

# Teoria dos Números

## Algoritmo da divisão

### Teorema

Dados dois números inteiros  $a$  e  $b$  tais que  $b \neq 0$ , existem inteiros únicos  $q$  e  $r$  tais que

$$a = bq + r \text{ e } 0 \leq r < b$$

### Corolário

Sejam  $a, b \in \mathbb{Z}$ , com  $b \neq 0$ . Então existem inteiros únicos  $q$  e  $r$  tais que  $a = bq + r$  e  $0 \leq r < |b|$ .

Para qualquer intuito  $a$  tem-se  $a = 2k$  ou  $a = 2k+1$ , para algum  $k \in \mathbb{Z}$ .

Um intuito  $a$  diz-se:

- um número par se  $a = 2k$ ,  $\forall k \in \mathbb{Z}$ ;
- um número ímpar se  $a = 2k+1$ ,  $\forall k \in \mathbb{Z}$ .

### Definição

Sejam  $a, b \in \mathbb{Z}$ . Diz-se que  $a$  divide  $b$ , e escreve-se  $a | b$ , se existe  $c \in \mathbb{Z}$  tal que  $b = ac$ .

Escrive-se  $a \nmid b$  para significar que  $a$  não divide  $b$ .

$$\rightarrow \forall_{x,y \in \mathbb{Z}} \quad x \mid y \Leftrightarrow \exists_{k \in \mathbb{Z}} \quad y = kx$$

### Teorema

Sejam  $a, b, c, d \in \mathbb{Z}$  números inteiros.

1)  $a | 0$ ,  $1 | a$  e  $a | a$

2)  $a | 1 \Leftrightarrow a = \pm 1$  e  $a | a \Leftrightarrow a = 0$

3)  $a | b \Leftrightarrow |a| | b$

4)  $a | b$  e  $c | d \Rightarrow a | bd$

5)  $a | b$  e  $b | c \Rightarrow a | c$

6)  $a | b$  e  $b | a \Rightarrow a = \pm b$

7)  $a | b$  e  $b \neq 0 \Rightarrow |a| \leq |b|$

8)  $a | b$  e  $a | c \Rightarrow a | (b + c)$   $\forall k, y \in \mathbb{Z}$

### Corolário

Sejam  $k \in \mathbb{N}$  e  $a, b_1, b_2, \dots, b_k \in \mathbb{Z}$ . Se, para cada  $i \in \{1, 2, \dots, k\}$ ,  
alô, então

$$a \mid \sum_{i=1}^k b_i n_i, \forall n_1, n_2, \dots, n_k \in \mathbb{Z}$$

### Máximo divisor comum

Dados  $a, b \in \mathbb{Z}$ . Diz-se que  $d$  é um divisor comum de  $a$  e  $b$  se  $d \mid a$  e  $d \mid b$ .

Como  $\vdash$  é divisor comum de  $a$  e  $b$  o conjunto dos inteiros positivos comuns entre dois números nunca é vazio.

$$D = \{d \in \mathbb{N} : d \mid a \text{ e } d \mid b\} \neq \emptyset$$

Caso  $a=0$  e  $b=0 \Rightarrow D = \mathbb{N}$ .

- $a \neq 0$  e  $b \neq 0 \Rightarrow D$  é finito e o elemento máximo é o maior nº que divide  $a$  e  $b$  simultaneamente.

### Definição

Sejam  $a, b \in \mathbb{Z}$  tais que  $a \neq 0$  e  $b \neq 0$ . Chama-se máximo divisor comum de  $a$  e  $b$ , e representa-se por  $m.d.c.(a, b)$ , ao inteiro positivo tal que:

- $d \mid a$  e  $d \mid b$
- $\forall c \in \mathbb{N}, (c \mid a \text{ e } c \mid b) \Rightarrow c \leq d$

Dados  $a, b \in \mathbb{Z}$ ,  $c$  diz-se combinação linear de  $a$  e  $b$  se  
 $\exists x, y \in \mathbb{Z}, c = ax + by$

