 0 < mn - p < n.$$

Como $mn - p < n$ e n é o **menor** resíduo não-quadrático, o número $mn - p$ deve ser um resíduo quadrático módulo p:

$$\left(\frac{mn-p}{p}\right) = 1 \implies \left(\frac{mn}{p}\right) = 1 \implies \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 1.$$

Como por definição $\left(\frac{n}{p}\right) = -1$, devemos ter $\left(\frac{m}{p}\right) = -1$.

Dado que n é o menor resíduo não-quadrático e $\left(\frac{m}{p}\right) = -1$, segue que $m \geq n$. Portanto:

$$(n-1)n \leq (m-1)n < p \implies (n-1)^2 < n(n-1) < p$$
$$\implies n - 1 < \sqrt{p} \implies n < 1 + \sqrt{p}.$$

□

Capítulo 5

Funções Aritméticas

5.1 Definição e Exemplos Iniciais

Definição. Uma **função aritmética** é qualquer função $f : \mathbb{Z}_{>0} \to \mathbb{C}$.

Exemplos Iniciais:

- **Função Constante:** $f(n) = c$ para todo $n \in \mathbb{Z}_{>0}$, onde $c \in \mathbb{C}$.
- **Função Identidade:** $f(n) = n$ para todo $n \in \mathbb{Z}_{>0}$.
- **Número de Divisores Positivos:** $d(n) = \#\{d \in \mathbb{Z}_{>0} : d \mid n\}$.

5.2 Função Parte Inteira

Definição. Dado $x \in \mathbb{R}$, a **função parte inteira** (ou função piso), denotada por $\lfloor x \rfloor$, é o maior inteiro menor ou igual a x. Equivalentemente, $\lfloor x \rfloor$ é o único inteiro tal que:

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Proposição 85 (Propriedades da Função Parte Inteira)**.** *Sejam $x, y \in \mathbb{R}$.*

a) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \iff x - 1 < \lfloor x \rfloor \leq x \iff 0 \leq x - \lfloor x \rfloor < 1$.

b) Se $x \geq 0$, então $\lfloor x \rfloor = \#\{i \in \mathbb{Z} : 1 \leq i \leq x\}$.

c) Se $m \in \mathbb{Z}$, então $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

d) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.

e) Se $x \in \mathbb{Z}$, então $\lfloor -x \rfloor = -\lfloor x \rfloor$.

f) Se $x \notin \mathbb{Z}$, então $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$.

g) Se $m \in \mathbb{Z}_{>0}$, então $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$.

h) $\left\lfloor x + \frac{1}{2} \right\rfloor$ é o inteiro mais próximo de x. Caso existam dois inteiros igualmente próximos, este é o maior deles.

i) $-\left\lfloor -x+\frac{1}{2}\right\rfloor$ *é o inteiro mais próximo de* x*. Caso existam dois inteiros igualmente próximos, este é o menor deles.*

j) Se $x \geq 0$ *e* $m \in \mathbb{Z}_{>0}$*,* $\left\lfloor \frac{x}{m} \right\rfloor$ *representa o número de inteiros positivos* $\leq x$ *divisíveis por* m*.*

Demonstrações Selecionadas. • **Demonstração da propriedade (d):** Somando as desigualdades $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ e $\lfloor y \rfloor \leq y < \lfloor y \rfloor + 1$, obtemos:

$$\lfloor x \rfloor + \lfloor y \rfloor \leq x + y < (\lfloor x \rfloor + \lfloor y \rfloor) + 2.$$

Como $\lfloor x + y \rfloor$ é o maior inteiro menor ou igual a $x + y$, segue que $\lfloor x + y \rfloor$ só pode assumir os valores $\lfloor x \rfloor + \lfloor y \rfloor$ ou $\lfloor x \rfloor + \lfloor y \rfloor + 1$.

Exemplos:

- $\lfloor 1{,}2 + 2{,}3 \rfloor = \lfloor 3{,}5 \rfloor = 3 = \lfloor 1{,}2 \rfloor + \lfloor 2{,}3 \rfloor$
- $\lfloor 3{,}7 + 4{,}8 \rfloor = \lfloor 8{,}5 \rfloor = 8 = \lfloor 3{,}7 \rfloor + \lfloor 4{,}8 \rfloor + 1$

- **Demonstração da propriedade (f):** Se $x \notin \mathbb{Z}$, então $\lfloor x \rfloor < x < \lfloor x \rfloor + 1$. Multiplicando por -1:
$$-\lfloor x \rfloor - 1 < -x < -\lfloor x \rfloor.$$
Pela definição da parte inteira, $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$.

- **Demonstração da propriedade (g):** Da desigualdade $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, dividindo por $m > 0$:
$$\frac{\lfloor x \rfloor}{m} \leq \frac{x}{m} < \frac{\lfloor x \rfloor + 1}{m} \quad (*).$$
Pelo Algoritmo da Divisão, existem inteiros q, r tais que $\lfloor x \rfloor = mq + r$, com $0 \leq r \leq m - 1$. Assim:
$$\frac{\lfloor x \rfloor}{m} = q + \frac{r}{m} \quad \text{e} \quad \frac{\lfloor x \rfloor + 1}{m} = q + \frac{r+1}{m} \leq q + 1.$$
Substituindo em $(*)$, temos $q \leq \frac{\lfloor x \rfloor}{m} \leq \frac{x}{m} < q + 1$, o que implica $\left\lfloor \frac{x}{m} \right\rfloor = q = \left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor$. □

5.2.1 Aplicação: Maior Potência de um Primo p que Divide $n!$ (Fórmula de Legendre)

Exemplo Prático: Escrever $20! = 2^k \cdot m$, onde m é um número ímpar. Qual o valor de k?

Para contar o total de fatores 2 no produto $20! = 1 \cdot 2 \cdot 3 \cdots 20$:

- Quantidade de inteiros ≤ 20 múltiplos de 2: $\left\lfloor \frac{20}{2} \right\rfloor = 10$.
- Quantidade de inteiros ≤ 20 múltiplos de $4 = 2^2$: $\left\lfloor \frac{20}{4} \right\rfloor = 5$.
- Quantidade de inteiros ≤ 20 múltiplos de $8 = 2^3$: $\left\lfloor \frac{20}{8} \right\rfloor = 2$.
- Quantidade de inteiros ≤ 20 múltiplos de $16 = 2^4$: $\left\lfloor \frac{20}{16} \right\rfloor = 1$.

