Elementos de Probabilidades e Teoria de Números

Licenciatura em Engenharia Informática

Mestrado Integrado em Engenharia Informática

Carla Mendes

2021/2022

Departamento de Matemática

Noções básicas de Teoria de Números

Teoria de números

A teoria de números é um dos ramos mais antigos da matemática e o seu início remonta ao período da Matemática Grega Antiga, cerca de 300 anos a.c.. Muitos dos assuntos aqui tratados apareciam já referidos na obra *Os Elementos* de Euclides.

A teoria de números estuda as propriedades dos números inteiros; em particular estuda propriedades relacionadas com a divisibilidade de inteiros, as quais permitem o estudo de resultados mais avançados nesta área.

Algoritmo da divisão

O resultado seguinte, conhecido por Algoritmo da Divisão, é a base do estudo da teoria de números.

Teorema (Algoritmo da Divisão)
Dados dois números inteiros a e b tais que $b > 0$, existem inteiros únicos q e r tais que

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

Demonstração: Consideremos o conjunto $S = \{a - xb \in \mathbb{N}_0 : x \in \mathbb{Z}\}$.

Comecemos por mostrar que o conjunto S não é vazio.

Uma vez que $b \geq 1$, tem-se $|a|b \geq |a|$. Assim, considerando $x = -|a|$, tem-se

$$a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0.$$

Portanto, $a - xb \in S$.

O conjunto S tem elemento mínimo:

- Se $0 \in S$, então 0 é o elemento mínimo de S.
- Se $0 \notin S$, então $S \subseteq \mathbb{N}$ e, pelo Príncípio da Boa Ordenação(1), S tem elemento mínimo.

[(1) *Princípio da Boa Ordenação*: Qualquer subconjunto não vazio de $\mathbb{N}$ tem elemento mínimo.]

Demonstração (continuação):

Seja $r = \min S$. Então $r \in S$, pelo que existe $q \in \mathbb{Z}$ tal que $r = a - qb$ e $r \geq 0$, i.e., existe $q \in \mathbb{Z}$ tal que $a = qb + r$ e $r \geq 0$.

Prova-se que $r < b$. De facto, se admitirmos que $b \leq r$, tem-se

$$a - (q+1)b = a - qb - b = r - b \geq 0,$$

pelo que $a - (q+1)b \in S$. Mas $a - (q+1)b = r - b < r$, o que contradiz o facto de r ser o mínimo de S. Logo $r < b$.

Demonstração (continuação): Mostremos, agora, que q e r são únicos.

Sejam $q, q', r, r' \in \mathbb{Z}$ tais que

$$a = bq + r, \quad a = bq' + r', \quad 0 \leq r < b \text{ e } 0 \leq r' < b.$$

Então

$$b(q - q') = r' - r,$$

donde segue que

$$b|q - q'| = |r' - r|.(*)$$

Considerando que $0 \leq r' < b$ e $-b < -r \leq 0$, tem-se $-b < r' - r < b$, o que é equivalente a $|r' - r| < b$. Então $b|q - q'| < b$, donde resulta $0 \leq |q - q'| < 1$. Como $q - q' \in \mathbb{Z}$, concluímos que $q - q' = 0$, i.e., $q = q'$. De $(*)$ concluímos que $r = r'$. □

Divisibilidade

O Algoritmo da Divisão pode ser generalizado pelo resultado seguinte, o qual estabelece a divisão de qualquer inteiro por qualquer inteiro não nulo.

Corolário

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

Demonstração.

Considerando o teorema anterior, resta provar o resultado para o caso em que $b \in \mathbb{Z}^-$. Como $|b| > 0$, pelo teorema anterior, existem inteiros únicos q' e r' tais que

$$a = q'|b| + r' \text{ e } 0 \leq r' < |b|.$$

Então, como $|b| = -b$, obtemos

$$a = (-q')b + r' \text{ com } 0 \leq r' < |b|.$$

□

Divisibilidade

Dados $a, b \in \mathbb{Z}$ e $b \neq 0$, os números q e r tais que $a = bq + r$ e $0 \leq r < |b|$ designam-se, respectivamente, por **quociente da divisão de** a **por** b e **resto da divisão de** a **por** b.

Dividir a por b significa obter o quociente e o resto da divisão de a por b.

Exemplo

- Para $a = 17$ e $b = 6$, temos $a = 17 = 6 \times 2 + 5 = b \times 2 + 5$ e $0 \leq 5 < 6$.
- Para $a = 3$ e $b = 6$, temos $a = 3 = 6 \times 0 + 3 = b \times 0 + 3$ e $0 \leq 3 < 6$.
- Para $a = -2$ e $b = -7$, temos $a = -2 = (-7) \times 1 + 5 = b \times 1 + 5$ e $0 \leq 5 < |-7|$.
- Para $a = -59$ e $b = -7$, temos $a = 59 = (-7) \times 9 + 4 = b \times 9 + 4$ e $0 \leq 4 < |-7|$.
- Para $a = 61$ e $b = -7$, temos $a = 61 = (-7) \times (-8) + 5 = b \times (-8) + 5$ e $0 \leq 5 < |-7|$.

Divisibilidade

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

Um inteiro a diz-se:

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

Divisibilidade

Apresentamos seguidamente algumas aplicações do Algoritmo da Divisão.

- Provar que o resto da divisão do quadrado de qualquer número inteiro por 4 ou é 0 ou é 1.

  Sejam $a \in \mathbb{Z}$ e $b = 2$. Pelo Algoritmo da Divisão, existem inteiros únicos $q, r \in \mathbb{Z}$ tais que $a = 2q + r$ e $r \in \{0, 1\}$.

  - Se $r = 0$, temos $a = 2q$ para algum $q \in \mathbb{Z}$ e, portanto, $a^2 = 4q^2 = 4q^2 + 0$, com $q^2 \in \mathbb{Z}$ e $0 \leq 0 < 4$.
  - Se $r = 1$, temos $a = 2q + 1$ para algum $q \in \mathbb{Z}$ e, portanto, $a^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$, com $q^2 + q \in \mathbb{Z}$ e $0 \leq 1 < 4$. .

Divisibilidade

- Provar que o quadrado de qualquer número inteiro ímpar é da forma $8k + 1$ para certo inteiro k.

  Sejam $a \in \mathbb{Z}$ um número ímpar e $b = 4$. Pelo Algoritmo da Divisão, obtemos $a = bq + r$ onde $q \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3\}$. Como a é ímpar, então $r \in \{1, 3\}$.

  - Se $r = 1$, tem-se $a = 4q + 1$ e

    $$a^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1,$$

    onde $2q^2 + q \in \mathbb{Z}$;
  - se $r = 3$, tem-se $a = 4q + 3$ e

    $$a^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1,$$

    onde $2q^2 + 3q + 1 \in \mathbb{Z}$.

Divisibilidade

- Provar que, para qualquer inteiro $a \geq 1$, $\frac{a(a^2+2)}{3}$ é um inteiro.

  Seja $a \in \mathbb{Z}$.

  Considerando a divisão de a por 3, temos $a = 3q + r$, para algum $q \in \mathbb{Z}$ e com $r \in \{0, 1, 2\}$.

  - Se $a = 3q$, então $\frac{a(a^2+2)}{3} = q(9q^2 + 2) = k$ onde $k \in \mathbb{Z}$;
  - Se $a = 3q + 1$, então $\frac{a(a^2+2)}{3} = (3q + 1)(3q^2 + 2q + 1) = k'$ onde $k' \in \mathbb{Z}$;
  - Se $a = 3q + 2$, então $\frac{a(a^2+2)}{3} = (3q + 2)(3q^2 + 4q + 2) = k''$ onde $k'' \in \mathbb{Z}$.

Divisibilidade

Definição

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

Observação: As expressões *a* **divide** *b*, *a* **é divisor de** *b*, *a* **é um factor** *b*, *b* **é divisível por** *a* e *b* **é um múltiplo de** *a* têm todos o mesmo significado.

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

Divisibilidade

Exemplo

- -36 é divisível por 4, pois $-36 = 4 \times (-9)$;
- 25 não é divisível por 3, pois, para todo $q \in \mathbb{Z}$, $25 \neq 3 \times q$.

Divisibilidade

A definição anteriormente introduzida define, no conjunto $\mathbb{Z}$ dos números inteiros, uma relação binária

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

Apresentam-se de seguida algumas propriedades desta relação.

Divisibilidade

Teorema

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

(1) $a \mid 0$, $1 \mid a$ *e* $a \mid a$.

(2) $a \mid 1 \Leftrightarrow a = \pm 1$ *e* $0 \mid a \Leftrightarrow a = 0$.

(3) $a \mid b \Leftrightarrow |a| \mid b$.

(4) $a \mid b$ *e* $c \mid d \Rightarrow ac \mid bd$.

(5) $a \mid b$ *e* $b \mid c \Rightarrow a \mid c$.

(6) $a \mid b$ *e* $b \mid a \Rightarrow a = \pm b$.

(7) $a \mid b$ *e* $b \neq 0 \Rightarrow |a| \leq |b|$.

(8) $a \mid b$ *e* $a \mid c \Rightarrow a \mid (bx + cy)$ *para todos* $x, y \in \mathbb{Z}$.

Demonstração.

Demonstramos as propriedades (4), (7) e (8); a prova das restantes alíneas fica como exercício.

(4) Sejam $a, b, c, d \in \mathbb{Z}$ tais que $a \mid b$ e $c \mid d$. Então existem $q, q' \in \mathbb{Z}$ tais que $b = aq$ e $d = cq'$. Logo, $bd = (aq)(cq') = ac(qq')$, com $qq' \in \mathbb{Z}$ e, portanto, $ac \mid bd$.

(7) Sejam $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \setminus \{0\}$ tais que $a \mid b$. Então existe $c \neq 0$ tal que $b = ac$. Assim, $|b| = |a||c|$ com $|c| \geq 1$ e, portanto, $|a| \leq |b|$.

(8) Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $a \mid c$. Então existem $q, q' \in \mathbb{Z}$ tais que $b = aq$ e $c = aq'$. Logo, para quaisquer $x, y \in \mathbb{Z}$, temos

$$bx + cy = (aq)x + (aq')y = a(qx + q'y).$$

Como $qx + q'y \in \mathbb{Z}$, concluímos que $a \mid (bx + cy)$.

□

A propriedade da alínea (8) do teorema anterior pode ser generalizada a somas com mais do que dois termos.