### Teorema

$\forall a, b \in \mathbb{Z}$ , com  $a \neq 0$  ou  $b \neq 0$ , existem  $x, y \in \mathbb{Z}$  tais que  
 $m.d.c.(a, b) = ax + by$

### Atenção

$(d = ax + by, \text{ para alguns } x, y \in \mathbb{Z}) \not\Rightarrow m.d.c.(a, b) = d$

nem sempre é verdade

• ( $d = ax + by$ , para alguns  $x, y \in \mathbb{Z}$ )  $\Rightarrow m.d.c.(a, b) | d$ ,  $a \neq 0$  e  $b \neq 0$

### Corolário

Se  $a$  e  $b$  são inteiros, não ambos nulos, então o conjunto

$$T = \{ax + by : x, y \in \mathbb{Z}\}$$

é exatamente o conjunto de todos os múltiplos de  $d = m.d.c.(a, b)$

### Teorema

Sejam  $a$  e  $b$  inteiros, não simultaneamente nulos, e seja  $d$  um inteiro positivo. Então  $d = m.d.c.(a, b)$  se e só se

$$1) d | a \text{ e } d | b;$$

$$2) \forall c \in \mathbb{Z}, (c | a \text{ e } c | b) \Rightarrow c | d$$

### Teorema

Sejam  $a, b$  inteiros não simultaneamente nulos.

$$1) m.d.c.(a, b) = m.d.c.(-a, b) = m.d.c.(a, -b) = m.d.c.(-a, -b)$$

$$2) \text{Se } a | b, \text{ então } m.d.c.(a, b) = |a|$$

$$3) \text{Se } m.d.c.(a, b) = d, \text{ então, } \forall k \in \mathbb{Z} \setminus \{0\}, m.d.c.(ka, kb) = |k|d.$$

$$4) \text{Se } m.d.c.(a, b) = d, \text{ então } m.d.c.(a/d, b/d) = 1.$$

$$5) \nexists d | a \text{ e } d | b, \text{ para algum } d \in \mathbb{Z}, \text{ então } m.d.c.(\frac{a}{d}, \frac{b}{d}) = \frac{m.d.c.(a, b)}{d}$$

### Números primos entre si

#### Definição

Dois números inteiros  $a, b$ , não simultaneamente nulos, dizem-se primos entre si se  $m.d.c.(a, b) = 1$ .

### Teorema

Sejam  $a$  e  $b$  números inteiros, não simultaneamente nulos. Então  $a$  e  $b$  são primos entre si se e só se existirem inteiros  $x$  e  $y$  tais que  $1 = ax + by$ .

### Corolário

Sejam  $a$  e  $b$  números inteiros, não simultaneamente nulos. Se  $m.d.c.(a, b) = d$ , então  $a/d$  e  $b/d$  são primos entre si.

### Corolário

Sejam  $a, b, c \in \mathbb{Z}$ , com  $a$  e  $b$  <sup>1/a, b</sup> simultaneamente ~~nulos~~ nulos. Se  $a | c$ ,  $b | c$  e  $m.d.c.(a, b) = 1$ , então  $ab | c$ .

Atenção

$\forall a, b, c \in \mathbb{Z} (a \neq 0 \wedge b \neq 0) \nrightarrow ab \mid c$   
não é verdadeiro  $a \Rightarrow$

Corolário - Lema de Euclides

Sejam  $a, b, c \in \mathbb{Z}$ , com  $a$  e  $b$  não simultaneamente nulos. se  $a \mid bc$  e  $\text{m.d.c.}(a, b) = 1$ , então  $a \mid c$ .  
Se  $a$  e  $b \in \mathbb{Z}$  não forem primos entre si, a conclusão do Lema de Euclides pode não ser verdadeira

## O Algoritmo de Euclides

Sejam  $a, b \in \mathbb{Z}$  não simultaneamente nulos. Considerando que  $\text{m.d.c.}(|a|, |b|) = \text{m.d.c.}(a, b) = \text{m.d.c.}(b, a)$ , podemos restringir o estudo que se segue ao caso em que  $a \geq b > 0$ .