Somando a contribuição de cada potência:

$$k = \left\lfloor \frac{20}{2} \right\rfloor + \left\lfloor \frac{20}{4} \right\rfloor + \left\lfloor \frac{20}{8} \right\rfloor + \left\lfloor \frac{20}{16} \right\rfloor = 10 + 5 + 2 + 1 = 18.$$

Proposição 86 (Fórmula de Legendre)**.** *Seja $n \in \mathbb{Z}_{>0}$ e p um número primo. O expoente k da maior potência de p que divide $n!$ (isto é, $p^k \mid n!$ e $p^{k+1} \nmid n!$) é dado por:*

$$k = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

5.3 Outros Exemplos de Funções Aritméticas

- **Soma dos Divisores:** $\sigma(n) = \sum_{d|n} d$.
  Exemplos: $\sigma(6) = 1 + 2 + 3 + 6 = 12$; $\sigma(8) = 1 + 2 + 4 + 8 = 15$.
- **Soma das k-ésimas Potências dos Divisores:** $\sigma_k(n) = \sum_{d|n} d^k$.
- **Número de Fatores Primos Distintos:** $\omega(n) = \#\{p \text{ primo} : p \mid n\}$.
- **Número Total de Fatores Primos (com multiplicidade):** $\Omega(n)$.
  Exemplos:
  - $\omega(6) = \omega(2 \cdot 3) = 2$ e $\Omega(6) = \Omega(2 \cdot 3) = 2$.
  - $\omega(8) = \omega(2^3) = 1$ e $\Omega(8) = \Omega(2^3) = 3$.
- **Função Totiente de Euler:** $\phi(n) = \#\{1 \le k \le n : \text{mdc}(k, n) = 1\}$.
  Para a fatoração $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$:

$$\phi(n) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

5.4 Funções Multiplicativas

Definição. Uma função aritmética f é dita **multiplicativa** se:

$$f(mn) = f(m)f(n) \quad \text{sempre que } \text{mdc}(m, n) = 1.$$

Dizemos que f é **completamente multiplicativa** se $f(mn) = f(m)f(n)$ para todos $m, n \in \mathbb{Z}_{>0}$.

Proposição 87. *A função $d(n)$ (número de divisores) é multiplicativa. Ou seja, se $\text{mdc}(m, n) = 1$, então $d(mn) = d(m)d(n)$.*

Demonstração. Provaremos que existe uma bijeção entre o conjunto dos divisores de mn e o produto cartesiano dos conjuntos de divisores de m e de n:

$$\psi : \{d \in \mathbb{Z}_{>0} : d \mid mn\} \to \{e \in \mathbb{Z}_{>0} : e \mid m\} \times \{f \in \mathbb{Z}_{>0} : f \mid n\}$$

dada por $\psi(d) = (\text{mdc}(d, m), \text{mdc}(d, n))$.

- **Bem-definida:** Para $d \mid mn$, temos $\mathrm{mdc}(d,m) \mid m$ e $\mathrm{mdc}(d,n) \mid n$. Além disso, como $\mathrm{mdc}(m,n) = 1$, vale $d = \mathrm{mdc}(d,m) \cdot \mathrm{mdc}(d,n)$ (Proposição 23).
- **Injetividade:** Suponha que $\psi(d_1) = \psi(d_2)$, de modo que $(e_1, f_1) = (e_2, f_2)$, onde $e_i = \mathrm{mdc}(d_i, m)$ e $f_i = \mathrm{mdc}(d_i, n)$. Como $\mathrm{mdc}(m,n) = 1$, temos $\mathrm{mdc}(e_i, f_j) = 1$. Dado que $d = ef$, segue que $d_1 = e_1 f_1 = e_2 f_2 = d_2$.
- **Sobrejetividade:** Seja $e \mid m$ e $f \mid n$. Como $\mathrm{mdc}(m,n) = 1$, temos $\mathrm{mdc}(e,f) = 1$. Definindo $d = ef$, verificamos que $\mathrm{mdc}(d,m) = e$ e $\mathrm{mdc}(d,n) = f$.

Portanto, a aplicação é uma bijeção, o que implica:

$$\#\{d \mid mn\} = \#\{e \mid m\} \cdot \#\{f \mid n\} \implies d(mn) = d(m)d(n).$$

□

Exemplo Ilustrativo da Bijeção: Seja $m = 8$ e $n = 15$, com $\mathrm{mdc}(8,15) = 1$ e $mn = 120$.

- Divisores de 8: $\{1, 2, 4, 8\}$
- Divisores de 15: $\{1, 3, 5, 15\}$

A correspondência bijetiva $d \leftrightarrow (e, f)$ para os 16 divisores de 120 é dada por:

1	$\to$	$(1,1)$	12	$\to$	$(4,3)$
2	$\to$	$(2,1)$	15	$\to$	$(1,15)$
3	$\to$	$(1,3)$	20	$\to$	$(4,5)$
4	$\to$	$(4,1)$	24	$\to$	$(8,3)$
5	$\to$	$(1,5)$	30	$\to$	$(2,15)$
6	$\to$	$(2,3)$	40	$\to$	$(8,5)$
8	$\to$	$(8,1)$	60	$\to$	$(4,15)$
10	$\to$	$(2,5)$	120	$\to$	$(8,15)$

Proposição 88. *As funções $\sigma_k(n)$ são multiplicativas para todo $k \in \mathbb{R}$.*

Demonstração. Usando a bijeção da demonstração da Proposição 87, para m, n tais que $\mathrm{mdc}(m,n) = 1$:

$$\sigma_k(mn) = \sum_{d \mid mn} d^k = \sum_{e \mid m} \sum_{f \mid n} (ef)^k = \left(\sum_{e \mid m} e^k \right) \left(\sum_{f \mid n} f^k \right) = \sigma_k(m)\sigma_k(n).$$

□

5.4.1 Cálculo a Partir da Fatoração em Primos

Da definição segue que, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ é a decomposição em fatores primos de n:

- Se f é multiplicativa:

$$f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_k^{\alpha_k}).$$

- Se f é completamente multiplicativa:

$$f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \cdots f(p_k)^{\alpha_k}.$$

Exemplos.

