# Sumário

# Capítulo 1

# Divisibilidade

**Definição 1.1** (Divisibilidade)
Dados dois inteiros $a$ e $b$, dizemos que $a$ divide $b$ (neste caso, escrevemos $a \mid b$) se, e somente se, existe um inteiro $c$ tal que $b = ac$. Neste caso, dizemos que $a$ é um divisor de $b$ e que $b$ é um múltiplo de $a$.

**Teorema 1.2** (Divisão Euclidiana)
Dado um inteiro $n$ e um inteiro positivo $d$, existem únicos inteiros $q, r$, com $0 \leq r < d$ tais que

$$n = qd + r.$$

**Exercício 1.1**
Demonstre o Teorema 1.2.

**Definição 1.3** (Maior Divisor Comum e Menor Múltiplo Comum)
Dados inteiros (não todos nulos) $a_1, a_2, \ldots, a_n$, chamamos de *maior divisor comum de* $a_1, a_2, \ldots, a_n$ o maior inteiro positivo $d$ tal que $d \mid a_i$, para todo $i \in \{1, 2, \ldots, n\}$. É comum denotarmos esse número por $\text{mdc}(a_1, a_2, \ldots, a_n)$ ou $(a_1, a_2, \ldots, a_n)$.

Chamamos de *menor múltiplo comum de* $a_1, a_2, \ldots, a_n$ o menor inteiro positivo $m$ tal que $a_i \mid m$, para todo $i \in \{1, 2, \ldots, n\}$. É comum denotarmos esse número por $\text{mmc}(a_1, a_2, \ldots, a_n)$.

**Definição 1.4** (Coprimos)
Dizemos que $a$ e $b$ são *coprimos* (ou *primos entre si*) se, e somente se, $(a, b) = 1$.

**Teorema 1.5** (Teorema Útil)
Dados $a, b, k$ inteiros, vale

$$(a, b) = (a, b + ka).$$

**Corolário 1.6**
Dados $a$ inteiro positivo e $b$ inteiro, seja $b = qa + r$ a divisão euclidiana de $b$ por $a$. Então,

$$(a, b) = (a, r).$$

**Exercício 1.2**
Demonstre o Teorema 1.5.

**Teorema 1.7** (Bezout)
Dados inteiros $a, b$, o menor inteiro positivo que pode ser escrito da forma $ra + sb$, com $r, s$ inteiros, é $(a, b)$.

**Corolário 1.8**
Dados inteiros $a, b$, o conjunto
$$\{ra + sb : r, s \in \mathbb{Z}\}$$
é o conjunto dos múltiplos de $(a, b)$.

**Algoritmo 1.9** (Algoritmo de Euclides)

**Definição 1.10** (Número Primo)
Um inteiro $p$ é *primo* se, e somente se, $p$ possui exatamente dois divisores positivos distintos[a].

[a] Esses divisores são 1 e $p$. Note que 1 não é primo, pois possui somente um divisor positivo.

**Lema 1.11**
Dados inteiros $a, b$ e um primo $p$,
$$p \mid ab \iff p \mid a \text{ ou } p \mid b.$$

**Exercício 1.3**
Demonstre o Lema 1.11.

**Teorema 1.12** (Teorema Fundamental da Aritmética)
Dado um inteiro positivo $n > 1$, existem únicos primos $p_1,\ p_2,\ \ldots,\ p_k$ e inteiros positivos $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k$ tais que
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

## 1.1 Problemas Interessantes

**Problema 1.4** (Andrei Neguț, Problems for the Mathematical Olympiads, N2)
Sejam $x$ e $y$ inteiros positivos tais que $3x^2 + x = 4y^2 + y$. Prove que $x - y$ é um quadrado perfeito.

# Capítulo 2

# Congruência módulo $n$

**Definição 2.1** (Relação de Equivalência)
Dado um conjunto $S$ e uma relação $\sim$ sobre $S$, dizemos que a relação $\sim$ é uma *relação de equivalência* se, e somente se, valem as seguintes propriedades:

– *Reflexidade:* para todo $a \in S$,
$$a \sim a.$$

– *Simetria:* para todos $a, b \in S$,
$$a \sim b \iff b \sim a.$$

– *Transitividade:* para todos $a, b, c \in S$,
$$a \sim b \text{ e } b \sim c \implies a \sim c.$$

**Definição 2.2** (Congruência módulo $n$)
Dado um inteiro positivo $n$, definimos a relação $\equiv \pmod{n}$ sobre $\mathbb{Z}$, definida por: para todo $a, b$,
$$a \equiv b \pmod{n} \iff n \mid a - b.$$

Neste caso, dizemos que $a$ é congruente a $b$ módulo $n$.

**Exercício 2.1**
Demonstre que a congruência módulo $n$ é uma relação de equivalência.

**Teorema 2.3** (Teorema Chinês dos Restos)
Seja $r$ um inteiro positivo qualquer. Sejam $m_1, m_2, m_3, \ldots, m_r$ inteiros positivos coprimos dois a dois e sejam $a_1, a_2, \ldots, a_r$ inteiros quaisquer. Então, o sistema de congruências
$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$
é equivalente a
$$x \equiv A \pmod{M},$$
para algum inteiro $A$ e para $M = m_1 m_2 \cdots m_r$.