Corolário

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

$$a \mid \sum_{i=1}^{k} b_i x_i,$$

para quaisquer $x_1, x_2, \ldots, x_k \in \mathbb{Z}$.

Demonstração.

Por indução sobre k. □

Máximo divisor comum

Dados inteiros a, b e d, diz-se que d *é um divisor comum de* a *e* b se $d \mid a$ e $d \mid b$.

Para quaisquer $a, b \in \mathbb{Z}$, 1 é um divisor comum de a e b, pelo que o conjunto dos inteiros positivos que são divisores comuns de a e b é não vazio, i.e.,

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

Todo o inteiro é um divisor de zero, pelo que se $a = b = 0$, tem-se $D = \mathbb{N}$.

Se $a \neq 0$ ou $b \neq 0$, o conjunto D é finito e tem elemento máximo: este elemento máximo é o maior número inteiro positivo que divide simultaneamente a e b.

Definição

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

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

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

Exemplo

- Determinando os divisores positivos de -12 e 30, é simples concluir que o máximo divisor comum de -12 e 30 é o 6. De facto, tem-se
  - divisores positivos de -12: 1, 2, 3, 4 e 6 e 12,
  - divisores positivos de 30: 1, 2, 3, 5, 6, 10, 15 e 30,

  pelo que

  $$D = \{d \in \mathbb{N} : d \mid -12 \text{ e } d \mid 30\} = \{1, 2, 3, 6\}.$$

  O elemento máximo de D é o 6 e, portanto, m.d.c.$(-12, 30) = 6$.

- O inteiro 1 é o único inteiro positivo que é disivor comum de 6 e 35; portanto, m.d.c.$(6, 35) = 1$.

Dados inteiros a, b e c, diz-se que c *é combinação linear de* a *e* b se existem $x, y \in \mathbb{Z}$ tais que $c = ax + by$.

Sendo a e b inteiros não simultaneamente nulos, o resultado seguinte estabelece que o m.d.c.(a, b) é combinação linear de a e b.

Teorema

Para quaisquer $a, b \in \mathbb{Z}$*, com* $a \neq 0$ *ou* $b \neq 0$*, existem* $x, y \in \mathbb{Z}$ *tais que*

$$\text{m.d.c.}(a, b) = ax + by.$$

Observação: O teorema anterior estebelece que, para quaisquer inteiros a, b, não simultaneamente nulos, o m.d.c.(a, b) é combinação linear de a e b, i.e., m.d.c.$(a, b) = ax + by$ para certos $x, y \in \mathbb{Z}$. Note-se, porém, que os coeficientes x e y podem não ser únicos.

Exemplo

Sendo $a = -12$ e $b = 30$, tem-se m.d.c.$(a, b) = 6$ e pode escrever-se 6 como combinação linear de a e b de mais do que uma forma; por exemplo,

$$6 = (-12) \times 2 + 30 \times 1, \quad 6 = (-12) \times (7) + 30 \times 3.$$

Divisibilidade

O teorema anterior estabelece a existência de inteiros x, y que permitem escrever m.d.c.$(a, b) = ax + by$, para quaisquer inteiros a, b, não simultaneamente nulos. Este teorema não fornece, porém, um método prático para os determinar. Mais à frente apresenta-se um método que permitirá determinar coeficientes nas condições indicadas de uma forma mais eficiente.

Observação: Note-se que se a, b são inteiros, não simultaneamente nulos, a implicação

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

nem sempre é verdadeira.

Exemplo

Tem-se $18 = (-12) \times 21 + 30 \times 9$, mas $18 \neq \text{m.d.c.}(-12, 30)$, pois $\text{m.d.c.}(-12, 30) = 6$.

Do próximo resultado é possível concluir a veracidade da implicação

$$(d = ax + by, \text{ para alguns } x, y \in \mathbb{Z}) \Rightarrow \text{m.d.c.}(a, b) \mid d$$

quaisquer que sejam os inteiros a, b tais que $a \neq 0$ ou $b \neq 0$.

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

Exemplo

Na tabela seguinte listam-se as combinações lineares $56x + 35y$, onde $-3 \leq x \leq 3$ e $-3 \leq y \leq 3$. Todas as entradas desta tabela são múltiplos de $7 = \text{m.d.c.}(56, 35)$.

				x			
y	-3	-2	-1	0	1	2	3
-3	-273	-217	-161	-105	-49	7	63
-2	-238	-182	-126	-70	-14	42	98
-1	-203	-147	-91	-35	21	77	133
0	-168	-112	-56	0	56	112	168
1	-133	-77	-21	35	91	147	203
2	-98	-42	14	70	126	182	238
3	-63	-7	49	105	161	217	273

Teorema

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

(1) $d \mid a$ e $d \mid b$;

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

Demonstração:

$\Rightarrow$) Seja $d = \text{m.d.c.}(a, b)$. Por (i) da definição de m.d.c.(a, b), $d \mid a$ e $d \mid b$, o que prova (1).

Se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então $c \mid (ax + by)$, para quaisquer $x, y \in \mathbb{Z}$. Assim, como $d = ax_0 + by_0$ para alguns $x_0, y_0 \in \mathbb{Z}$, concluímos que $c \mid d$, o que prova (2).

Demonstração (continuação):

$\Leftarrow$) Seja $d \in \mathbb{N}$ tal que d satisfaz as condições (1) e (2). Então a condição (i) da definição é obviamente satisfeita.

Seja $c \in \mathbb{N}$ tal que $c \mid a$ e $c \mid b$. Então, por (2), $c \mid d$. Logo, $c = |c| \leq |d| = d$, o que prova (ii).

Assim, $d = \text{m.d.c.}(a, b)$.

Apresentam-se seguidamente mais algumas propriedades a respeito do máximo divisor comum.

Teorema

Sejam a, b inteiros não simultaneamente nulos.

(1) $\text{m.d.c.}(a, b) = \text{m.d.c.}(-a, b) = \text{m.d.c.}(a, -b) = \text{m.d.c.}(-a, -b)$.

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

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

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

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

Demonstração.

Apresenta-se a prova das propriedades (3) e (4) ficando a prova das restantes propriedades como exercício.

(3) Considerando a propriedade (1), basta estudar o caso em que $k > 0$.

Sejam m.d.c.$(a, b) = d$ e m.d.c.$(ka, kb) = d'$.

Uma vez que $d \,|a$, $d \,|\, b$, então $|k|d \,|\, ka$ e $|k|d \,|\, kb$, pelo que $|k|d \,|\, d'$.

Como m.d.c.$(a, b) = d$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = d$. Então $(ka)x + (kb)y = kd$, pelo que $d' \,|\, kd = |k|d$.

Atendendo a que d' e $|k|d$ são ambos positivos, conclui-se que $d' = |k|d$, ou seja, m.d.c.$(ka, kd) = |k|d$.

Demonstração (continuação).

(4) Admitamos que m.d.c.$(a, b) = d$. Então $d \mid a$ e $d \mid b$ e, portanto, $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros. Além disso, existem $x, y \in \mathbb{Z}$ tais que

$$d = ax + by.$$

Desta igualdade segue que

$$1 = \frac{a}{d}x + \frac{b}{d}y$$

pelo que m.d.c.$(\frac{a}{d}, \frac{b}{d}) \mid 1$. Como m.d.c.$(\frac{a}{d}, \frac{b}{d})$ e 1 são ambos positivos, então m.d.c.$(\frac{a}{d}, \frac{b}{d}) = 1$.

Números primos entre si

Os inteiros 1 e -1 são divisores de qualquer número inteiro. Para certos $a, b \in \mathbb{Z}$, 1 e -1 podem ser os únicos divisores comuns de a e b, pelo que $\text{m.d.c.}(a, b) = 1$. Esta situação ocorre frequentemente, motivando a definição seguinte.

Definição

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

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 $1 = ax + by$.

Demonstração.

$\Rightarrow$) Se a e b são primos entre si, então $1 = \text{m.d.c.}(a, b)$. Logo, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.

$\Leftarrow$) Se existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$, então 1 é múltiplo do $\text{m.d.c.}(a, b)$. Como 1 e $\text{m.d.c.}(a, b)$ são ambos positivos, concluímos que $1 = \text{m.d.c.}(a, b)$. $\square$

Corolário

Sejam a e b números inteiros, não simultaneamente nulos. Se $\text{m.d.c.}(a, b) = d$*, então* $\frac{a}{d}$ *e* $\frac{b}{d}$ *são primos entre si.*

Demonstração.

Já provámos anteriormente que se $\text{m.d.c.}(a, b) = d$, então $\text{m.d.c.}(\frac{a}{d}, \frac{b}{d}) = 1$ e, portanto, $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si. □

Corolário

Sejam $a, b, c \in \mathbb{Z}$, com a e b não simultaneamente nulos. Se $a \mid c$, $b \mid c$ e m.d.c.$(a, b) = 1$, *então $ab \mid c$.*

Demonstração.

Como $a \mid c$ e $b \mid c$, existem $r, s \in \mathbb{Z}$ tais que $c = ar = bs$.

Uma vez que $1 =$ m.d.c.(a, b), existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.

Logo,

$$c = c \cdot 1 = c(ax + by) = cax + cby = bsax + arby = (ab)(sx + ry).$$

Como $sx + ry \in \mathbb{Z}$, conclui-se que $ab \mid c$. □

Observação: Note-se que não é verdade que

$$\forall_{a,b,c\in\mathbb{Z}} \quad (a \mid c \wedge b \mid c) \Rightarrow ab \mid c.$$

Por exemplo,

$$6 \mid 24 \text{ e } 8 \mid 24, \text{ mas } 6 \cdot 8 \nmid 24.$$

Assim, no corolário anterior, a condição de a e b serem primos entre si não pode ser omitida.

Corolário (Lema de Euclides)

Sejam $a, b, c \in \mathbb{Z}$, com a e b não simultaneamente nulos. Se $a \mid bc$ e m.d.c.$(a, b) = 1$, *então $a \mid c$.*

Demonstração.