Lema

Sejam  $a$  e  $b \in \mathbb{Z}$  não simultaneamente nulos e  $q, r \in \mathbb{Z}$  tais que  $a = bq + r$ ,  $0 \leq r < b$ . Então  $\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r)$

Teorema - Algoritmo de Euclides

Sejam  $a$  e  $b$  inteiros tais que  $a \geq b > 0$ . Se existem  $q_1, q_2, \dots, q_{n+1}$ ,  $r_1, r_2, \dots, r_n \in \mathbb{Z}$  tais que

$$a = q_1b + r_1, \quad 0 < r_1 < b$$

$$b = q_2r_1 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = q_3r_2 + r_3, \quad 0 < r_3 < r_2$$

:

$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

então  $\text{m.d.c.}(a, b) = r_n$

## Mínimo múltiplo comum

Sejam  $a, b \in \mathbb{Z} \setminus \{0\}$ . Chama-se mínimo múltiplo comum de  $a$  e  $b$ , e representa-se por  $m.m.c(a, b)$ , ao menor  $k \in \mathbb{N}$  s.t.  $a|k$  e  $b|k$ , i.e., ao inteiro positivo  $m$  que satisfaz as condições seguintes:

$$1) a|m \text{ e } b|m.$$

$$2) \text{ se } c \in \mathbb{N} \text{ é tal que } a|c \text{ e } b|c, \text{ então } m \leq c.$$

Se  $a=0$  ou  $b=0$  diz-se que  $m.m.c(a, b)=0$

### Lema

Sejam  $a, b \in \mathbb{Z} \setminus \{0\}$  e  $m \in \mathbb{N}$ . Então  $m = m.m.c(a, b)$  se e só se

$$1) a|m \text{ e } b|m$$

$$2) \text{ se } c \in \mathbb{Z} \text{ é tal que } a|c \text{ e } b|c, \text{ então } m|c.$$

$$\rightarrow \forall a, b \in \mathbb{Z} \setminus \{0\}, ab \Rightarrow |ab| = m.m.c(a, b)$$

### Teorema

Para quaisquer inteiros positivos  $a$  e  $b$ ,

$$m.m.c(a, b) = \frac{a \cdot b}{m.d.c(a, b)}$$

### Corolário

Para quaisquer  $a, b \in \mathbb{Z} \setminus \{0\}$  tem-se

$$m.m.c(a, b) = a \cdot b \Leftrightarrow m.d.c(a, b) = 1$$

### Teorema

Sejam  $a, b \in \mathbb{Z} \setminus \{0\}$ . Então

$$1) \text{ se } k > 0, m.m.c(ka, kb) = k \cdot m.m.c(a, b)$$

$$2) m.m.c(a, b) = m.d.c(a, b) \Leftrightarrow a = b$$

## Números Primos

Um inteiro  $p > 1$  diz-se um número primo se 1 e  $p$  forem os únicos divisores primos positivos de  $p$ .

Um inteiro  $k > 1$  que não seja um número primo diz-se número composto

### Teorema

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

### Corolário

Sejam  $n \in \mathbb{N}$  e  $p, a_1, a_2, \dots, a_n \in \mathbb{Z}$ . Se  $p$  é primo e  $p | a_1 a_2 \dots a_n$ , então  $p | a_k$ , para algum  $k \in \{1, 2, \dots, n\}$ .

### Corolário

Seja  $n \in \mathbb{N}$ . Se  $p, q_1, q_2, \dots, q_n$  são números primos tais que  $p | q_1 q_2 \dots q_n$ , então  $p = q_k$ , para algum  $k \in \{1, 2, \dots, n\}$ .

### Teorema - Teorema Fundamental da Álgebra

Todo o número inteiro  $n \geq 1$  exprime-se como produto de um número finito de números primos.

Esta representação é única a menos da ordem dos fatores.