**Exercício 2.2**

Demonstre o Teorema Chinês dos Restos.

(a) Demonstre para $r = 2$.

(b) Demonstre para $r$ qualquer usando indução.

**Pergunta 2.3**

Quantos elementos dentre

$$\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$$

possuem denominador $d$, quando escritos de forma simplificada[a]?

[a] escrever um racional de forma simplificada significa escrevê-lo como $p/q$, onde $p$ e $q$ são coprimos.

**Definição 2.4** (Função $\phi$ de Euler)

Dado um inteiro positivo $n$, definimos

$$\phi(n) = |\{x \in \mathbb{Z} : (x, n) = 1 \text{ e } 0 < x \leq n\}|,$$

ou seja, $\phi(n)$ é o número de inteiros positivos menores ou iguais a $n$ que são coprimos com $n$.

**Exercício 2.4**

Demonstre que

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

**Lema 2.5**

A função $\phi$ é multiplicativa, isto é, para quaisquer inteiros positivos $m, n$ coprimos,

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

**Lema 2.6**

Dados $p$ primo e $k$ inteiro positivo,

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

**Exercício 2.5**

Demonstre os Lemas 2.5 e 2.6 e caracterize $\phi(n)$ para $n$ inteiro positivo qualquer.

**Teorema 2.7** (Pequeno Teorema de Fermat)

Dados um inteiro $a$ e um primo $p$,

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

Alternativamente, dados inteiros $a$ e primo $p$, com $a$ e $p$ coprimos (isto é, $p$ não divide $a$),

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

**Teorema 2.8** (Teorema de Euler)
Dado um inteiro $a$ e um inteiro positivo $n$, com $a, n$ coprimos,

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

O Teorema de Euler mostra que a sequência $a^0, a^1, a^2, a^3 \ldots \pmod{n}$ é periódica, e que ela volta pro 1 em $a^{\phi(n)}$. Talvez essa não seja a primeira vez que isso aconteça, mas com certeza existe alguma primeira vez que isso acontece!

**Definição 2.9** (Ordem)
Dados inteiros $a, n$ coprimos, o menor inteiro positivo $m$ tal que $a^m \equiv 1 \pmod{n}$ é chamado de *ordem de a módulo n*. É comum denotarmos esse número por $\operatorname{ord}_n(a)$.

**Lema 2.10**
Sejam $a$ um inteiro e $x, y$ inteiros positivos. Então,

$$(a^x - 1, a^y - 1) = a^{(x,y)} - 1.$$

**Teorema 2.11**
Sejam $a, m$ inteiros e $n$ um inteiro positivo, com $a, n$ coprimos. Se $a^m \equiv 1 \pmod{n}$, então

$$\operatorname{ord}_n(a) \mid m.$$

**Corolário 2.12**
Sejam $a$ um inteiro e $n$ um inteiro positivo, com $a, n$ coprimos. Então,

$$\operatorname{ord}_n(a) \mid \phi(n).$$

## 2.1 Questões Divertidas

**Problema 2.6** (Teorema de Wilson)
Calcule
$$1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

**Problema 2.7**
Sejam $a$ e $n$ inteiros positivos. Mostre que $n$ divide $\phi(a^n - 1)$.

**Problema 2.8**
Seja $p$ um número primo e $q$ um fator primo de $p^p - 1$. Prove que $q \equiv 1 \pmod{p}$.

## 2.2 Problemas Interessantes

**Problema 2.9** (Andrei Neguț, Problems for the Mathematical Olympiads, N5)
Seja $p \geq 5$ um primo. Se
$$1 + \frac{1}{2} + \cdots + \frac{1}{p} = \frac{a}{b},$$
prove que $p^4$ divide $ap - b$.

# Capítulo 3

# Raízes Primitivas

**Definição 3.1** (Raíz primitiva)
Dizemos que $g$ é uma raíz primitiva módulo $n$ se, e somente se, $\text{ord}_n(g) = \phi(n)$.

**Lema 3.2**
$g$ é uma raíz primitiva módulo $n$ se, e somente se, para todo inteiro $a$ coprimo com $n$, existe inteiro não-negativo $k$ tal que $g^k \equiv a \pmod{n}$.

**Teorema 3.3** (Caracterização total dos $n$ que possuem raízes primitivas)
Existem raíz primitiva módulo $n$ se, e somente se, $n = 2$ ou $n = 4$ ou $n = p^k$ ou $n = 2p^k$, para $p$ primo ímpar e $k$ inteiro positivo.

**Exercício 3.1** (Versão fraca do Teorema 3.3)
Seja $p$ um primo ímpar. Prove que existe raíz primitiva módulo $p$.

**Lema 3.4**
Se existe raíz primitva módulo $n$, então existem exatamente $\phi(\phi(n))$ raízes primitivas módulo $n$.

## 3.1 Questões Divertidas

**Problema 3.2** (Teorema de Wilson)

Calcule

$$1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

**Problema 3.3**

Seja $p$ um primo ímpar e $1 \leq n < p-1$ um inteiro. Prove que

$$1^n + 2^n + \cdots + (p-1)^n$$

é divisível por $p$.