Se $1 = \text{m.d.c}(a, b)$, então existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$. Logo,

$$c = c \cdot 1 = acx + bcy.$$

Como $a \mid ac$ e $a \mid bc$, segue que $a \mid (ac)x + (bc)y$, ou seja, $a \mid c$. □

Observação: Se $a, b \in \mathbb{Z}$ não forem primos entre si, a conclusão do Lema de Euclides pode não ser verdadeira. De facto,

$$12 \mid (9 \times 8), \text{ mas } 12 \nmid 9 \text{ e } 12 \nmid 8.$$

O Algoritmo de Euclides

O máximo divisor comum de dois inteiros a, b, não simultaneamente nulos, pode ser calculado determinando todos os divisores positivos comuns a a e b e escolhendo o maior destes. Porém, este processo não é o mais eficiente quando se pretende determinar o máximo divisor comum de números elevados. Um método mais eficiente para o cálculo do máximo divisor comum de dois inteiros, conhecido por Algoritmo de Euclides, é apresentado no livro VII da obra *Os Elementos*. Este método é baseado em aplicações sucessivas do Algoritmo da Divisão.

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 inteiros positivos não nulos e $q, r \in \mathbb{Z}$ tais que $a = bq + r$ e $0 \leq r < b$. Então

$$\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r).$$

Demonstração:

Sejam a e b inteiros positivos não nulos e $q, r \in \mathbb{Z}$ tais que $a = bq + r$ e $0 \leq r < b$.

Seja $d = \text{m.d.c.}(a, b)$.

Mostremos que $\text{m.d.c.}(b, r) = d$, ou seja, provemos que

(i) $d \mid b$ e $d \mid r$;

(ii) $\forall c \in \mathbb{N}$, $(c \mid b \text{ e } c \mid r) \Rightarrow c \leq d$.

Demonstração (continuação):

(i) Uma vez que $d = \text{m.d.c.}(a, b)$, temos que $d \mid a$ e $d \mid b$, pelo que

$$d \mid (1 \cdot a + (-q)b),$$

ou seja, $d \mid r$.

(ii) Seja $c \in \mathbb{N}$ tal que $c \mid b$ e $c \mid r$. Então

$$c \mid (qb + r),$$

ou seja, $c \mid a$. Uma vez que $c \mid a$, $c \mid b$ e $d = \text{m.d.c.}(a, b)$, segue que $c \leq d$.

Teorema (Algoritmo de Euclides)

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

$$\begin{aligned}
a &= q_1 b + r_1 && e \quad 0 < r_1 < b \\
b &= q_2 r_1 + r_2 && e \quad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && e \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && e \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

então $\text{m.d.c.}(a, b) = r_n$.

Demonstração.

No processo de divisões indicado no enunciado, uma das divisões será exata, i.e., obter-se-á resto 0,

$$0 = r_{n+1} < r_n \ldots < r_5 < r_4 < r_3 < r_2 < r_1 < b,$$

sendo r_n o último resto não nulo.

Pelo lema anterior, temos

$$\begin{aligned} \text{m.d.c.}(a, b) &= \text{m.d.c.}(b, r_1) \\ &= \text{m.d.c.}(r_1, r_2) \\ &= \ldots \\ &= \text{m.d.c.}(r_{n-1}, r_n) \\ &= \text{m.d.c.}(r_n, 0) \end{aligned}$$

Como $\text{m.d.c.}(r_n, 0) = r_n$, temos, então, $\text{m.d.c.}(a, b) = r_n$. □

Divisibilidade

O máximo divisor comum de dois inteiros a, b, não simultaneamente nulos, é combinação linear de a e b, i.e., m.d.c.$(a, b) = ax + by$ para certos inteiros x, y. Nesta combinação linear, os coeficientes de a e b não estão univocamente determinados. A aplicação do Algoritmo de Euclides permite obter uma combinação linear de a e b.

Exemplo

Calcular o m.d.c.$(12378, 3054)$ e escrevê-lo como combinação linear de 12378 e 3054. Como

$$\begin{aligned} 12378 &= 4 \times 3054 + 162 && (1) \\ 3054 &= 18 \times 162 + 138 && (2) \\ 162 &= 1 \times 138 + 24 && (3) \\ 138 &= 5 \times 24 + 18 && (4) \\ 24 &= 1 \times 18 + 6 && (5) \\ 18 &= 3 \times 6 + 0 \end{aligned}$$

obtemos, pelo Algoritmo de Euclides, que m.d.c.$(12378, 3054) = 6$.

exemplo

Das igualdades (1), (2), (3), (4) e (5), obtemos

$$\begin{aligned}
6 &= 24 - 1 \times 18 && \text{por (5)}\\
&= 24 - (138 - 5 \times 24) && \text{por (4)}\\
&= 6 \times 24 - 1 \times 138\\
&= 6 \times (162 - 1 \times 138) - 138 && \text{por (3)}\\
&= 6 \times 162 - 7 \times 138\\
&= 6 \times 162 - 7(3954 - 18 \times 162) && \text{por (2)}\\
&= 132 \times 162 - 7 \times 3054\\
&= 132(12378 - 4 \times 3054) - 7 \times 3054 && \text{por (1)}\\
&= 132 \times 12378 - 535 \times 3054.
\end{aligned}$$

Assim, $x = 132$ e $y = -535$ são inteiros tais que

$$\text{m.d.c.}(12378, 3054) = 6 = 12378x + 3054y$$

Mínimo múltiplo comum

Dados inteiros a, b, c, diz-se que c é um múltiplo comum de a e b se $a \mid c$ e $b \mid c$.

Para quaisquer inteiros a, b, sabe-se que $a \mid 0$ e $b \mid 0$, pelo que 0 é um múltiplo comum de a e b.

Além disso, se $a, b \in \mathbb{Z} \setminus \{0\}$, $a \mid \pm ab$ e $b \mid \pm ab$ pelo que o conjunto

$$\{k \in \mathbb{N} : a \mid k \text{ e } b \mid k\}$$

é não vazio. Pelo Princípio da Boa Ordenação de $\mathbb{N}$, este conjunto tem elemento mínimo, i.e., existe o menor inteiro positivo múltiplo de a e de b, o que motiva a definição seguinte.

Definição

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

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

(ii) *se* $c \in \mathbb{N}$ *é tal que* $a \mid c$ *e* $b \mid c$, *então* $m \leq c$.

Se $a = 0$ *ou* $b = 0$ *diz-se que* $\text{m.m.c.}(a, b) = 0$.

Lema

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

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

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

É consequência imediata do lema anterior que, para quaisquer $a, b \in \mathbb{Z} \setminus \{0\}$, se $a \mid b$, então $|b| = \text{m.m.c.}(a, b)$.

Teorema

Para quaisquer inteiros positivos a e b,

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

O resultado do teorema anterior permite calcular o mínimo múltiplo comum de dois inteiros positivos recorrendo ao seu máximo divisor comum, sendo que este último poderá ser determinado aplicando o Algoritmo de Euclides.

Exemplo

$$\text{m.m.c.}(3054, 12378) = \frac{3054 \times 12378}{\text{m.d.c.}(3054,12378)} = \frac{3054 \times 12378}{6} = 6300402.$$

Corolário

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

$$\text{m.m.c.}(a, b) = ab \Leftrightarrow \text{m.d.c.}(a, b) = 1.$$

Teorema

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

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

(2) $\text{m.m.c.}(a, b) = \text{m.d.c.}(a, b) \Leftrightarrow a = \pm b$.

Números primos

Um dos conceitos fundamentais em teoria de números é o conceito de número primo. Os números primos funcionam como "blocos de contrução" de todos os inteiros positivos, pois todo o inteiro maior do que 1 pode ser fatorizado num produto de números primos.

Definição

Um inteiro $p > 1$ diz-se um **número primo** *se 1 e p forem os únicos divisores positivos de p.*
Um inteiro $k > 1$ que não seja um número primo diz-se um **número composto**.

Números primos

Teorema

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

Demonstração.

Admitamos que p é um número primo tal que $p \mid ab$ e $p \nmid a$. Então m.d.c.$(a, p) = 1$ e, portanto, pelo Lema de Euclides, $p \mid b$. □

Números primos

Exemplo

O inteiro 36 é divisível pelo número primo 3 e pode ser fatorizado das formas a seguir indicadas

$$36 = 3 \times 12, \quad 36 = 9 \times 4, \quad 36 = 18 \times 2, \quad 36 = 6 \times 6.$$

Em qualquer uma das fatorizações, 3 divide um dos fatores.

Números primos

O teorema anterior pode ser generalizado a produtos com mais do que dois fatores.

Corolário

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

Corolário

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

Números primos

O resultado seguinte, conhecido por *Teorema Fundamental da Aritmética*, é um resultado essencial no estudo da teoria de números. No Livro IX da obra *Os Elementos* encontram-se diversos resultados que motivaram este teorema, embora só mais tarde (em 1796) este tenha sido explicitamente estabelecido e demonstrado por Karl Gauss.

Teorema (Teorema Fundamental da Aritmética)

Todo o número inteiro $n > 1$ exprime-se como produto de um número finito de números primos. Esta representação é única a menos da ordem dos fatores.

Demonstração:

Seja $n \in \mathbb{Z}$ tal que $n > 1$.

existência

Se n é primo, então n escreve-se como produto de um único fator primo.

Se n não é primo, existe $d \in \mathbb{Z}$ tal que $1 < d < n$ e $d \mid n$.

Seja p_1 o menor inteiro positivo tal que $1 < p_1 < n$ e $p_1 \mid n$. Então p_1 é primo (caso contrário, existiria $q \in \mathbb{Z}$ tal que $1 < q < p_1$ e $q \mid p_1$; por conseguinte, tem-se que $q \mid n$, uma contradição).

Assim,

$$\exists n_1 \in \mathbb{Z} : \quad n = p_1 n_1 \text{ em que } p_1 \text{ é primo e } 1 < n_1 < n.$$

Números primos

Demonstração (continuação):

Se n_1 é primo, então n é produto de dois números primos.

Se n_1 não é primo, então existem p_2 primo e $1 < n_2 < n_1$ tais que $n_1 = p_2 n_2$, pelo que

$$n = p_1 p_2 n_2 .$$

Repetindo sucessivamente o raciocínio, obtem-se uma cadeia finita e decrescente de inteiros positivos

$$1 < \ldots < n_2 < n_1 < n,$$

pelo que, ao fim de um número finito de passos, obtemos um número primo.

Portanto,

$$n = p_1 p_2 \ldots p_k .$$

Demonstração (continuação):

unicidade

Sejam $r, s \in \mathbb{N}$ e $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ números primos tais que

$$n = p_1 p_2 \ldots p_r \quad \text{e} \quad n = q_1 q_2 \ldots q_s.$$

Suponhamos que $r \leq s$ e que

$$p_1 \leq p_2 \leq \ldots \leq p_r \quad \text{e} \quad q_1 \leq q_2 \leq \ldots q_s.$$

Como $p_1 \mid n$ e $n = q_1 q_2 \ldots q_s$,

$$p_1 \mid q_1 q_2 \ldots q_s$$

e, portanto, $p_1 = q_k$, para algum $k \in \{1, 2, \ldots, s\}$. Logo $q_1 \leq p_1$. De modo análogo, como $q_1 \mid n$ concluímos que $p_1 \leq q_1$. Logo $p_1 = q_1$.