### Corolário

Todo o número inteiro  $n \geq 1$ , pode escrever-se, de modo único, como  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ ,

onde, para cada  $i \in \{1, 2, \dots, r\}$ ,  $k_i \in \mathbb{N}$ ,  $p_i$  é um número primo e

$$p_1 < p_2 < \dots < p_r$$

### Proposição

Seja  $n \in \mathbb{N}$ . Se  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  é a fatorização de  $n$  em números primos, então o conjunto dos divisores positivos de  $n$  é o conjunto de todos os números da forma

$$p_1^{c_1} p_2^{c_2} \dots p_r^{c_r} \text{ onde, para todo } i \in \{1, 2, \dots, r\}, 0 \leq c_i \leq k_i.$$

### Proposição

Sejam  $a = \prod_{i=1}^r p_i^{a_i}$  e  $b = \prod_{i=1}^r p_i^{b_i}$ , onde,  $\forall i \in \{1, 2, \dots, r\}$ ,  $a_i \geq 0, b_i \geq 0$  e  $p_i$  é primo.

Para cada  $i \in \{1, 2, \dots, r\}$ , sejam  $c_i = \min\{a_i, b_i\}$  e  $d_i = \max\{a_i, b_i\}$ .

Então

$$1) \text{m.d.c.}(a, b) = \prod_{i=1}^r p_i^{c_i}$$

$$2) \text{m.m.c.}(a, b) = \prod_{i=1}^r p_i^{d_i}$$

## Teorema

Existe uma infinidade de números primos

## Proposição

Todo o número composto  $a \in \mathbb{N}$  tem um divisor primo  $p$  tal que  $p \leq \sqrt{a}$ .

## Alema

Sejam  $a \in \mathbb{N}$  e  $R = \{p \in \mathbb{N} \mid p \text{ é primo e } p \leq \sqrt{a}\}$ .

$a$  é composto  $\Rightarrow (\exists p \in R \mid a \text{ é múltiplo de } p) \Rightarrow (\forall p \in R \mid p \neq 1) \Rightarrow a$  é primo

Crivo de Erastótenes - algoritmo de determinação de todos os  $n^{\text{os}}$  primos até  $n$ .

- 1) Listar todos os inteiros de 2 a  $n$  de acordo com a ordem usual.
- 2) Eliminam-se todos os  $n^{\text{os}}$  compostos, cancelando todos os múltiplos de primos  $p$ , com  $p$  tais que  $p \leq \sqrt{n}$
- 3) Os elementos restantes são os primos inferiores a  $n$ .

## Equações diofantinas

↳ equações com uma ou mais variáveis com coeficientes inteiros

## Definição

Uma equação diofônica é uma equação do tipo

$$a_1x_1^{n_1} + a_2x_2^{n_2} + \dots + a_kx_k^{n_k} = c, \quad i \in \{1, 2, \dots, k\}, n_i \in \mathbb{N}, a_i \in \mathbb{Z} \text{ e } c \in \mathbb{Z}$$

Vamos estudar apenas com duas variáveis

$ax+by=c$ ,  $a, b, c \in \mathbb{Z}$ , com  $a$  e  $b$  não simultaneamente nulos

$(x', y') \rightarrow$  solução da equação  $ax+by=c$  se  $ax'+by'=c$

$ax+by=c$  diz-se sólivel se tem pelo menos uma solução

## Proposição

Sejam  $a, b, c \in \mathbb{Z}$  com  $a$  e  $b$  não ambos nulos. A diofônica  $ax+by=c$  tem solução se e só se m.d.c.( $a, b$ ) |  $c$ .

## Proposição

Sejam  $a, b, c \in \mathbb{Z}$  com  $a$  e  $b$  não ambos nulos. Se  $ax+by=c$  admite uma solução, então admite uma infinidade de soluções.

## Definição

Sejam  $a, b, c \in \mathbb{Z}$  com  $a$  e  $b$  não ambos nulos. Chama-se solução geral da equação solúvel  $ax+by=c$  ao par  $(x', y')$  definido por

$$\begin{cases} x' = x_0 + \frac{a}{d}t \\ y' = y_0 - \frac{b}{d}t \end{cases}, t \in \mathbb{Z}$$

Onde  $(x_0, y_0)$  é uma solução particular da equação  $ax+by=c$  e  $d = \text{m.d.c.}(a, b)$ .