1. **Função Totiente de Euler (ϕ):**

$$\phi(p^\alpha) = \#\{1 \leq n \leq p^\alpha : \text{mdc}(n, p^\alpha) = 1\} = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

   Pela propriedade multiplicativa:

$$\phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

2. **Número de Divisores Positivos ($d(n)$):**

$$d(p^\alpha) = \#\{1, p, p^2, \ldots, p^\alpha\} = \alpha+1 \implies d(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1+1)(\alpha_2+1) \cdots (\alpha_k+1).$$

3. **Soma dos Divisores Positivos ($\sigma(n)$):**

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

$$\implies \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

5.5 Convolução de Dirichlet

Definição. Sejam f e g funções aritméticas. A **convolução de Dirichlet** entre f e g, denotada por $f * g$, é a função aritmética dada por:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Notações e Identidades Especiais: Denotando a função constante $1(n) = 1$ e a função identidade $\text{id}(n) = n$:

- $d = 1 * 1 \implies d(n) = \sum_{d|n} 1$
- $\sigma = \text{id} * 1 \implies \sigma(n) = \sum_{d|n} d$
- $\text{id} = \phi * 1 \implies \sum_{d|n} \phi(d) = n$

Teorema 89. *Se f e g são funções multiplicativas, então a convolução $f * g$ também é multiplicativa.*

Demonstração. Seja $\text{mdc}(m,n)=1$. Existe uma bijeção entre os divisores $d \mid mn$ e os pares de divisores (d_1,d_2) com $d_1 \mid m$ e $d_2 \mid n$, dada por $d=d_1d_2$.

Como $\text{mdc}(m,n)=1$, temos $\text{mdc}(d_1,d_2)=1$ e $\text{mdc}\left(\frac{m}{d_1},\frac{n}{d_2}\right)=1$. Pela multiplicatividade de f e g:

$$f(d_1d_2)=f(d_1)f(d_2) \quad \text{e} \quad g\left(\frac{mn}{d_1d_2}\right)=g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right).$$

Assim:

$$\begin{aligned}(f*g)(mn) &= \sum_{d\mid mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{d_1\mid m}\sum_{d_2\mid n} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right)\\ &= \sum_{d_1\mid m}\sum_{d_2\mid n} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)\\ &= \left(\sum_{d_1\mid m} f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2\mid n} f(d_2)g\left(\frac{n}{d_2}\right)\right) = (f*g)(m)\cdot(f*g)(n).\end{aligned}$$

□

Corolário 90. *Como $1(n)=1$ e $\text{id}(n)=n$ são multiplicativas, $d=1*1$ e $\sigma=\text{id}*1$ são multiplicativas.*

Teorema 91 (Propriedades da Convolução de Dirichlet)**.** *a) **Comutatividade:** $f*g=g*f$.*

*b) **Associatividade:** $(f*g)*h=f*(g*h)$.*

*c) **Elemento Neutro:** A função $\delta(n)$ definida por*

$$\delta(n)=\begin{cases}1, & \text{se } n=1\\ 0, & \text{se } n>1\end{cases}$$

satisfaz $f*\delta=\delta*f=f$ para toda função aritmética f.

Demonstração. a) Quando d percorre os divisores de n, $d'=\frac{n}{d}$ percorre os mesmos divisores em ordem inversa. Logo, $\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right)=\sum_{d'\mid n} g(d')f\left(\frac{n}{d'}\right)=(g*f)(n)$.

b) Ambas as expressões se reduzem à soma sobre triplas de divisores:

$$((f*g)*h)(n)=(f*(g*h))(n)=\sum_{d_1d_2d_3=n} f(d_1)g(d_2)h(d_3).$$

c) $(f*\delta)(n)=\sum_{d\mid n}\delta(d)f\left(\frac{n}{d}\right)=\delta(1)f\left(\frac{n}{1}\right)+0=f(n)$.

□

5.6 Função de Möbius e Fórmula de Inversão

Definição. A **função de Möbius** $\mu : \mathbb{Z}_{>0} \to \{-1, 0, 1\}$ é definida por:

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1, \\ (-1)^k, & \text{se } n = p_1 p_2 \cdots p_k \text{ (produto de } k \text{ primos distintos)}, \\ 0, & \text{se } n \text{ é divisível por algum quadrado } p^2 \ (p \text{ primo}). \end{cases}$$

Exemplos.

- $\mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1$
- $\mu(4) = \mu(2^2) = 0$
- $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$
- $\mu(12) = \mu(2^2 \cdot 3) = 0$

Proposição 92. *A função de Möbius μ é multiplicativa.*

Demonstração. Sejam $m, n \in \mathbb{Z}_{>0}$ com $\text{mdc}(m, n) = 1$.

- Se $p^2 \mid m$ para algum primo p, então $p^2 \mid mn$, o que implica $\mu(m) = 0$ e $\mu(mn) = 0$. Logo $\mu(mn) = 0 = \mu(m)\mu(n)$. O caso $p^2 \mid n$ é análogo.
- Se m e n são livres de quadrados, escrevemos $m = p_1 \cdots p_k$ e $n = q_1 \cdots q_l$. Como $\text{mdc}(m, n) = 1$, todos os p_i e q_j são primos distintos. Portanto, $mn = p_1 \cdots p_k q_1 \cdots q_l$ é livre de quadrados com $k + l$ fatores primos:

$$\mu(mn) = (-1)^{k+l} = (-1)^k (-1)^l = \mu(m)\mu(n).$$

□

Teorema 93 (Fórmula de Inversão de Möbius)**.** *a) $\mu * 1 = \delta$, ou seja:*

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{se } n = 1 \\ 0, & \text{se } n > 1. \end{cases}$$

b) ***Inversão de Möbius:*** *Para quaisquer funções aritméticas f e g:*

$$f * 1 = g \iff g * \mu = f$$

isto é, $\sum_{d \mid n} f(d) = g(n) \iff f(n) = \sum_{d \mid n} g(d)\mu\left(\frac{n}{d}\right)$.

Demonstração. a) Como μ e 1 são multiplicativas, a convolução $\mu * 1$ é multiplicativa. Dado que δ também é multiplicativa, basta verificar a igualdade para potências de primos p^α:

- Para $n = 1$: $(\mu * 1)(1) = \mu(1) = 1 = \delta(1)$.

- Para $n = p^\alpha$ ($\alpha \geq 1$):

$$(\mu * 1)(p^\alpha) = \sum_{j=0}^{\alpha} \mu(p^j) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^\alpha)$$
$$= 1 + (-1) + 0 + \cdots + 0 = 0.$$

Como $\delta(p^\alpha) = 0$ para todo $\alpha \geq 1$, provamos que $\mu * 1 = \delta$.

b) Se $f * 1 = g$, aplicando a convolução por μ em ambos os lados:

$$(f * 1) * \mu = g * \mu \implies f * (1 * \mu) = g * \mu \implies f * \delta = g * \mu \implies f = g * \mu.$$

A implicação recíproca é análoga multiplicando por 1.