Demonstração (continuação):

Então

$$p_1 p_2 \ldots p_r = p_1 q_2 \ldots q_s,$$

donde

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s.$$

Repetindo o processo anterior, obtem-se $p_2 = q_2$ e, portanto,

$$p_3 \ldots p_r = q_3 \ldots q_s.$$

Se admitirmos que $r < s$ e repetirmos o raciocínio sucessivamente, obtem-se

$$1 = q_{r+1} q_{r+2} \ldots q_s,$$

um absurdo (pois cada $q_j > 1$). O absurdo resultou de admitirmos que $r < s$. Logo, $r = s$, pelo que as duas fatorizações são iguais.

Corolário

Todo o número inteiro $n > 1$, 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

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

Exemplo

- $4725 = 3^3 \times 5^2 \times 7^1$.
- $17460 = 2^3 \times 3^2 \times 5^1 \times 7^2$.

Números primos

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

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

A possibilidade de se fatorizar qualquer inteiro positivo num produto de números primos permite estabelecer um outro método para o cálculo do máximo divisor comum e do mínimo múltiplo comum de quaisquer inteiros maiores do que 1.

Proposição

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

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

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

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

Exemplo

Sejam $a = 4725$ *e* $b = 17460$. *Fatorizando* a *e* b *em números primos, tem-se*

$$4725 = 2^0 \times 3^3 \times 5^2 \times 7^1$$

e

$$17460 = 2^3 \times 3^2 \times 5^1 \times 7^2,$$

pelo que

$$\text{m.d.c.}(4725, 17460) = 2^0 \times 3^2 \times 5^1 \times 7^1 = 315$$

e

$$\text{m.m.c.}(4725, 17460) = 2^3 \times 3^3 \times 5^2 \times 7^2 = 264600.$$

Números primos

Teorema

Existe uma infinidade de números primos.

Demonstração.

Admitamos que existe um número finito de números primos, i.e., suponhamos que

$$p_1, p_2, \ldots, p_k, \qquad (*)$$

onde $k \in \mathbb{N}$, são os únicos primos.

Consideremos

$$m = p_1 p_2 \ldots p_k + 1.$$

Como $m > 1$, m admite pelo menos um divisor primo p, ou seja, admite um divisor p que pertence à lista $(*)$.

Logo $p \mid m$ e $p \mid (p_1 p_2 \ldots p_k)$ e, portanto, $p \mid (m - p_1 p_2 \ldots p_k) = 1$. Assim, $p = 1$, o que contradiz o facto de p ser primo.

Logo, há uma infinidade de números primos. □

Números primos

Considerando a existência de uma infinidade de números primos, uma questão que se coloca no estudo dos números inteiros é a de como determinar se um dado inteiro positivo é ou não um número primo.

A abordagem óbvia para avaliar se um dado inteiro positivo n é primo consiste em averiguar se existe algum inteiro q tal que $1 < q < n$ e $q \mid n$; se nenhum destes inteiros dividir n significa que n é primo. Este método para avaliar se um certo inteiro positivo é primo não é eficiente quando se pretende estudar números elevados.

Apresenta-se seguidamente uma propriedade que permitir reduzir o número de cálculos necessários para determinar se um dado inteiro positivo é ou não um número primo.

Proposição

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

Demonstração.

Seja $a \in \mathbb{N}$.

Se a é um número composto, então $a = bc$ para alguns inteiros b e c tais que $1 < b < a$ e $1 < c < a$.

Admitamos que $b \leq c$. Então $b^2 \leq bc = a$, pelo que $b \leq \sqrt{a}$.

Uma vez que $b > 1$, b tem um divisor primo p.

Então $p \leq b \leq \sqrt{a}$ e, como $p \mid b$ e $b \mid a$, tem-se que $p \mid a$. □

Números primos

Observação: Sejam $a \in \mathbb{N} \setminus \{1\}$ e $R = \{p \in \mathbb{N} \mid p \text{ é primo e } p \leq \sqrt{a}\}$.

A proposição anterior estabelece que

$$a \text{ é composto} \Rightarrow (\exists_{p \in R}\ p \mid a)$$

o que é equivalente à proposição

$$(\forall_{p \in R}\ p \nmid a) \Rightarrow \ a \text{ é primo.}$$

Exemplo

Consideremos o número 509.

Como

$$22^2 = 484 \leq 509 \leq 529 = 23^2,$$

temos que

$$22 < \sqrt{509} < 23.$$

Os números primos não superiores a $\sqrt{509}$ são os números $2, 3, 5, 7, 11, 13, 17$ e 19.

Como nenhum destes números primos divide 509, podemos concluir que 509 é um número primo.

Números primos

Exemplo

O número 2093 é primo?

Como

$$45^2 = 2025 \leq 2093 \leq 2116 = 46^2,$$

temos

$$45 < \sqrt{2093} < 46.$$

Os primos não superiores a $\sqrt{2093}$ são os números

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.$$

Tem-se que $2 \nmid 2093$, $3 \nmid 2093$, $5 \nmid 2093$, mas $7 \mid 2093$ ($2093 = 7 \times 299$).

Como $2093 = 7 \times 299$, o número 2093 não é primo.

Números primos

Exemplo (continuação):

No sentido de determinar a fatorização de 2093 num produto de números primos, estudemos a primalidade de 299.

Uma vez que

$$17^2 = 289 < 299 < 324 = 18^2,$$

tem-se

$$17 = \sqrt{289} < \sqrt{299} < \sqrt{324} = 18,$$

pelo que os números primos não superiores a $\sqrt{299}$ são

$$2, 3, 5, 7, 11, 13, 17.$$

Tem-se que

$$2 \nmid 299, 3 \nmid 299, 5 \nmid 299, 7 \nmid 299, 11 \nmid 299 \text{ e } 13 \mid 299 \ (299 = 13 \times 23).$$

Assim,

$$2093 = 7 \times 13 \times 23,$$

onde 7, 13 e 23 são números primos.

Números primos

O matemático grego Erastótenes (276-194 a.c.) elaborou um algoritmo para determinar todos os números primos inferiores a um dado número natural n. Este algoritmo, conhecido como *crivo de Erastótenes*, é baseado na proposição anterior e consiste no seguinte:

1. Listam-se todos os inteiros de 2 a n de acordo com a ordem usual.
2. Eliminam-se todos os números compostos, cancelando todos os que sejam múltiplos de primos p, com p tais que $p \leq \sqrt{n}$.
3. Os elementos restantes (i.e., os números que não passaram no crivo) são os primos inferiores a n.

Números primos

Exemplo

Quais os números primos inferiores a 100?

Comecemos por listar todos os números de 2 a 100.

	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

Os números primos menores ou iguais a $\sqrt{100}$ são os números 2, 3, 5 e 7.

Números primos

Exemplo (continuação):

Seguidamente cancelam-se todos os números compostos múltiplos de 2, de 3, de 5 e de 7.

	2	3	■	5	■	7	■	■	■
11	■	13	■	■	■	17	■	19	■
■	■	23	■	■	■	■	■	29	■
31	■	■	■	■	■	37	■	■	■
41	■	43	■	■	■	47	■	■	■
■	■	53	■	■	■	■	■	59	■
61	■	■	■	■	■	67	■	■	■
71	■	73	■	■	■	■	■	79	■
■	■	83	■	■	■	■	■	89	■
■	■	■	■	■	■	97	■	■	■

O cancelamento anterior permitiu eliminar todos os números compostos não superiores a 100. Portanto, os números primos menores do que 100 são:

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$

Equações diofantinas

São frequentes os problemas cuja resoluçao implica determinar soluções inteiras de equações com uma ou mais variáveis e cujos coeficientes são inteiros. A este tipo de equações dá-se a designação de *equações diofantinas*, em homenagem ao matemático Diophantus (250 a.c.), o qual estudou equações similares na sua obra chamada *Arithmetica*.

Equações diofantinas

Exemplo

O envio de uma encomenda tem um custo de $1,83$ euros. Se os únicos selos disponíveis para o envio da encomenda são de 12 cêntimos e de 15 cêntimos, quantos selos de cada tipo serão necessários para o envio da encomenda?

O problema anterior pode ser modelado pela equação seguinte

$$12x + 15y = 183,$$

onde x e y são, respetivamente, o número de selos de 12 cêntimos e o número de selos de 15 cêntimos.

Equações diofantinas

Definição

Uma **equação diofantina** *é uma equação do tipo*

$$a_1 {x_1}^{n_1} + a_2 {x_2}^{n_2} + \ldots + a_k {x_k}^{n_k} = c,$$

onde, para cada $i \in \{1, 2, \ldots, k\}$, $n_i \in \mathbb{N}$, $a_i \in \mathbb{Z}$ *e* $c \in \mathbb{Z}$.

Estudaremos equações diofantinas lineares com duas variáveis, i.e., equações do tipo

$$ax + by = c$$

onde $a, b, c \in \mathbb{Z}$ e a, b não são simultaneamente nulos.

Equações diofantinas

Chama-se **solução da equação** $ax + by = c$ a qualquer par $(x', y') \in \mathbb{Z} \times \mathbb{Z}$ tal que $ax' + by' = c$.

Resolver a equação diofantina $ax + by = c$ é determinar o conjunto de todas as suas soluções.

A equação $ax + by = c$ **diz-se solúvel** se admite pelo menos uma solução.

Equações diofantinas

Uma equação diofantina pode ter mais do que uma solução, como é o caso da equação $3x + 6y = 18$, pois

$$3 \times 4 + 6 \times 1 = 18,$$

$$3 \times (-6) + 6 \times 6 = 18.$$

Outras equações podem não ter solução. A equação

$$8x + 2y = 15$$

não tem solução, pois, para quaisquer $x, y \in \mathbb{Z}$, $8x + 2y$ é um número par e 15 é um número ímpar.

Proposição

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

Demonstração.

Seja $d = \text{m.d.c.}(a, b)$. Então $d \mid a$ e $d \mid b$, pelo que $d \mid ax + by$, para quaisquer $x, y \in \mathbb{Z}$.