## Congruências módulo $n$

### Definição

Seja  $n \in \mathbb{N}$ . Diz-se que um inteiro  $a$  é congruente módulo  $n$  com um inteiro  $b$  se escreve-se  $a \equiv b \pmod{n}$ , se  $n$  é um divisor de  $a - b$ , i.e., se  $a - b = nk$ , para algum  $k \in \mathbb{Z}$ . Se  $a$  não é congruente módulo  $n$  com  $b$ , escreve-se  $a \not\equiv b \pmod{n}$  e diz-se que  $a$  é incongruente com  $b$  módulo  $n$ .

### Teorema

Seja  $n \in \mathbb{N}$ . Para quaisquer inteiros  $a$  e  $b$ ,

$$a \equiv b \pmod{n} \Leftrightarrow a$$
 e  $b$  têm o mesmo resto na divisão por  $n$ .

### Corolário

Seja  $n \in \mathbb{N}$ . Cada inteiro  $a$  é congruente módulo  $n$  com um e um só dos inteiros

$$0, 1, 2, \dots, n-2, n-1.$$

### Definição

Seja  $n \in \mathbb{N}$ . Um conjunto de  $n$  inteiros  $\{a_1, a_2, \dots, a_n\}$  diz-se um sistema completo de resíduos módulo  $n$  se todo o inteiro  $i$  congruente módulo  $n$  com um e um só  $a_k$  ( $k \in \{1, 2, \dots, n\}$ ).

Obs: Dado  $n \in \mathbb{N}$ , um conjunto de  $n$  inteiros  $\{a_1, a_2, \dots, a_n\}$  é um sistema completo de resíduos módulo  $n$  se e só se não existem em  $\{a_1, a_2, \dots, a_n\}$  dois inteiros distintos que sejam congruentes módulo  $n$  entre si.

### Teorema

Sejam  $n \in \mathbb{N}$  e  $a, b, c, d \in \mathbb{Z}$ . Então

i)  $a \equiv a \pmod{n}$ ;

ii)  $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ ;

iii)  $a \equiv b \pmod{n}$  e  $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ ;

iv)  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n} \Rightarrow \begin{cases} ac \equiv bd \pmod{n} \\ ac \equiv bc \pmod{n} \end{cases}$

v)  $a \equiv b \pmod{n} \Rightarrow \begin{cases} ac \equiv bc \pmod{n} \\ ac \equiv b + c \pmod{n} \end{cases}$

vi)  $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}, \forall k \in \mathbb{N}$ .

→ relações  $\equiv \pmod{n}$  → compatível com a adição e a multiplicação em  $\mathbb{Z}$ .

### Lei do Corte

Sejam  $n \in \mathbb{N}$  e  $a, b, c \in \mathbb{Z}$ . No teorema anterior vimos que

$$a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$$

mas

$$ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{n} \rightarrow \text{não sempre é verdade}$$

### Teorema

Sejam  $n \in \mathbb{N}$  e  $a, b, c \in \mathbb{Z}$ . Se  $ca \equiv cb \pmod{n}$ , então  $a \equiv b \pmod{\frac{n}{d}}$ , onde  $d = \text{m.d.c.}(c, n)$ .

### Corolário

Sejam  $n \in \mathbb{N}$  e  $a, b, c \in \mathbb{Z}$ . Se  $ca \equiv cb \pmod{n}$  e  $\text{m.d.c.}(c, n) = 1$ , então  $a \equiv b \pmod{n}$ .

### Corolário

Sejam  $p \in \mathbb{N}$  e  $a, b, c \in \mathbb{Z}$ . Se  $ca \equiv cb \pmod{p}$ ,  $p$  é primo se e só se  $a \equiv b \pmod{p}$ .

### Lei do Anulamento do Produto

A Lei do anulamento do produto, válida para a relação de igualdade, nem sempre é válida para a relação  $\equiv \pmod{n}$ , ou seja, a implicação nem sempre é verdadeira:  $ab = 0 \pmod{n} \Rightarrow (a \equiv 0 \pmod{n}) \vee (b \equiv 0 \pmod{n})$

### Teorema

Sejam  $n \in \mathbb{N}$  e  $a, b \in \mathbb{Z}$ . Se  $ab \equiv 0 \pmod{n}$  e m.d.c.( $a, n$ ) = 1, então  $b \equiv 0 \pmod{n}$ .