□

5.7 Inversa de Dirichlet

Definição. Dada uma função aritmética f, dizemos que g é a **inversa de Dirichlet** de f se:

$$f * g = \delta.$$

Teorema 94. *Uma função aritmética f possui inversa de Dirichlet se, e somente se, $f(1) \neq 0$.*

Teorema 95. *Se f é uma função aritmética multiplicativa, então a sua inversa de Dirichlet também é multiplicativa.*

As demonstrações destes dois teoremas ficam como exercício.

Observação. Quando consideramos funções multiplicativas, excluímos a função identicamente nula. Em particular, se f é multiplicativa, necessariamente $f(1) = 1 \neq 0$, garantindo a existência de sua inversa de Dirichlet.

5.8 Exercícios

Função parte inteira (Seção 4.1 de [NZM91])

174. (NZM, 4.1.1) Qual é a maior potência de 2 que divide 533!? A maior potência de 3? A maior potência de 6? A maior potência de 12? A maior potência de 70?

175. (NZM, 4.1.3) Para quais números reais x é verdade que

(a) $\lfloor x \rfloor + \lfloor x \rfloor = \lfloor 2x \rfloor$?

(b) $\lfloor x + 3 \rfloor = 3 + \lfloor x \rfloor$?

(c) $\lfloor x + 3 \rfloor = 3 + x$?

Funções aritméticas (Seção 4.2 de [NZM91])

176. (NZM, 4.2.5) Prove que $\prod_{d|n} d = n^{d(n)/2}$.

177. (NZM, 4.2.14) Dado qualquer inteiro positivo n, prove que existe apenas um número finito de inteiros x satisfazendo $\sigma(x) = n$.

178. (NZM, 4.2.15) Prove que se $(a, b) > 1$ então $\sigma_k(ab) < \sigma_k(a)\sigma_k(b)$ e $d(ab) < d(a)d(b)$.

179. (NZM, 4.2.25) Mostre que, para todo inteiro positivo n,

$$\sum_{\substack{a=1 \\ (a,n)=1}}^{n} (a-1, n) = d(n)\phi(n).$$

Função de Möbius e fórmula de inversão (Seção 4.3 de [NZM91])

180. (NZM, 4.3.6) Se $F(n) = \sum_{d|n} f(d)$ para todo inteiro positivo n, prove que $f(n) = \sum_{d|n} \mu(n/d)F(d)$.

181. (NZM, 4.3.7) Prove que, para todo inteiro positivo n, $\sum_{d|n} \mu(d)d(d) = (-1)^{\omega(n)}$. Analogamente, calcule $\sum_{d|n} \mu(d)\sigma(d)$.

182. (NZM, 4.3.23) Suponha que $f(n)$ seja uma função aritmética cujos valores são todos não nulos, e ponha $F(n) = \prod_{d|n} f(d)$. Mostre que

$$f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$$

para todo inteiro positivo n.

183. (NZM, 4.3.24) Mostre que $\prod_{\substack{a=1 \\ (a,n)=1}}^{n} a = n^{\phi(n)} \prod_{d|n} \left(d!/d^d\right)^{\mu(n/d)}$.

184. (NZM, 4.3.25) Dizemos que um número complexo ζ é uma raiz n-ésima da unidade se $\zeta^n = 1$. Mostre que ζ é uma raiz n-ésima da unidade se, e somente se, ζ é um dos n números $e^{2\pi ia/n}$, onde $a = 1, 2, \ldots, n$. Dizemos que ζ é uma raiz n-ésima primitiva da unidade se n é o menor inteiro positivo tal que $\zeta^n = 1$. Mostre que, entre as raízes n-ésimas da unidade, $\zeta = e^{2\pi ia/n}$ é uma raiz n-ésima primitiva se, e somente se, $(a, n) = 1$.

185. (NZM, 4.3.26) Denote por $\Phi_n(x)$ o polinômio com coeficiente líder 1 e grau $\phi(n)$ cujas raízes são as $\phi(n)$ diferentes raízes n-ésimas primitivas da unidade. Prove que $\prod_{d|n} \Phi_d(x) = x^n - 1$ para todos os números reais ou complexos x. Deduza que $\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)}$. Mostre que os coeficientes de $\Phi_n(x)$ são inteiros. Este é o polinômio ciclotômico de ordem n.

186. (NZM, 4.3.27) Seja $F(n) = \sum_{a=1}^{n} e^{2\pi ia/n}$. Mostre que $F(1) = 1$ e que $F(n) = 0$ para todo $n > 1$.

187. (NZM, 4.3.28) Mostre que, para cada inteiro positivo n, $\sum_{\substack{a=1 \\ (a,n)=1}}^{n} e^{2\pi ia/n} = \mu(n)$.

188. (NZM, 4.3.29) Seja p primo, e denote por $\Phi_{p-1}(x)$ o polinômio ciclotômico de ordem $p-1$. Mostre que g é uma solução da congruência $\Phi_{p-1}(x) \equiv 0 \pmod{p}$ se, e somente se, g é uma raiz primitiva $\pmod{p}$. Mostre também que a soma de todas as raízes primitivas $\pmod{p}$ é $\equiv \mu(p-1) \pmod{p}$.

Capítulo 6

Representação de Inteiros como Soma de Quadrados

6.1 Resultados Principais

Dado um inteiro positivo n, busca-se analisar quais números podem ser representados nas seguintes formas:

$$\begin{aligned} &n = x^2 \quad \text{(Quadrado perfeito)} \\ &n = x^2 + y^2 \\ &n = x^2 + y^2 + z^2 \\ &n = x^2 + y^2 + z^2 + w^2. \end{aligned}$$

Teorema 96 (Soma de Dois Quadrados)**.** *Seja $n \in \mathbb{Z}_{>0}$ com fatoração em primos dada por*

$$n = 2^{\alpha} p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_l^{\gamma_l}$$

onde cada $p_i \equiv 1 \pmod 4$ e cada $q_j \equiv 3 \pmod 4$.

A equação $n = x^2 + y^2$ possui solução com $x, y \in \mathbb{Z}$ se, e somente se, todos os expoentes γ_j forem pares.