Assim, se a equação $ax + by = c$ tem solução, então $d \mid c$.

Se $d \mid c$, existe $k \in \mathbb{Z}$ tal que

$$c = dk.$$

Considerando que $d = \text{m.d.c.}(a, b)$,

$$\exists_{x_0, y_0 \in \mathbb{Z}} \; d = ax_0 + by_0.$$

Logo,

$$c = (ax_0 + by_0)k = a(x_0 k) + b(y_0 k)$$

e, portanto, $(x_0 k, y_0 k)$ é solução da equação diofantina $ax + by = c$. $\square$

Equações diofantinas

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.

Demonstração.

Sejam $d = \text{m.d.c.}(a, b)$ e (x_0, y_0) uma solução particular de $ax + by = c$. Para qualquer $t \in \mathbb{Z}$, o par

$$\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$$

é também solução da equação $ax + by = c$. De facto,

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = ax_0 + by_0 = c.$$

Assim, caso seja solúvel, a equação $ax + by = c$ tem 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*

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

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

Exemplo

Consideremos a equação $172x + 20y = 1000$.

A equação indicada é solúvel?

Para averiguar se a equação é solúvel, comecemos por determinar m.d.c.$(172, 20)$. Tem-se

$$\begin{aligned} 172 &= 8 \times 20 + 12, && \text{com } 0 < 12 < 20 \\ 20 &= 1 \times 12 + 8, && \text{com } 0 < 8 < 12 \\ 12 &= 1 \times 8 + 4, && \text{com } 0 < 4 < 8 \\ 8 &= 2 \times 4 + 0 \end{aligned}$$

e, portanto, m.d.c.$(172, 20) = 4$.

Como $4 \mid 1000$, a equação $172x + 20y = 1000$ admite soluções.

Exemplo (continuação):

Determinemos, caso existam, as soluções (x, y) da equação $172x + 20y = 1000$ tais que $x, y > 0$.

Para tal, calculemos primeiramente a solução geral da equação.

Como

$$\begin{aligned} 4 &= 12 - 1 \times 8 \\ &= 12 - 1 \times (20 - 1 \times 12) \\ &= 2 \times 12 - 1 \times 20 \\ &= 2 \times (172 - 8 \times 20) - 1 \times 20 \\ &= 2 \times 172 - 17 \times 20, \end{aligned}$$

temos

$$1000 = 4 \times 250 = 172 \times 500 + 20 \times (-4250)$$

e, portanto, $(500, -4250)$ é uma solução particular da equação.

Exemplo (continuação):

Logo, $(x', y') \in \mathbb{Z} \times \mathbb{Z}$, com

$$\begin{cases} x' &= 500 + \frac{20}{4}t \\ y' &= -4250 - \frac{172}{4}t \end{cases}, t \in \mathbb{Z}, i.e., \begin{cases} x' &= 500 + 5t \\ y' &= -4250 - 43t \end{cases}, t \in \mathbb{Z},$$

é a solução geral da equação.

Determinemos, agora, as soluções (x, y) tais que $x, y > 0$.

Tem-se

$$\begin{cases} x > 0 \\ y > 0 \end{cases} \Leftrightarrow \begin{cases} 500 + 5t > 0 \\ -4250 - 43t > 0 \end{cases} \Leftrightarrow \begin{cases} t > -100 \\ t < -\frac{4250}{43} \approx -98,83 \end{cases}$$

Exemplo (continuação):

Como t é um inteiro, tem-se $t = -99$, pelo que a equação tem uma única solução (x, y) tal que $x, y > 0$, sendo essa solução o par

$$\begin{aligned}(x, y) &= (500 + 5 \times (-99), -4250 - 43 \times (-99)) \\ &= (5, 7).\end{aligned}$$

Exemplo

Tenho um certo número de pérolas. Se fizer 76 pulseiras todas com o mesmo número de pérolas, faltam 50 pérolas para fazer a 77^a pulseira. Se fizer 78 pulseiras com o mesmo número de pérolas, uso a totalidade de pérolas. Qual o número mínimo de pérolas que tenho?

O problema pode ser modelado pela equação $76x + (x - 50) = 78y$, i.e.,

$$77x - 78y = 50.$$

Como m.d.c.$(77, -78) = 1$ e $1 \mid 50$, a equação é solúvel.

De $1 = 77 \times (-1) + (-78) \times (-1)$, obtemos

$$50 = 77 \times (-50) + (-78) \times (-50)$$

pelo que $(-50, -50)$ é uma solução particular da equação.

Exemplo (continuação:)

As soluções do problema são os pares (x, y) tais que

$$\begin{cases} 77x - 78y = 50 \\ x > 0 \\ y > 0 \end{cases}$$

o que equivale a

$$\begin{cases} x = -50 + (-78)t \\ y = -50 - 77t \\ x > 0 \\ y > 0 \end{cases}, \text{ com } t \in \mathbb{Z}.$$

Assim, as soluções são os pares (x, y) tais que

$$\begin{cases} x = -50 - 78t \\ y = -50 - 77t \end{cases}, \text{ com } t \leq -1.$$

Exemplo (continuação:)

Portanto, o número mínimo de pérolas que tenho é

$$78y = 78 \times (-50 - 77 \times (-1)) = 2106.$$

Com esse número de pérolas fazem-se 78 pulseiras com 27 pérolas cada.

Congruências módulo n

Uma das obras mais marcantes no estudo da teoria de números é a obra *Disquisitiones Arithmeticae* do matemático alemão Karl Gauss (1777-1855). Nesta obra, Karl Gauss introduz e desenvolve o estudo da teoria de conguências. As relações de congruência, como iremos ver mais à frente, satisfazem bastantes propriedades semelhantes às da relação de igualdade, o que motivou a notação introduzida por Karl Gauss para as relações de congruência. O conceito de relação congruência permite estudar questões de divisibilidade com base na aritmética dos restos.

Definições e resultados básicos

Definição

Seja $n \in \mathbb{N}$. Diz-se que um inteiro a **é congruente módulo n com um inteiro** *b, e escreve-se $a \equiv b (\mathrm{mod}\, n)$, 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 $a \not\equiv b (\mathrm{mod}\, n)$ e diz-se que a é* **incongruente com b módulo n.**

Exemplo

$$3 \equiv 24 (\mathrm{mod}\, 7), \quad -31 \equiv 11 (\mathrm{mod}\, 7), \quad -15 \equiv -64 (\mathrm{mod}\, 7),$$

pois

$$3 - 24 = (-3) \times 7, \quad -31 - 11 = (-6) \times 7, \quad -15 - (-64) = 7 \times 7.$$

Congruências módulo n

Teorema

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

$$a \equiv b (\mathrm{mod}\, n) \Leftrightarrow a \text{ e } b \text{ têm o mesmo resto na divisão por } n.$$

Demonstração:

Seja $n \in \mathbb{N}$. Para quaisquer $a, b \in \mathbb{Z}$, tem-se que

$$a \equiv b (\mathrm{mod}\, n) \Leftrightarrow \exists_{k \in \mathbb{Z}} \ a - b = nk \Leftrightarrow \exists_{k \in \mathbb{Z}} \ a = b + kn.$$

Pelo Algoritmo da Divisão, existem $q, r \in \mathbb{Z}$ tais que

$$b = qn + r \quad \text{e} \quad 0 \leq r < n.$$

Logo,

$$a = qn + r + kn = (q + k)n + r, \text{ com } q + k \in \mathbb{Z} \text{ e } 0 \leq r < n.$$

Assim, a e b têm o mesmo resto na divisão por n.

Demonstração (continuação):

Reciprocamente, suponhamos que existem $q, q', r \in \mathbb{Z}$ tais que

$$a = qn + r, \quad b = q'n + r \quad \text{e} \quad 0 \leq r < n.$$

Então

$$a - b = qn + r - q'n - r = (q - q')n,$$

com $q - q' \in \mathbb{Z}$, pelo que

$$n \mid a - b,$$

ou seja,

$$a \equiv b (\mathrm{mod}\, n).$$

Exemplo

- Os inteiros -56 e -11 têm o mesmo na divisão por 9, pois

$$-56 = 9 \times (-7) + 7 \quad \text{e} \quad -11 = 9 \times (-2) + 7.$$

Por conseguinte, pelo teorema anterior,

$$-56 \equiv -11 (\mathrm{mod}\, 9).$$

De facto, $9 \mid (-56) - (-11)$, pois $(-56) - (-11) = -45 = 9 \times (-5)$.

- Os inteiros -40 e 13 não têm o mesmo resto na divisão por 3, pois

$$-40 = 3 \times (-14) + 2, \text{ com } 0 \leq 2 < 3,$$

$$13 = 3 \times 4 + 1, \text{ com } 0 \leq 1 < 3,$$

pelo que -40 e 13 têm, respetivamente, resto 2 e 1 na divisão inteira por 3. Então, pelo teorema anterior, $-40 \not\equiv 13 (\mathrm{mod} 3)$. De facto, $3 \nmid -40 - 13$, pois $-53 \neq 3 \times k$, para todo $k \in \mathbb{Z}$.

Exemplo

- Uma vez que $(-31) \equiv 11 (\mathrm{mod}\, 7)$, pode-se concluir, pelo teorema anterior, que -31 e 11 têm o mesmo resto na divisão por 7. Tal pode ser confirmado pelas igualdades seguintes

$$-31 = 7 \times (-5) + 4, \quad 11 = 7 \times 1 + 4,$$

onde $0 \leq 4 < 7$.

Congruências módulo n

Sejam $n \in \mathbb{N}$ e $a \in \mathbb{Z}$. Pelo Algoritmo da Divisão, existem e estão univocamente determinados, inteiros $q, r \in \mathbb{Z}$ tais que

$$a = qn + r \quad \text{e} \quad 0 \leq r < n,$$

i.e., tais que

$$a - r = qn \quad \text{e} \quad 0 \leq r < n.$$

Portanto, a é congruente módulo n com o resto da sua divisão por n.

Assim, temos o seguinte corolário.

Corolário

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

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

Congruências módulo n

Definição

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

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

Exemplo

Sejam $A = \{1, 2, 3, 4\}$, $B = \{4, 50, -5, -3\}$ e $C = \{0, 1, 2, 4\}$.

Os conjuntos A e B são sistemas completos de resíduos módulo 4:

- conjunto A: como $1 \equiv 1 (\mathrm{mod}\, 4)$, $2 \equiv 2 (\mathrm{mod}\, 4)$, $3 \equiv 3 (\mathrm{mod}\, 4)$ e $4 \equiv 0 (\mathrm{mod}\, 4)$, todo o inteiro é congruente mod 4 com um e um só dos elementos de $\{1, 2, 3, 4\}$.