A relação  $\equiv \pmod{n}$  é uma relação de equivalência.

→ determina em  $\mathbb{Z}$  uma partição em classes de equivalência

Para cada  $a \in \mathbb{Z}$ , representa-se por  $[a]_n$  a classe de equivalência de  $a$  para a relação  $\equiv \pmod{n}$ , i.e.

$$[a]_n = \{k \in \mathbb{Z} \mid a \equiv k \pmod{n}\}$$

•  $a \equiv r \pmod{n} \rightarrow$  resto da divisão de  $a$  p/n.

↓  
 $[a]_n = [r]_n \rightarrow$  existem exatamente  $n$  classes de equivalência módulo  $n$ :  $[0]_n, [1]_n, \dots, [n-1]_n$

### O conjunto quociente

$$\mathbb{Z}/\equiv \pmod{n} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

representa-se por  $\mathbb{Z}_n$ ; as classes  $[0]_n, [1]_n, \dots, [n-1]_n$  designam-se por inteiros módulos  $n$ .

$$[a]_n + [b]_n = [a+b]_n \quad [a]_n [b]_n = [ab]_n$$

## Critérios de divisibilidade

Se  $a_0, \dots, a_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ , o número

$$a = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_2 \times 10^2 + a_1 \times 10 + a_0$$

é representado por

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} \rightarrow \text{representação decimal de } a$$

digitos / algarismos  $\rightarrow a_n, a_{n-1}, \dots, a_1, a_0$

$a_0 \rightarrow$  dígito das unidades

$a_1 \rightarrow$  dígito das dezenas

$a_2 \rightarrow$  dígito das centenas

Se  $a_0 \neq 0 \rightarrow a$  tem  $n+1$  algarismos

Se não há ambiguidade  
não se coloca a barra

## Teorema

Seja  $n \in \mathbb{N}$ . Se  $r_1, r_2, \dots, r_{n-1}, r_n$  são os restos da divisão de,

respectivamente,  $10, 10^2, \dots, 10^{n-1}, 10^n$  por  $n$ , então

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} = a_n r_n + a_{n-1} r_{n-1} + \dots + a_2 r_2 + a_1 r_1 + a_0 \pmod{n}$$

## Critério de divisibilidade por 2

- O resto da divisão de um inteiro positivo  $a$  por 2 é o resto que se obtém dividindo por 2 o algarismo das unidades de  $a$ .

## Critério de divisibilidade por 5

- O resto da divisão de um inteiro positivo  $a$  por 5 é o resto que se obtém dividindo por 5 o algarismo das unidades de  $a$ .

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} \equiv a_0 \pmod{2} \quad \overline{a_n a_{n-1} \dots a_2 a_1 a_0} \equiv a_0 \pmod{5}$$

## Critério de divisibilidade por 3

- O resto da divisão de um inteiro positivo  $a$  por 3 é o resto que se obtém dividindo por 3 a soma de todos os algarismos de  $a$ .

## Critério de divisibilidade por 9

- O resto da divisão de um inteiro positivo  $a$  por 9 é o resto que se obtém dividindo por 9 a soma de todos os algarismos de  $a$ .

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} \equiv a_n + a_{n-1} + \dots + a_2 + a_1 + a_0 \pmod{3}$$

$\hookrightarrow$  ou 9.

## Critério de divisibilidade por 4

- O resto da divisão de um inteiro positivo  $a$  por 4 é o resto que se obtém dividindo por 4 a soma do dobro do algarismo das dezenas de  $a$  com o algarismo das unidades de  $a$ .

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} \equiv 2 \times a_1 + a_0 \pmod{4}$$

## Critério da divisibilidade por 11

- O resto da divisão de um inteiro positivo por 11 é o resto que se obtém dividindo por 11 a diferença entre a soma dos algarismos de ordem ímpar e a soma dos algarismos de ordem par.
- Considerando o algarismo das unidades par, terímos

$$a_{n-1} \dots a_2 a_1 a_0 = (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots) \pmod{11}$$

## Congruências lineares

### Definição

- Congruência linear → toda a expressão da forma  $ax \equiv b \pmod{n}$ ,  $a, b \in \mathbb{Z}$  e  $n$  é um símbolo

Soluções da congruência linear → qualquer intérprete  $x$  tal que  $ax \equiv b \pmod{n}$  é verdade.