Corolário 97. *Um número primo positivo p pode ser escrito como soma de dois quadrados se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$.*

Teorema 98 (Lagrange / Quatro Quadrados)**.** *Para todo inteiro $n \geq 0$, a equação $n = x^2 + y^2 + z^2 + w^2$ possui solução com $x, y, z, w \in \mathbb{Z}$.*

6.1.1 Tabela de Exemplos ($n = 1$ a 20)

$\mathbf{n}$	$\mathbf{x^2 + y^2 + z^2 + w^2}$	$\mathbf{x^2 + y^2}$ (se possível)
1	$1^2 + 0^2 + 0^2 + 0^2$	$1^2 + 0^2$
2	$1^2 + 1^2 + 0^2 + 0^2$	$1^2 + 1^2$
3	$1^2 + 1^2 + 1^2 + 0^2$	Não
4	$2^2 + 0^2 + 0^2 + 0^2$	$2^2 + 0^2$
5	$2^2 + 1^2 + 0^2 + 0^2$	$2^2 + 1^2$
6	$2^2 + 1^2 + 1^2 + 0^2$	Não
7	$2^2 + 1^2 + 1^2 + 1^2$	Não
8	$2^2 + 2^2 + 0^2 + 0^2$	$2^2 + 2^2$
9	$3^2 + 0^2 + 0^2 + 0^2$	$3^2 + 0^2$
10	$3^2 + 1^2 + 0^2 + 0^2$	$3^2 + 1^2$
11	$3^2 + 1^2 + 1^2 + 0^2$	Não
12	$2^2 + 2^2 + 2^2 + 0^2$	Não
13	$3^2 + 2^2 + 0^2 + 0^2$	$3^2 + 2^2$
14	$3^2 + 2^2 + 1^2 + 0^2$	Não
15	$3^2 + 2^2 + 1^2 + 1^2$	Não
16	$4^2 + 0^2 + 0^2 + 0^2$	$4^2 + 0^2$
17	$4^2 + 1^2 + 0^2 + 0^2$	$4^2 + 1^2$
18	$3^2 + 3^2 + 0^2 + 0^2$	$3^2 + 3^2$
19	$3^2 + 3^2 + 1^2 + 0^2$	Não
20	$4^2 + 2^2 + 0^2 + 0^2$	$4^2 + 2^2$

6.2 Demonstração do Teorema dos Dois Quadrados

Proposição 99. *Se $p \equiv 3 \pmod 4$ é um número primo, então a equação $p = x^2 + y^2$ não possui solução inteira.*

Demonstração. Suponha, por absurdo, que existam $x, y \in \mathbb{Z}$ tais que $p = x^2 + y^2$. Reduzindo módulo p:

$$x^2 + y^2 \equiv 0 \pmod p \implies x^2 \equiv -y^2 \pmod p$$

- Se $\text{mdc}(y, p) = 1$, seja y' o inverso multiplicativo de y módulo p. Multiplicando por $(y')^2$:
$$(xy')^2 \equiv -1 \pmod p \implies \left(\frac{-1}{p}\right) = 1 \implies p \equiv 1 \pmod 4$$
o que contradiz $p \equiv 3 \pmod 4$.

- Se $p \mid y$, então $p \mid (p - y^2) = x^2 \implies p \mid x$. Logo, $p^2 \mid x^2$ e $p^2 \mid y^2$, implicando $p^2 \mid (x^2 + y^2) = p \implies p^2 \mid p$, um absurdo.

□

Proposição 100 (Teorema de Fermat das Somas de Dois Quadrados)**.** *Se $p \equiv 1 \pmod 4$ é primo, então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + y^2$.*

Demonstração. Como $p \equiv 1 \pmod 4$, existe um inteiro ξ tal que $\xi^2 \equiv -1 \pmod p$.

Considere o conjunto de pares ordenados:

$$S = \{(x, y) \in \mathbb{Z}^2 : 1 \leq x \leq A,\ 1 \leq y \leq B\}$$

com $|S| = AB$. Escolha $A = B = \lfloor \sqrt{p} \rfloor + 1$. Como $A = B > \sqrt{p}$, temos $AB > p$.

Pelo Princípio da Casa dos Pombos, existem dois pares distintos (x_1, y_1), $(x_2, y_2) \in S$ tais que:

$$x_1 - \xi y_1 \equiv x_2 - \xi y_2 \pmod{p} \implies (x_1 - x_2) \equiv \xi(y_1 - y_2) \pmod{p}.$$

Defina $x = x_1 - x_2$ e $y = y_1 - y_2$. Como $(x_1, y_1) \neq (x_2, y_2)$, não temos $x = y = 0$. Além disso:

$$|x| \leq A - 1 = \lfloor \sqrt{p} \rfloor < \sqrt{p} \quad \text{e} \quad |y| \leq B - 1 = \lfloor \sqrt{p} \rfloor < \sqrt{p}.$$

Elevando ao quadrado a relação $x \equiv \xi y \pmod{p}$:

$$x^2 \equiv \xi^2 y^2 \equiv -y^2 \pmod{p} \implies x^2 + y^2 \equiv 0 \pmod{p}.$$

Como $0 < x^2 + y^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$, a única opção para que $x^2 + y^2$ seja um múltiplo de p é:

$$x^2 + y^2 = p.$$

□

Proposição 101. *Se $n = 2^\alpha p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_l^{\gamma_l}$ onde cada $p_i \equiv 1 \pmod{4}$ e cada γ_j é par, então n pode ser escrito como soma de dois quadrados.*

Demonstração. Cada fator primo pode ser escrito como soma de dois quadrados:

- $2 = 1^2 + 1^2$
- Cada $p_i = x_i^2 + y_i^2$ (pelo Teorema de Fermat)
- Cada $q_j^{\gamma_j} = (q_j^{\gamma_j/2})^2 + 0^2$ (pois γ_j é par)

Para concluir a demonstração, basta observar que o produto de dois números que são somas de dois quadrados também é uma soma de dois quadrados, graças à identidade algébrica de Brahmagupta-Fibonacci:

$$(x^2 + y^2)(z^2 + w^2) = (xz + yw)^2 + (xw - yz)^2.$$

Por indução, o produto n é uma soma de dois quadrados. □

Proposição 102. *Se $q \equiv 3 \pmod{4}$ é primo e $n \in \mathbb{Z}_{>0}$ é um múltiplo de q que se escreve como soma de dois quadrados ($n = x^2 + y^2$), então $q^2 \mid n$ e $\frac{n}{q^2}$ também se escreve como soma de dois quadrados.*

Demonstração. Como $q \mid n$, temos $x^2 + y^2 \equiv 0 \pmod{q}$. Pelo argumento da demonstração da Proposição 99, como $q \equiv 3 \pmod{4}$, essa congruência só possui solução se $q \mid x$ e $q \mid y$.