- conjunto B: como $4 \equiv 0 (\mathrm{mod}\, 4)$, $-3 \equiv 1 (\mathrm{mod}\, 4)$, $50 \equiv 2 (\mathrm{mod}\, 4)$ e $-5 \equiv 3 (\mathrm{mod}\, 4)$, todo o inteiro é congruente mod 4 com um e um só dos elementos de $\{4, 50, -5, -3\}$.

O conjunto C não é um sistema completo de resíduos módulo 4, pois

$$0, 4 \in C, \quad 4 \neq 0 \quad \text{e} \quad 4 \equiv 0 (\mathrm{mod}\, 4).$$

Congruências módulo n

Teorema

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

(i) $a \equiv a (\mathrm{mod}\, n)$;

(ii) $a \equiv b (\mathrm{mod}\, n) \Rightarrow b \equiv a (\mathrm{mod}\, n)$;

(iii) $a \equiv b (\mathrm{mod}\, n)$ *e* $b \equiv c (\mathrm{mod}\, n) \Rightarrow a \equiv c (\mathrm{mod}\, n)$;

(iv) $a \equiv b (\mathrm{mod}\, n)$ *e* $c \equiv d (\mathrm{mod}\, n) \Rightarrow \begin{cases} ac \equiv bd (\mathrm{mod}\, n) \\ a + c \equiv b + d (\mathrm{mod}\, n) \end{cases}$;

(v) $a \equiv b (\mathrm{mod}\, n) \Rightarrow \begin{cases} ac \equiv bc (\mathrm{mod}\, n) \\ a + c \equiv b + c (\mathrm{mod}\, n) \end{cases}$;

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

Demonstração.

Apresentamos a prova de (iv) ficando como exercício a prova das restantes propriedades.

Suponhamos que

$$a \equiv b (\mathrm{mod}\, n) \quad \text{e} \quad c \equiv d (\mathrm{mod}\, n).$$

Então

$$n \mid a - b \quad \text{e} \quad n \mid c - d.$$

Logo, para quaisquer $x, y \in \mathbb{Z}$,

$$n \mid (a - b)x + (c - d)y.$$

Se considerarmos $x = 1$ e $y = 1$, então $n \mid (a + c) - (b + d)$ e, portanto, $a + c \equiv b + d (\mathrm{mod}\, n)$.

Considerando $x = c$ e $y = b$, tem-se que $n \mid ac - bd$, pelo que $ac \equiv bd (\mathrm{mod}\, n)$. □

Congruências módulo n

Se $a \equiv b \pmod{n}$, também se tem $b \equiv a \pmod{n}$, pelo que diremos apenas que a e b são congruentes módulo n.

As propriedades da relação $\equiv \pmod{n}$ apresentadas no teorema anterior são similares a propriedades satisfeitas pela relação de igualdade. Em particular, a relação $\equiv \pmod{n}$ respeita a adição e a multiplicação de inteiros, pelo que dizemos que a relação $\equiv \pmod{n}$ **é compatível com a adição e a multiplicação em** $\mathbb{Z}$.

Como iremos ver a seguir, nem todas as propriedades satisfeitas pela relação de igualdade são válidas para as congruências.

Lei do corte

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

$$a \equiv b (\mathrm{mod} n) \Rightarrow ac \equiv bc (\mathrm{mod} n),$$

porém, o recíproco nem sempre é verdade. Por exemplo, se $n = 6$, $a = 1$, $b = 4$, $c = 2$, tem-se

$$1 \times 2 \equiv 4 \times 2 (\mathrm{mod}\, 6) \text{ mas } 1 \not\equiv 4 (\mathrm{mod}\, 6).$$

A relação $\equiv (\mathrm{mod}\, n)$ não satisfaz a lei do corte, mas sob certas condições o cancelamento pode ser válido.

Teorema

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

Demonstração.

Suponhamos que $ca \equiv cb (\mathrm{mod}\, n)$. Então $n \mid ca - cb$, i.e.,

$$c(a-b) = kn, \text{ para algum } k \in \mathbb{Z}. \qquad (*)$$

Seja $d = \text{m.d.c.}(c, n)$. Então existem $r, s \in \mathbb{Z}$ tais que

$$c = dr \text{ e } n = ds.$$

Substituindo em $(*)$, obtemos

$$dr(a-b) = kds$$

e, portanto,

$$r(a-b) = ks.$$

Logo,

$$s \mid r(a-b).$$

Como r e s são primos entre si, segue que $s \mid a - b$ (Lema de Euclides), ou seja,

$$a \equiv b (\mathrm{mod}\, s), \text{ onde } s = \frac{n}{d}.$$

Corolário

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

Corolário

Sejam $p \in \mathbb{N}$ *e* $a, b, c \in \mathbb{Z}$. *Se* $ca \equiv cb (\mathrm{mod}\, p)$, p *é um número primo e* $p \nmid c$, *então* $a \equiv b (\mathrm{mod}\, p)$.

Exemplo

Consideremos a congruência $33 \equiv 15 (\mathrm{mod}\, 9)$. Como

$$3 \times 11 \equiv 3 \times 5 (\mathrm{mod}\, 9) \text{ e } \mathrm{m.d.c.}(9, 3) = 3,$$

então

$$11 \equiv 5 \left(\mathrm{mod}\, \frac{9}{\mathrm{m.d.c.}(9, 3)} \right), \text{ ou seja } 11 \equiv 5 (\mathrm{mod}\, 3).$$

Consideremos, agora, a congruência $-35 \equiv 45 (\mathrm{mod}\, 8)$. Uma vez que

$$5 \times (-7) \equiv 5 \times 9 (\mathrm{mod}\, 8) \text{ e } \mathrm{m.d.c.}(5, 8) = 1,$$

então

$$-7 \equiv 9 (\mathrm{mod}\, 8).$$

Lei do anulamento do produto

A lei do anulamento do produto, válida para a relação de igualdade (quando se considera a multiplicação usual em $\mathbb{Z}$), nem sempre é válidade para a relação $\equiv (\mathrm{mod}\, n)$, ou seja, nem sempre é verdade que dados $a, b \in \mathbb{Z}$ a implicação seguinte seja válida

$$ab \equiv 0(\mathrm{mod}\, n) \Rightarrow (a \equiv 0(\mathrm{mod}\, n) \text{ ou } b \equiv 0(\mathrm{mod}\, n)).$$

Por exemplo,

$$2 \times 3 \equiv 0(\mathrm{mod}\, 6), \quad 2 \not\equiv 0(\mathrm{mod}\, 6) \text{ e } 3 \not\equiv 0(\mathrm{mod}\, 6).$$

Teorema

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

Demonstração.

Imediato, considerando o penúltimo corolário e atendendo a que

$$ab \equiv 0 (\mathrm{mod}\, n) \Leftrightarrow ab \equiv a \times 0 (\mathrm{mod}\, n).$$

□

Congruências módulo n

Seja $n \in \mathbb{N}$. Considerando que, para quaisquer $a, b, c \in \mathbb{Z}$, tem-se

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

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

Esta relação 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.

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

Congruências módulo n

Sendo r o resto da divisão de a por n, tem-se

$$a \equiv r \pmod{n},$$

logo

$$[a]_n = [r]_n.$$

Assim, existem exatamente n classes de equivalência módulo n:

$$[0]_n, [1]_n, \ldots, [n-1]_n.$$

O conjunto quociente

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

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

Congruências módulo n

Como já verificámos anteriormente, a relação $\equiv \pmod{n}$ é compativel com as operações de adição e de multiplicação de inteiros, o que permite definir em $\mathbb{Z}_n$ as seguintes operações:

- $[a]_n + [b]_n = [a+b]_n$, para quaisquer $[a]_n, [b]_n \in \mathbb{Z}_n$;
- $[a]_n [b]_n = [ab]_n$, para quaisquer $[a]_n, [b]_n \in \mathbb{Z}_n$.

Apresentam-se seguidamente alguns exemplos onde se pode verificar a utilidade da aplicação da teoria de congruências na resolução de questões relacionadas com divisibilidade.

Exemplo

Mostrar que $41 \mid 2^{20} - 1$.

Tem-se

$$41 \mid 2^{20} - 1 \Leftrightarrow 2^{20} \equiv 1 (\mathrm{mod}\, 41).$$

Então, como

$$2^5 = 32 \equiv (-9) (\mathrm{mod}\, 41),$$

segue que

$$2^{20} = (2^5)^4 \equiv (-9)^4 (\mathrm{mod}\, 41). \quad (1)$$

Como

$$(-9)^2 = 81 \equiv (-1) (\mathrm{mod}\, 41),$$

tem-se

$$(-9)^4 = ((-9)^2)^2 \equiv 1 (\mathrm{mod}\, 41). \quad (2)$$

De (1) e (2), concluímos que $2^{20} \equiv 1 (\mathrm{mod}\, 41)$.

Exemplo

Determinar o resto da divisão de $\sum_{n=1}^{100} n!$ por 12.

Como $4! = 24 \equiv 0 (\mathrm{mod}\, 12)$, então, para $n \geq 4$,

$$n! = n(n-1)\ldots 5 \cdot 4! \equiv 0 (\mathrm{mod}\, 12).$$

Logo,

$$\sum_{n=1}^{100} n! = 1! + 2! + 3! + \sum_{n=4}^{100} n! \equiv 1 + 2 + 6 + 0 (\mathrm{mod}\, 12),$$

ou seja,

$$\sum_{n=1}^{100} n! \equiv 9 (\mathrm{mod}\, 12).$$

Assim , o resto da divisão de $\sum_{n=1}^{100} n!$ por 12 é 9.

Critérios de divisibilidade

A teoria de congruências possibilita a definição de critérios que permitem avaliar de forma simples se um certo inteiro é ou não divisível por outro. Estes critérios, designados por critérios de divisibilidade, estão dependentes do sistema de numeração adotado para representar os números inteiros, sendo que os critérios aqui apresentados são definidos com base na sua representação decimal.

Congruências módulo n

Se $a_0, a_1, \ldots, a_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, o número

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

é representado por

$$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0}.$$

A esta representação chamamos **representação decimal de a.**
Aos inteiros a_0, a_1, ..., a_n dá-se a designação de **dígitos** ou **algarismos** de a. Se $a_n \neq 0$, o número a tem $n + 1$ algarismos. Os inteiros a_0, a_1, a_2 designam-se, respetivamente, por dígito das unidades, dígito das dezenas e dígito das centenas do inteiro a.