Resolver uma congruência linear → determinar o conjunto de todas as soluções dessa congruência linear.

### Teorema

Sejam  $n \in \mathbb{N}$ ,  $a, b \in \mathbb{Z}$  e  $d = \text{m.d.c.}(a, n)$ . A congruência  $ax \equiv b \pmod{n}$  admite soluções se e só se  $\text{m.d.c.}(a, n) | b$ . Se a congruência linear  $ax \equiv b \pmod{n}$  é solúvel e  $x_0$  é solução, então

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}$$

é a lista completa das soluções da congruência linear  $ax \equiv b \pmod{n}$ , não congruentes módulo  $n$ .

### Corolário

Sejam  $n \in \mathbb{N}$  e  $a, b \in \mathbb{Z}$ . Se  $\text{m.d.c.}(a, n) = 1$ , então a congruência linear  $ax \equiv b \pmod{n}$  tem uma e uma só solução módulo  $n$ .

Sejam  $n \in \mathbb{N}$  e  $a \in \mathbb{Z} \setminus \{0\}$ . Se  $a$  e  $n$  são primos entre si, a congruência  $ax \equiv 1 \pmod{n}$  tem uma única solução módulo  $n$ ; a esta solução dá-se a designação de inverso multiplicativo de  $a$  módulo  $n$ .

### Teorema

Sejam  $n \in \mathbb{N}$  e  $a, b \in \mathbb{Z}$ . Sejam  $ax \equiv b \pmod{n}$  uma congruência linear solúvel. Então  $x_0$  é solução de  $ax \equiv b \pmod{n}$  se e só se  $x_0$  é solução de  $\frac{n}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ , onde  $d = \text{m.d.c.}(a, n)$  e  $a^* \equiv 1 \pmod{\frac{n}{d}}$  é a única solução de  $\frac{a}{d}x \equiv 1 \pmod{\frac{n}{d}}$ .

## Sistemas de congruências lineares

Sistema de congruências lineares : (S)  $\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_Kx \equiv b_K \pmod{n_K} \end{cases}$

onde  $K \in \mathbb{N} \setminus \{1\}$  e,  $\forall i \in \{1, \dots, K\}, a_i, b_i \in \mathbb{Z}$  e  $n_i \in \mathbb{N}$ .

Uma solução do (S) é qualquer inteiro que é solução de todas as congruências lineares do (S).

### Definições

sistema solúvel  $\rightarrow$  admite solução

sistemas equivalentes  $\rightarrow$  sistemas que tiverem o mesmo conjunto de soluções.

### Proposição

Sejam  $n \in \mathbb{N}$  e

$$n = p_1^{m_1} p_2^{m_2} \cdots p_K^{m_K}$$

a fatorização de  $n$  em fatores primos distintos  $p_1, p_2, \dots, p_K$ . Então, para quaisquer  $a$  e  $b$ ,  $x$  é solução da congruência linear  $ax \equiv b \pmod{n}$  se e só se  $x$  é solução do sistema

$$(S) \begin{cases} ax \equiv b \pmod{p_1^{m_1}} \\ ax \equiv b \pmod{p_2^{m_2}} \\ \vdots \\ ax \equiv b \pmod{p_K^{m_K}} \end{cases}$$

### Teorema - Teorema Chines dos Restos

Sejam  $K \in \mathbb{N} \setminus \{1\}$ ,  $a_1, a_2, \dots, a_K \in \mathbb{Z}$  e  $n_1, n_2, \dots, n_K \in \mathbb{N}$  tais que

$$\forall i, j \in \{1, \dots, K\} \quad i \neq j \Rightarrow \text{m.d.c.}(n_i, n_j) = 1.$$

Então o sistema de congruências lineares

$$(S') \begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_K \pmod{n_K} \end{cases}$$

tem uma e uma só solução módulo  $n_1, n_2, \dots, n_K$ .