Assim, existem $x', y' \in \mathbb{Z}$ tais que $x = qx'$ e $y = qy'$. Substituindo:

$$n = (qx')^2 + (qy')^2 = q^2((x')^2 + (y')^2) \implies q^2 \mid n.$$

Dividindo por q^2:

$$\frac{n}{q^2} = (x')^2 + (y')^2$$

que é uma soma de dois quadrados. □

Conclusão da demonstração do Teorema dos Dois Quadrados. Se todos os γ_j são pares, n é soma de dois quadrados pela Proposição 101. Reciprocamente, se $n = x^2 + y^2$ e $q \equiv 3 \pmod{4}$ divide n, a Proposição 102 dá $q^2 \mid n$ e $\frac{n}{q^2}$ soma de dois quadrados; repetindo o argumento, o expoente de q em n é par.

6.3 Soma de Quatro Quadrados

6.3.1 Identidade dos Quatro Quadrados de Euler

Na demonstração da Proposição 101, para estudar os números que são soma de dois quadrados, utilizamos a seguinte identidade de Brahmagupta-Fibonacci:

$$(x^2+y^2)(z^2+w^2) = (xz+yw)^2 + (xw-yz)^2.$$

Para estudar os números que são soma de quatro quadrados, precisaremos de uma identidade semelhante, conhecida como **Identidade dos Quatro Quadrados de Euler**:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(r^2+s^2+t^2+u^2) = &(ar+bs+ct+du)^2\\ &+(as-br-cu+dt)^2\\ &+(at+bu-cr-ds)^2\\ &+(au-bt+cs-dr)^2.\end{aligned}$$

6.3.2 Teorema de Lagrange

Vamos agora demonstrar o Teorema de Lagrange (Teorema 98).

Demonstração. Graças à identidade de Euler, o produto de dois números que são somas de quatro quadrados também é uma soma de quatro quadrados. Portanto, basta mostrar que todo número primo p pode ser escrito como soma de quatro quadrados. Como $2 = 1^2+1^2+0^2+0^2$, podemos supor p ímpar.

Passo 1: Solubilidade da congruência módulo p

Primeiramente, provaremos que para qualquer primo p, existem $a, b, c, d \in \mathbb{Z}$, não todos nulos módulo p, tais que:

$$a^2+b^2+c^2+d^2 \equiv 0 \pmod{p}$$

- Se $p = 2$, basta tomar $a = 1, b = 1, c = 0, d = 0$, pois $1^2+1^2+0^2+0^2 = 2 \equiv 0 \pmod 2$.
- Se $p \equiv 1 \pmod 4$, pela Proposição 100, a congruência $a^2+b^2 \equiv 0 \pmod p$ possui solução não trivial, logo basta tomar $c = d = 0$.
- Se $p \equiv 3 \pmod 4$, mostremos que existe solução para $a^2+b^2+1^2+0^2 \equiv 0 \pmod p$. Seja t o menor inteiro positivo que é não-resíduo quadrático módulo p. Como $\left(\frac{-1}{p}\right) = -1$, existe $b \in \mathbb{Z}$ tal que $t \equiv -b^2 \pmod p$. Como t é o *menor* não-resíduo quadrático, $t-1$ deve ser um resíduo quadrático módulo p. Logo, existe $a \in \mathbb{Z}$ tal que $t-1 \equiv a^2 \pmod p$. Juntando as duas congruências:

$$a^2 \equiv t-1 \equiv -b^2-1 \pmod p \implies a^2+b^2+1^2+0^2 \equiv 0 \pmod p.$$

Passo 2: Delimitação de um múltiplo de p

Concluímos que para todo primo p, existem $a, b, c, d \in \mathbb{Z}$ não todos nulos tais que $p \mid (a^2+b^2+c^2+d^2)$. Trocando $x \in \{a, b, c, d\}$ por seu resto de menor valor absoluto em relação a p, podemos supor que:

$$-\frac{p}{2} < a, b, c, d < \frac{p}{2}.$$

Assim, temos:

$$a^2 + b^2 + c^2 + d^2 < 4 \cdot \left(\frac{p}{2}\right)^2 = p^2.$$

Como a, b, c, d não são todos nulos mod p, temos $a^2 + b^2 + c^2 + d^2 = kp$ com $0 < k < p$.

Passo 3: Método da Descida (Minimalidade)

Seja m o menor inteiro positivo tal que mp é soma de quatro quadrados:

$$mp = a^2 + b^2 + c^2 + d^2.$$

Queremos mostrar que $m = 1$. Suponha, por absurdo, que $m > 1$.

- **Caso 1: m é ímpar.** Escolha a_1, b_1, c_1, d_1 tais que:

$$a_1 \equiv a, \quad b_1 \equiv b, \quad c_1 \equiv c, \quad d_1 \equiv d \pmod{m}$$

com $-\frac{m}{2} < a_1, b_1, c_1, d_1 < \frac{m}{2}$. Então:

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}.$$

Logo, $a_1^2+b_1^2+c_1^2+d_1^2 = mm'$, onde $0 \leq m' < m$. Se $m' = 0$, teríamos $a_1 = b_1 = c_1 = d_1 = 0$, o que implicaria $m \mid a, b, c, d$ e portanto $m^2 \mid (a^2 + b^2 + c^2 + d^2) = mp \implies m \mid p$, um absurdo pois $1 < m < p$ ($m < p$ pelo Passo 2). Logo, $0 < m' < m$.

Pela Identidade dos Quatro Quadrados de Euler:

$$(mp)(mm') = m^2m'p = a_2^2 + b_2^2 + c_2^2 + d_2^2$$

onde a_2, b_2, c_2, d_2 são dados pelas fórmulas da identidade. Verificando módulo m:

$$\begin{aligned}
a_2 &= aa_1 + bb_1 + cc_1 + dd_1 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m} \\
b_2 &= ab_1 - ba_1 - cd_1 + dc_1 \equiv ab - ba - cd + dc = 0 \pmod{m} \\
c_2 &= ac_1 + bd_1 - ca_1 - db_1 \equiv ac + bd - ca - db = 0 \pmod{m} \\
d_2 &= ad_1 - bc_1 + cb_1 - da_1 \equiv ad - bc + cb - da = 0 \pmod{m}.
\end{aligned}$$

Logo, podemos escrever $a_2 = ma_3$, $b_2 = mb_3$, $c_2 = mc_3$ e $d_2 = md_3$. Substituindo:

$$m^2m'p = m^2(a_3^2 + b_3^2 + c_3^2 + d_3^2) \implies m'p = a_3^2 + b_3^2 + c_3^2 + d_3^2.$$

Como $0 < m' < m$, isto contradiz a minimalidade de m.