Não havendo ambiguidade, não se coloca a barra na representação do inteiro. Por exemplo,

$$1492 = 1 \times 10^3 + 4 \times 10^2 + 9 \times 10 + 2$$

e

$$\overline{5p8} = 5 \times 10^2 + p \times 10 + 8.$$

Congruências módulo n

Teorema

Seja $n \in \mathbb{N}$. Se $r_1, r_2, \ldots, r_{n-1}, r_n$ são os restos da divisão de, respetivamente, $10, 10^2, \ldots, 10^{n-1}, 10^n$ por n, então

$$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv a_n r_n + a_{n-1} r_{n-1} + \ldots + a_2 r_2 + a_1 r_1 + a_0 (\mathrm{mod}\, n).$$

Exemplo

Pretendemos determinar o resto da divisão de 1492 por 3.

Como

$$\begin{aligned} 10 &\equiv 1 (\mathrm{mod}\, 3), \\ 10^2 = 100 &\equiv 1 (\mathrm{mod}\, 3), \\ 10^3 = 1000 &\equiv 1 (\mathrm{mod}\, 3), \end{aligned}$$

então

$$1492 = 1 \times 10^3 + 4 \times 10^2 + 9 \times 10 + 2 \equiv 1 \times 1 + 4 \times 1 + 9 \times 1 + 2 (\mathrm{mod}\, 3),$$

ou seja,

$$1492 \equiv 16 (\mathrm{mod}\, 3).$$

Uma vez que $16 \equiv 1 (\mathrm{mod}\, 3)$, segue que

$$1492 \equiv 1 (\mathrm{mod}\, 3).$$

Logo, o resto da divisão de 1492 por 3 é 1.

Congruências módulo n

Considerando a representação decimal de inteiros, estabelecemos de seguida os critérios de divisibilidade por 2, 3, 5, 9, 4 e 11.

- $n = 2$

  Como $10 \equiv 0 (\mathrm{mod}\, 2)$, temos $10^i \equiv 0 (\mathrm{mod}\, 2)$, para qualquer inteiro $i \geq 1$. Logo, pelo teorema anterior,

  $$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv a_0 (\mathrm{mod}\, 2).$$

  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.

Congruências módulo n

- $n = 5$

  Como $10 \equiv 0 (\mathrm{mod}\, 5)$, temos que $10^i \equiv 0 (\mathrm{mod}\, 5)$, para qualquer inteiro $i \geq 1$. Logo,

  $$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv a_0 (\mathrm{mod}\, 5).$$

  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.

- $n = 3$

  Como $10 \equiv 1 (\mathrm{mod}\, 3)$, temos que $10^i \equiv 1 (\mathrm{mod}\, 3)$, para qualquer inteiro $i \geq 1$. Logo,

  $$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 (\mathrm{mod}\, 3).$$

  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.

- $n = 9$

  Como $10 \equiv 1 (\mathrm{mod}\, 9)$, temos que $10^i \equiv 1 (\mathrm{mod}\, 9)$, para qualquer inteiro $i \geq 1$. Logo,

  $$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 (\mathrm{mod}\, 9).$$

  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.

- $n = 4$

  Como $10 \equiv 2 (\mathrm{mod}\, 4)$, temos que $10^2 \equiv 0 (\mathrm{mod}\, 4)$ e, portanto, $10^i \equiv 0 (\mathrm{mod}\, 4)$, para qualquer inteiro $i \geq 2$. Logo,

  $$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv 2 \times a_1 + a_0 (\mathrm{mod}\, 4).$$

  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.

- $n = 11$

  Como $10 \equiv (-1) (\mathrm{mod}\, 11)$, temos que $10^2 \equiv 1 (\mathrm{mod}\, 11)$ e, portanto, $10^i \equiv (-1)^i (\mathrm{mod}\, 11)$, para qualquer inteiro $i \geq 1$. Logo,

  $$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) (\mathrm{mod}\, 11).$$

  Critério de divisibilidade por 11: O resto da divisão de um inteiro positivo a por 11 é o resto que se obtém dividindo por 11 a diferença entre a soma dos algarismos de a de ordem par e a soma dos algarismos de a de ordem ímpar (considerando que o algarismo das unidades é de ordem par).

Exemplo

Determinar $x, y \in \{0,1,2,3,4,5,6,7,8,9\}$ de modo que o inteiro $n = \overline{3x5y}$ seja simultaneamente divisível por 4 e por 9.

Dado um inteiro a, tem-se

$$4 \mid a \Leftrightarrow a \equiv 0 (\mathrm{mod}\, 4).$$

Considerando o inteiro n e o critério de divisibilidade por 4, tem-se

$$4 \mid n \Leftrightarrow 2 \times 5 + y \equiv 0 (\mathrm{mod}\, 4).$$

Além disso,

$$\begin{array}{lllll} 2 \times 5 + y \equiv 0 (\mathrm{mod}\, 4) & \Leftrightarrow & 10 + y \equiv 0 (\mathrm{mod}\, 4) & \Leftrightarrow & 2 + y \equiv 0 (\mathrm{mod}\, 4) \\ & \Leftrightarrow & y \equiv -2 (\mathrm{mod}\, 4) & \Leftrightarrow & y \equiv 2 (\mathrm{mod}\, 4). \end{array}$$

Como $y \in \{0,1,2,3,4,5,6,7,8,9\}$, então $y \in \{2,6\}$.

Exemplo (continuação):

Analisemos, agora, a divisibilidade de n por 9. Tem-se

$$9 \mid n \Leftrightarrow n \equiv 0 (\mathrm{mod}\, 9).$$

Considerando o critério de divisibilidade por 9, segue que

$$n \equiv 0 (\mathrm{mod}\, 9) \Leftrightarrow 3 + x + 5 + y \equiv 0 (\mathrm{mod}\, 9) \Leftrightarrow 8 + x + y \equiv 0 (\mathrm{mod}\, 9).$$

Se $y = 2$, obtemos

$$10 + x \equiv 0 (\mathrm{mod}\, 9) \Leftrightarrow x \equiv -10 (\mathrm{mod}\, 9) \Leftrightarrow x \equiv 8 (\mathrm{mod}\, 9).$$

Como $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, então $x = 8$. Logo, $n = 3852$.

Se $y = 6$, obtemos

$$14 + x \equiv 0 (\mathrm{mod}\, 9) \Leftrightarrow x \equiv -14 (\mathrm{mod}\, 9) \Leftrightarrow x \equiv 4 (\mathrm{mod}\, 9).$$

Como $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, então $x = 4$. Logo, $n = 3456$.

Congruências lineares

Definição

Chama-se **congruência linear** *a toda a expressão da forma* $ax \equiv b (\mathrm{mod}\, n)$ *em que* $a, b \in \mathbb{Z}$ *e* x *é um símbolo.*
Chama-se **solução da congruência linear** $ax \equiv b (\mathrm{mod}\, n)$ *a qualquer inteiro* x_0 *tal que "*$ax_0 \equiv b (\mathrm{mod}\, n)$*"é uma afirmação verdadeira.*

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

Exemplo

A congruência linear $4x \equiv 5 (\mathrm{mod}\, 6)$ não tem soluções em $\mathbb{Z}$, uma vez que, para qualquer $x \in \mathbb{Z}$, $6 \nmid 4x - 5$; de facto, para todo $y \in \mathbb{Z}$, $4x - 5 \neq 6y$, uma vez que $4x - 5$ é um inteiro ímpar e $6y$ é um inteiro par.

Exemplo

A congruência linear $3x \equiv 9 (\mathrm{mod}\, 12)$ admite, entre outras, as soluções $x_0 = 3$, $x_1 = -9$ e $x_2 = 7$. Observe-se que $x_0 \equiv x_1 (\mathrm{mod}\, 12)$ e $x_0 \not\equiv x_2 (\mathrm{mod}\, 12)$.

Do exemplo anterior conclui-se que, de entre as soluções de uma congruência linear, existem soluções que são congruentes entre si e outras que não o são.

Como se verá na demonstração da proposição seguinte, a solubilidade e o processo de resolução de uma congruência linear estão relacionados com a solubilidade e a resolução de uma equação diofantina.

Teorema

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

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

é a lista completa das soluções da congruência linear $ax \equiv b (\text{mod}\, n)$, *não congruentes módulo* n.

Demonstração:

Seja $d = \text{m.d.c.}(a, n)$. Tem-se

$$\begin{aligned} ax \equiv b(\text{mod}\, n) \text{ é solúvel} &\Leftrightarrow \exists_{x_0 \in \mathbb{Z}}\ ax_0 \equiv b(\text{mod}\, n) \\ &\Leftrightarrow \exists_{x_0 \in \mathbb{Z}}\ n \mid (ax_0 - b) \\ &\Leftrightarrow \exists_{x_0, y_0 \in \mathbb{Z}}\ ax_0 - b = ny_0 \\ &\Leftrightarrow \exists_{x_0, y_0 \in \mathbb{Z}}\ ax_0 + (-n)y_0 = b \\ &\Leftrightarrow \text{ a equação diofantina } ax + (-n)y = b \text{ é solúvel} \\ &\Leftrightarrow d \mid b. \end{aligned}$$

Assim, a congruência linear $ax \equiv b(\text{mod}\, n)$ é solúvel se e só se $\text{m.d.c.}(a, n) \mid b$.

Demonstração:

Vejamos, agora, quais são as soluções de uma congruência linear $ax \equiv b (\mathrm{mod}\, n)$ solúvel.

$$
\begin{aligned}
& x_0 \text{ é solução de } ax \equiv b (\mathrm{mod}\, n) \\
\Rightarrow \quad & \exists_{y_0 \in \mathbb{Z}} \ (x_0, y_0) \text{ é solução da equação diofantina } ax - ny = b \\
\Rightarrow \quad & (x_0 + \tfrac{-n}{d} t, y_0 - \tfrac{a}{d} t), \text{ com } t \in \mathbb{Z}, \text{ é a solução geral da equação} \\
\Rightarrow \quad & \forall_{t \in \mathbb{Z}}, x' = x_0 + \tfrac{-n}{d} t \text{ é solução da congruência linear } ax \equiv b (\mathrm{mod}\, n).
\end{aligned}
$$

Considerando $t \in \{-(d-1), -(d-2), \ldots, -1, 0\}$, obtemos as d soluções

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

da congruência linear $ax \equiv b (\mathrm{mod}\, n)$.