## Teorema

15  
23

Sejam  $k \in \mathbb{N} \setminus \{0\}$ ,  $a_1, a_2, \dots, a_k \in \mathbb{Z}$  e  $n_1, n_2, \dots, n_k \in \mathbb{N}$ . Então o sistema de congruências lineares

$$(S') \quad \begin{cases} u \equiv a_1 \pmod{n_1} \\ u \equiv a_2 \pmod{n_2} \\ \vdots \\ u \equiv a_k \pmod{n_k} \end{cases}$$

tem solução se e só se, para qualquer  $i, j \in \{1, 2, \dots, k\}$ ,

$$\text{m.d.c}(n_i, n_j) \mid a_i - a_j$$

Se o sistema tiver solução, ela é única módulo  $n$  onde  $n = 0$  m.m.c de  $n_1, n_2, \dots, n_k$ .

## Teoremas Relevantes na Teoria de Números

### Pequeno Teorema de Fermat

Se  $p$  é primo e  $a$  é um inteiro não divisível por  $p$ , então  $p | a^{p-1} - 1 \pmod{p}$

#### Corolário

Se  $p$  é primo, então  $a^p \equiv a \pmod{p}$ , para qualquer inteiro  $a$ .

Pelo contra-recíproco do Teorema

$$(\exists_{a \in \mathbb{Z}} a^{p-1} \not\equiv 1 \pmod{p}) \Rightarrow (p \text{ não é primo} \vee p | a)$$

ou o contra-recíproco do corolário

$$(\exists_{a \in \mathbb{Z}} a^{p-1} \not\equiv 1 \pmod{p}) \Rightarrow p \text{ não é primo}$$

permite verificar se um dado  $n^{\circ}$  natural é ou não primo.

#### Proposição

Sejam  $p$  e  $q$  números primos distintos e  $a$  um inteiro tal que  $a^p \equiv a \pmod{q}$  e  $a^q \equiv a \pmod{p}$ . Então  $a^{pq} \equiv a \pmod{pq}$

## Teorema de Euler

### Função de Euler

Para cada  $n \geq 1$ , seja  $\phi(n)$  o n.º de inteiros positivos  $k$  tais que  $\text{h} \leq n$  e m.d.c. ( $K, n$ ) = 1.

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

$$n \mapsto \phi(n)$$

e)

### Proposição

Um inteiro positivo  $n$  é primo se e só se  $\phi(n) = n - 1$ .

m.d.

### Proposição

Se  $p$  é primo e  $k > 0$ , então

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

### Proposição

Sejam  $m$  e  $n$  inteiros positivos tais que  $\text{m.d.c.}(m, n) = 1$ . Então

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

Obs: só é válido se  $m$  e  $n$  forem primos entre si.

### Teorema

Se um inteiro  $n > 1$  admite a fatorização

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

onde  $p_1, p_2, \dots, p_r$  são primos distintos  $\geq 2$ , então

$$\begin{aligned}\phi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_r^{k_r} - p_r^{k_r-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \dots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

### Lema

Sejam  $n \in \mathbb{N}$  e  $a \in \mathbb{Z}$  tais que  $\text{m.d.c.}(a, n) = 1$ . Sejam  $r_1, r_2, \dots, r_{\phi(n)}$  os  $\phi(n)$  inteiros menores do que  $n$  e primos com  $n$ . Então, para cada  $i \in \{1, 2, \dots, \phi(n)\}$ , existe  $j \in \{1, 2, \dots, \phi(n)\}$  tal que  $ar_i \equiv r_j \pmod{n}$ .

### Teorema de Euler

Se  $a \in \mathbb{Z}$  e  $n \in \mathbb{N}$  são tais que  $\text{m.d.c.}(a, n) = 1$ , então  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

### Teorema de Wilson

Se  $p$  é um número primo, então  $(p-1)! \equiv -1 \pmod{p}$ .

### Teorema

Se  $(n-1)! \equiv -1 \pmod{n}$ , então  $n$  é primo.