- **Caso 2: m é par.** Se m é par, então $mp = a^2 + b^2 + c^2 + d^2$ é par. Analisando a paridade de a, b, c, d, há apenas três possibilidades: todos pares, todos ímpares, ou dois pares e dois ímpares. Em todos os casos, reordenando se necessário, podemos supor que $a \equiv b \pmod 2$ e $c \equiv d \pmod 2$. Isso implica que $\frac{a+b}{2}, \frac{a-b}{2}, \frac{c+d}{2}, \frac{c-d}{2} \in \mathbb{Z}$.

Observe que:

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{a^2 + b^2 + c^2 + d^2}{2} = \frac{m}{2}p$$

obtendo uma representação para $\frac{m}{2}p$ como soma de quatro quadrados, o que contradiz a minimalidade de m.

Portanto, $m = 1$, provando que p é soma de quatro quadrados para todo primo p. $\square$

6.4 Número de Representações como Soma de Dois Quadrados

Teorema 103 (Número de Representações como Soma de Dois Quadrados)**.** *Seja $n \in \mathbb{Z}_{>0}$ com fatoração em primos dada por:*

$$n = 2^{\alpha} p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_l^{\gamma_l}$$

onde $p_i \equiv 1 \pmod 4$ e $q_j \equiv 3 \pmod 4$ (com cada γ_j par).

Se $r(n)$ denota o número de maneiras de escrever n como soma de dois quadrados (isto é, $r(n) = \#\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 = n\}$), então:

$$r(n) = 4(\beta_1 + 1)(\beta_2 + 1) \cdots (\beta_k + 1).$$

Equivalentemente:

$$r(n) = 4 \cdot \#\{d \mid n : p \mid d \implies p \equiv 1 \pmod 4\}.$$

Em particular, a função $\frac{r(n)}{4}$ é multiplicativa.

6.4.1 Recapitulação e Objetivo

Nas seções anteriores, estabelecemos a caracterização dos números representáveis como soma de dois quadrados e quatro quadrados:

- $n = x^2 + y^2 \iff n = 2^{\alpha} p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_l^{\gamma_l}$, onde $p_i \equiv 1 \pmod 4$, $q_j \equiv 3 \pmod 4$ e cada γ_j é par.
- $n = x^2 + y^2 + z^2 + w^2$ para todo $n \in \mathbb{Z}_{\geq 0}$ (Teorema de Lagrange).

Também demonstramos o lema auxiliar: se $p \equiv 3 \pmod 4$ e $p \mid (x^2 + y^2)$, então $p \mid x$ e $p \mid y$, implicando que $p^2 \mid (x^2 + y^2)$.

Objetivo principal desta seção: Demonstrar que o número de soluções inteiras $(x, y) \in \mathbb{Z}^2$ para a equação $x^2 + y^2 = n$, denotado por $r(n)$, é dado por:

$$r(n) = \#\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 = n\} = 4 \prod_{i=1}^{k} (\beta_i + 1).$$

6.4.2 Proposições Auxiliares

Proposição 104. *Se $p = a^2 + b^2$ é um primo com $p \equiv 1 \pmod 4$ e $py = c^2 + d^2$ com $\mathrm{mdc}(c,d) = 1$, então existem $e, f \in \mathbb{Z}$ tais que $\mathrm{mdc}(e,f) = 1$ e $y = e^2 + f^2$.*

Demonstração. Como p é primo, temos $\mathrm{mdc}(a,b) = 1$ (caso contrário, $g^2 \mid p$ para algum $g > 1$, o que é impossível).

Considere a seguinte identidade algébrica:

$$a^2 py - c^2 p = a^2(c^2 + d^2) - c^2(a^2 + b^2) = a^2 d^2 - b^2 c^2 = (ad - bc)(ad + bc).$$

Logo, $p \mid (ad - bc)(ad + bc)$. Assim, $p \mid (ad - bc)$ ou $p \mid (ad + bc)$. Sem perda de generalidade, suponha que $p \mid (ad - bc)$ (o outro caso é análogo).

Observe que:

$$p \mid (ad - bc) \implies p \mid (a^2d - abc).$$

Como $a^2 \equiv -b^2 \pmod{p}$, temos:

$$a^2d - abc \equiv -b^2d - abc = -b(bd + ac) \pmod{p}.$$

Como $p \nmid b$ (pois $p = a^2 + b^2$ é primo), conclui-se que $p \mid (bd + ac)$.

Defina $e, f \in \mathbb{Z}$ por:

$$e = \frac{ad - bc}{p} \quad \text{e} \quad f = \frac{bd + ac}{p}.$$

Verificando a soma dos quadrados:

$$e^2 + f^2 = \frac{(ad - bc)^2 + (bd + ac)^2}{p^2} = \frac{(a^2 + b^2)(c^2 + d^2)}{p^2} = \frac{p \cdot (py)}{p^2} = y.$$

Para mostrar que $\text{mdc}(e, f) = 1$, note que:

$$ae + bf = a\left(\frac{ad - bc}{p}\right) + b\left(\frac{bd + ac}{p}\right) = \frac{(a^2 + b^2)d}{p} = d$$

$$af - be = a\left(\frac{bd + ac}{p}\right) - b\left(\frac{ad - bc}{p}\right) = \frac{(a^2 + b^2)c}{p} = c.$$

Se existisse $g = \text{mdc}(e, f) > 1$, então $g \mid (ae + bf) = d$ e $g \mid (af - be) = c$, o que implicaria $\text{mdc}(c, d) \geq g > 1$, contradizendo a hipótese $\text{mdc}(c, d) = 1$. Logo, $\text{mdc}(e, f) = 1$. □

Proposição 105. *Se $m = c^2 + d^2$ com $\text{mdc}(c, d) = 1$, então m não possui nenhum fator primo $q \equiv 3 \pmod{4}$.*