**Problema 3.4**

Seja $p$ um primo tal que $p \equiv 3 \pmod{4}$. Prove que

$$\prod_{j=1}^{p-1} \left(j^2+1\right) \equiv 4 \pmod{p}.$$

# Capítulo 4

# Resíduos Quadráticos

**Definição 4.1** (Resíduo Quadrático)
Dizemos que $a$ é *resíduo quadrático módulo $n$* se, e somente se, $x^2 \equiv a \equiv 0 \pmod{n}$ possui solução.

**Proposição 4.2**
Seja $p$ um primo ímpar. Existem exatamente $\frac{p+1}{2}$ resíduos quadráticos módulo $p$. Eles são:

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

**Definição 4.3** (Símbolo de Legendre)
Seja $p$ um primo e $a \in \mathbb{Z}$.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático} \pmod{p}, \\ -1, \text{se } p \nmid a \text{ e } a \text{ não é um resíduo quadrático} \pmod{p}, \\ 0, \text{se } p \mid a. \end{cases}$$

**Teorema 4.4** (Critério de Euler)
Sejam $p$ um primo ímpar e $a \in \mathbb{Z}$. Então

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

*Demonstração.* Se $a$ é multiplo de $p$, então

$$a^{(p-1)/2} \equiv 0 \equiv \left(\frac{a}{p}\right).$$

Se $a$ é resíduo quadrático não nulo, então existe $y$ tal que $a \equiv y^2$. Portanto,

$$a^{(p-1)/2} \equiv y^{p-1} = 1 = \left(\frac{a}{p}\right).$$

Considere o polinômio

$$P(x) = x^{p-1} - 1 = \underbrace{(x^{(p-1)/2} - 1)}_{Q(x)} \underbrace{(x^{(p-1)/2} + 1)}_{R(x)}.$$

Como $P(x)$ possui grau $p-1$, ele possui no máximo $p-1$ raízes (contando multiplicidade). Note que $1, 2, \ldots, p-1$ são raízes de $P(x)$; consequentemente, são todas as raízes de $P(x)$.

Como $Q(x)$ possui no máximo $(p-1)/2$ raízes e todos os $(p-1)/2$ resíduos quadráticos não nulos são raízes de $Q(x)$, eles são todas as raízes de $Q(x)$.

Desse modo, os não residuos quadraticos não nulos são raízes de $P(x)$, mas não de $Q(x)$, e portanto são raízes de $R(x)$. Logo, para $a$ não multiplo de $p$ e não resíduo quadrático,

$$a^{(p-1)/2} \equiv -1 = \left(\frac{a}{p}\right).$$

$\square$

**Corolário 4.5**

Sejam $p$ um primo ímpar e $a, b \in \mathbb{Z}$.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

**Corolário 4.6**

$-1$ é resíduo quadrático módulo $p$ se, e somente se, $p \equiv 1 \pmod 4$.

**Teorema 4.7** (Lei da Reciprocidade Quadrática)

Sejam $p$ e $q$ primos ímpares distintos. Temos:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, \text{ se } p \equiv 1 \text{ ou } q \equiv 1 \pmod 4 \\ -1, \text{ se } p \equiv 3 \text{ e } q \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \text{ se } p \equiv 1 \text{ ou } p \equiv 7 \pmod 8 \\ -1, \text{ se } p \equiv 3 \text{ ou } p \equiv 5 \pmod 8 \end{cases}$$

Usando os dois teoremas a seguir, podemos determinar se $a$ é resíduo quadrático módulo $n$ apenas olhando módulo as potências de 2 que dividem $n$ e módulo os primos ímpares que dividem $n$.

**Teorema 4.8**

Sejam $p$ primo ímpar e $a, k \in \mathbb{Z}$ com $k > 0$. Se $x^2 \equiv a \pmod{p^k}$, existe $t \in \{0, 1, \ldots, p-1\}$ tal que

$$(x + tp)^2 \equiv a \pmod{p^{k+1}}.$$

**Teorema 4.9**

Sejam $a$ um inteiro ímpar e $n \geq 3$. $a$ é resíduo quadrático módulo $2^n$ se, e somente se, $a \equiv 1 \pmod 8$.

## Capítulo 5

# Descenso de Fermat

**Exercício 5.1**

Sejam $a$ e $b$ inteiros positivos tais que $ab+1$ divide $a^2+b^2$. Mostre que

$$\frac{a^2+b^2}{ab+1}$$

é um quadrado perfeito.

## 5.1 Problemas Interessantes

**Problema 5.2**

Ache todos os pares de inteiros positivos $(a, b)$ tais que

$$\frac{a^2 + b^2 + 1}{ab}$$

é um inteiro.

**Problema 5.3**

Ache todos os pares de inteiros positivos $(a, b)$ tais que $a$ divide $b^2 + 1$ e $b$ divide $a^2 + 1$.

**Problema 5.4** (IMO 2007, 5)

Let $a$ and $b$ be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)^2$, then $a = b$.