Demonstração. Suponha, por absurdo, que exista um primo $q \mid m$ tal que $q \equiv 3 \pmod{4}$. Como $m = c^2 + d^2$, temos $c^2 + d^2 \equiv 0 \pmod{q}$. Conforme a demonstração da Proposição 99, para primos $q \equiv 3 \pmod{4}$, essa congruência implica que $q \mid c$ e $q \mid d$. Consequentemente, $q \mid \text{mdc}(c, d)$, o que contradiz $\text{mdc}(c, d) = 1$. Portanto, todos os fatores primos de m devem ser 2 ou da forma $4k + 1$. □

6.4.3 Unicidade da Representação de Primos

Teorema 106 (Unicidade)**.** *Se $p \equiv 1 \pmod{4}$ é primo, então existe uma única maneira de escrever $p = a^2 + b^2$ com $a, b > 0$, onde a é ímpar e b é par.*

Demonstração. Suponha que existam duas representações:

$$p = a^2 + b^2 = c^2 + d^2$$

com $a, c > 0$ ímpares e $b, d > 0$ pares. Reorganizando os termos:

$$a^2 - c^2 = d^2 - b^2 \implies (a + c)(a - c) = (d - b)(d + b).$$

Assuma, sem perda de generalidade, que $a > c$ (o caso $a = c$ implica $b = d$, obtendo a unicidade).

Seja $m = \text{mdc}(a - c, d - b)$ e $n = \text{mdc}(a + c, d + b)$. Podemos escrever:

$$a - c = rm, \quad d - b = sm, \quad \text{com } \text{mdc}(r, s) = 1$$

$$a + c = un, \quad d + b = vn, \quad \text{com } \operatorname{mdc}(u, v) = 1.$$

Substituindo na igualdade $(a + c)(a - c) = (d - b)(d + b)$:

$$(un)(rm) = (sm)(vn) \implies ur = sv.$$

Como $\operatorname{mdc}(r, s) = 1$ e $\operatorname{mdc}(u, v) = 1$, deduz-se que $r = v$ e $u = s$. Isso nos permite isolar a, b, c, d em termos de m, n, r, s:

$$a = \frac{sn + rm}{2}, \quad c = \frac{sn - rm}{2}, \quad d = \frac{sm + rn}{2}, \quad b = \frac{rn - sm}{2}.$$

Substituindo na expressão $p = a^2 + b^2$:

$$p = \left(\frac{sn + rm}{2}\right)^2 + \left(\frac{rn - sm}{2}\right)^2 = \left(\left(\frac{m}{2}\right)^2 + \left(\frac{n}{2}\right)^2\right)\left(r^2 + s^2\right).$$

Como a e c são ímpares e b e d são pares, os números $a \pm c$ e $d \pm b$ são pares; logo m e n são pares e os dois fatores acima são inteiros. Além disso, como $a > c > 0$ e $d > b > 0$, temos $r, s \geq 1$ e $m, n \geq 2$, de modo que ambos os fatores são estritamente maiores que 1. Isso fatoraria o número primo p como produto de dois inteiros maiores que 1, o que é uma contradição. Portanto, a representação de p como soma de dois quadrados é única a menos da ordem e dos sinais dos termos. □

6.4.4 Fórmula para o Número de Soluções $r(n)$

Exercício 189. Demonstrar que o número de soluções de $x^2 + y^2 = n$ em inteiros $\mathbb{Z}^2$ é dado por:

$$r(n) = 4\prod_{i=1}^{k}(\beta_i + 1)$$

onde $n = 2^\alpha p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_l^{\gamma_l}$ com $p_i \equiv 1 \pmod 4$ e cada γ_j par.

Roteiro de resolução:

1. Provar o resultado para potências de números primos:
   - $r(2^\alpha) = 4$ para todo $\alpha \geq 0$.
   - $r(p^\beta) = 4(\beta + 1)$ para primos $p \equiv 1 \pmod 4$.
   - $r(q^\gamma) = 4$ se γ for par e $r(q^\gamma) = 0$ se γ for ímpar, para primos $q \equiv 3 \pmod 4$.
2. Demonstrar que a função $f(n) = \frac{r(n)}{4}$ é multiplicativa, reduzindo ao caso em que n possui apenas fatores primos da forma $4k + 1$.

6.5 Exercícios

Ternas pitagóricas (Seção 5.3 de [NZM91])

190. (NZM, 5.3.1) Encontre todas as ternas pitagóricas primitivas para as quais $0 < z < 30$.

191. (NZM, 5.3.2) Prove que se x, y, z é uma terna pitagórica, então pelo menos um entre x, y é divisível por 3, e pelo menos um entre x, y, z é divisível por 5.

192. (NZM, 5.3.4) Sejam u e v inteiros positivos cujo produto uv é um quadrado perfeito, e seja $g = (u, v)$. Mostre que existem inteiros positivos r, s tais que $u = gr^2$ e $v = gs^2$.

193. (NZM, 5.3.11) Usando [NZM91, Teorema 5.5], determine todas as soluções da equação $x^2 + y^2 = 2z^2$.

194. (NZM, 5.3.17) Usando a demonstração de [NZM91, Teorema 5.5] como modelo, mostre que se x e y são inteiros para os quais $x^4 - 2y^2 = 1$, então $x = \pm 1, y = 0$.

Equações diofantinas diversas (Seção 5.4 de [NZM91])

195. (NZM, 5.4.1) Mostre que a equação $x^2 + y^2 = 9z + 3$ não tem solução inteira.

196. (NZM, 5.4.2) Mostre que a equação $x^2 + 2y^2 = 8z + 5$ não tem solução inteira.

197. (NZM, 5.4.11) Seja $F(x) = (x^2 - 17)(x^2 - 19)(x^2 - 323)$. Mostre que, para todo inteiro m, a congruência $F(x) \equiv 0 \pmod{m}$ tem solução. Observe que a equação $F(x) = 0$ não tem solução inteira, nem mesmo qualquer solução racional.

198. (NZM, 5.4.14) Construa um argumento de descida que relacione as duas equações $x^4 + 4y^4 = z^2, a^4 + b^2 = c^4$. Deduza que nenhuma dessas equações tem solução em inteiros positivos.

Bibliografia

[Gre24] Great Internet Mersenne Prime Search: *GIMPS discovers largest known prime number:* $2^{136279841} - 1$. https://www.mersenne.org, 2024. Comunicado de 21 de outubro de 2024.

[NZM91] Niven, Ivan, Herbert S. Zuckerman e Hugh L. Montgomery: *An introduction to the theory of numbers*. John Wiley & Sons, 1991.

[San98] Santos, José Plínio de Oliveira: *Introdução à teoria dos números*. Coleção Matemática Universitária. IMPA, Rio de Janeiro, 1998.