Demonstração (continuação):

Vejamos que:

- As d soluções indicadas anteriormente não são congruentes módulo n duas a duas.
- Qualquer outra solução da congruência linear é conguente a alguma das d soluções indicadas.

Demonstração (continuação):

Se admitirmos que

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 (\mathrm{mod}\, n),$$

com $0 \leq t_2 < t_1 \leq d-1$, então

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 (\mathrm{mod}\, n).$$

Como m.d.c. $\left(\frac{n}{d}, n\right) = \frac{n}{d}$ e $\frac{n}{\frac{n}{d}} = d$, pelo teorema referido na página 105, tem-se

$$t_1 \equiv t_2 (\mathrm{mod}\, d).$$

Assim, $d \mid t_1 - t_2$, o que é uma contradição, pois $0 < t_1 - t_2 < d$. Logo

$$x_0 + \frac{n}{d}t_1 \not\equiv x_0 + \frac{n}{d}t_2 (\mathrm{mod}\, n).$$

Demonstração (continuação):

Falta provar que qualquer outra solução $x_0 + \frac{-n}{d}t$, onde $t \in \mathbb{Z}$, é congruente com uma das d soluções indicadas antes.

Pelo Algoritmo da Divisão, existem $q, r \in \mathbb{Z}$ tais que $-t = dq + r$ e $0 \leq r \leq d - 1$. Logo,

$$\begin{aligned} x_0 + \frac{-n}{d}t &= x_0 + \frac{n}{d}(-t) \\ &= x_0 + \frac{n}{d}(dq + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r (\mathrm{mod}\, n). \end{aligned}$$

Como $0 \leq r \leq d - 1$, $x_0 + \frac{-n}{d}t$ é congruente módulo n com uma das d soluções apresentadas anteriormente. □

Corolário

Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$. Se m.d.c.$(a, n) = 1$*, então a congruência linear $ax \equiv b (\mathrm{mod}\, n)$ 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 $ax \equiv 1 (\mathrm{mod}\, n)$ tem uma única solução módulo n; a esta solução dá-se a designação de inverso (multiplicativo) de a módulo n.

Exemplo

Determinemos o conjunto de soluções da congruência linear $9x \equiv 21 (\mathrm{mod}\, 30)$.

Como m.d.c.$(9, 30) = 3$ e $3 \mid 21$, esta congruência linear é solúvel e admite exatamente 3 soluções módulo 30, sendo estas soluções incongruentes entre si módulo 30.

Temos que

$$x_0 \text{ é solução de } 9x \equiv 21 (\mathrm{mod}\, 30)$$

sse

$$\exists_{y_0 \in \mathbb{Z}} \ (x_0, y_0) \text{ é solução da equação diofantina } 9x - 30y = 21.$$

Para resolver a congruência linear $9x \equiv 21 (\mathrm{mod}\, 30)$, comecemos por obter uma solução particular da equação diofantina $9x - 30y = 21$.

Exemplo (continuação):

No sentido de obter uma solução da equação diofantina, expressamos o m.d.c.$(9, -30)$ como combinação linear de 9 e -30:

$$3 = 9 \times (-3) - 30 \times (-1).$$

(Recorde-se que aplicando o Algoritmo de Euclides é possível obter coeficientes que permitem expressar o m.d.c.$(9, -30)$ como combinação linear de 9 e -30).

Da igualdade anterior, obtem-se

$$21 = 7 \times 3 = 9 \times (-21) - 30 \times (-7),$$

e, portanto, $(-21, -7)$ é uma solução particular da equação diofantina.

Exemplo (continuação):

Assim, -21 é uma solução da congruência linear, pelo que as soluções da congruência linear são

$$x \equiv -21 + \frac{-30}{3}t, \text{ com } t \in \{0, 1, 2\},$$

i.e., as 3 soluções da congruência linear, inconguentes entre si módulo 30, são

$$x_1 \equiv -21 \,(\mathrm{mod}\, 30), \quad x_2 \equiv -31 \,(\mathrm{mod}\, 30), \quad x_3 \equiv -41 \,(\mathrm{mod}\, 30)$$

que correspondem, respetivamente, às soluções positivas

$$x_1 \equiv 9 \,(\mathrm{mod}\, 30), \quad x_2 \equiv 29 \,(\mathrm{mod}\, 30), \quad x_3 \equiv 19 \,(\mathrm{mod}\, 30).$$

Exemplo

A congruência linear $4x \equiv 5 (\mathrm{mod}\, 6)$ não admite soluções inteiras porque m.d.c.$(4, 6) = 2$ e $2 \nmid 5$.

Exemplo

Consideremos a congruência linear $18x \equiv 30 (\mathrm{mod}\, 42)$. Como $\mathrm{m.d.c.}(18, 42) = 6$ e $6 \mid 30$, a congruência linear admite exatamente 6 soluções não congruentes entre si módulo 42. Uma solução possível é 4, pois

$$18 \times 4 = 72 \equiv 30 (\mathrm{mod}\, 42).$$

Logo, as 6 soluções referidas são

$$x \equiv 4 + \frac{42}{6} t (\mathrm{mod}\, 42), \quad t \in \{0, 1, 2, 3, 4, 5\},$$

i.e.,

$$\begin{array}{lllllllll} x_1 & \equiv & 4 (\mathrm{mod}\, 42), & x_2 & \equiv & 11 (\mathrm{mod}\, 42), & x_3 & \equiv & 18 (\mathrm{mod}\, 42), \\ x_4 & \equiv & 25 (\mathrm{mod}\, 42), & x_5 & \equiv & 32 (\mathrm{mod}\, 42), & x_6 & \equiv & 39 (\mathrm{mod}\, 42). \end{array}$$

Teorema

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

Demonstração:

Seja $ax \equiv b (\mathrm{mod}\, n)$ uma congruência linear solúvel. Então, sendo $d = \text{m.d.c.}(a, n)$, temos que $d \mid b$. Seja x_0 uma solução de $ax \equiv b (\mathrm{mod}\, n)$. Então $ax_0 \equiv b (\mathrm{mod}\, n)$, pelo que como $d \mid b$, se tem

$$\frac{a}{d} x_0 \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{n}{d}\right). \quad (*)$$

Uma vez que $\text{m.d.c.}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, a equação $\frac{a}{d} x_0 \equiv 1 \left(\mathrm{mod}\, \frac{n}{d}\right)$ é solúvel e existe um e um só $a^* \in \mathbb{Z}$ tal que

$$\frac{a}{d} a^* \equiv 1 \left(\mathrm{mod}\, \frac{n}{d}\right).$$

Multiplicando ambos os membros de (*) por a^*, obtemos

$$x_0 \equiv \frac{b}{d} a^* \left(\mathrm{mod}\, \frac{n}{d}\right),$$

i.e., x_0 é solução de $x \equiv c (\mathrm{mod}\, m)$, onde $c = \frac{b}{d} a^*$ e $m = \frac{n}{d}$.

Demonstração (continuação):

Reciprocamente, se x_0 é solução de $x \equiv \frac{b}{d}a^* \left(\mathrm{mod}\, \frac{n}{d}\right)$, é óbvio que x_0 é também solução de $ax \equiv b(\mathrm{mod}\, n)$. De facto, se x_0 é solução de $x \equiv \frac{b}{d}a^* \left(\mathrm{mod}\, \frac{n}{d}\right)$, então

$$x_0 \equiv \frac{b}{d}a^* \left(\mathrm{mod}\, \frac{n}{d}\right),$$

donde segue que

$$\frac{a}{d}x_0 \equiv \frac{b}{d}\frac{a}{d}a^* \left(\mathrm{mod}\, \frac{n}{d}\right).$$

Logo,

$$\frac{a}{d}x_0 \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{n}{d}\right),$$

e, por conseguinte,

$$ax_0 \equiv b \,(\mathrm{mod}\, n).$$

Exemplo

Consideremos a congruência linear $14x \equiv 18 (\mathrm{mod}\, 60)$. Como

$$\text{m.d.c.}(14, 60) = 2 \text{ e } 2 \mid 18,$$

a congruência linear $14x \equiv 18 (\mathrm{mod}\, 60)$ é solúvel. Como

$$\text{m.d.c.}\left(\frac{14}{2}, \frac{60}{2}\right) = \text{m.d.c.}(7, 30) = 1,$$

a congruência linear $7x \equiv 1 (\mathrm{mod}\, 30)$ tem uma e uma só solução módulo 30. Essa solução é $a^* = 13$. Assim, pelo teorema anterior,

$$x_0 \text{ é solução de } 14x \equiv 18 (\mathrm{mod}\, 60)$$

sse

i.e.

$$x_0 \text{ é solução de } x \equiv \frac{18}{2} \times 13 (\mathrm{mod}\, \frac{60}{2})$$

x_0 é solução de $14x \equiv 18 (\mathrm{mod}\, 60)$ sse x_0 é solução de $x \equiv 27 (\mathrm{mod}\, 30)$.

Sistemas de congruências lineares

Já sabemos caracterizar congruências lineares solúveis e como resolver congruências lineares. Seguidamente vamos estudar problemas que impliquem a resolução de várias congruências lineares em simultâneo. No século I, o matemático chinês Sun-Tsu estudou problemas deste tipo, como, por exemplo, o seguinte: determinar um inteiro cujo resto na divisão por 3, 5 e 7 seja 2, 3 e 2, respetivamente. Este problema pode ser modelado pelo sistema seguinte

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 3) \\ x \equiv 3 (\mathrm{mod}\, 5) \\ x \equiv 2 (\mathrm{mod}\, 7) \end{cases}$$

Definição

Chama-se **sistema de congruências lineares** *a um sistema do tipo*

$$(S) \begin{cases} a_1 x & \equiv & b_1 (\mathrm{mod}\, n_1) \\ a_2 x & \equiv & b_2 (\mathrm{mod}\, n_2) \\ & \vdots & \\ a_k x & \equiv & b_k (\mathrm{mod}\, n_k) \end{cases}$$

onde $k \in \mathbb{N} \setminus \{1\}$ *e, para todo* $i \in \{1, \ldots, k\}$, $a_i, b_i \in \mathbb{Z}$ *e* $n_i \in \mathbb{N}$.

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

Exemplo

O sistema de congruências lineares

$$\begin{cases} x & \equiv & 1 (\mathrm{mod}\, 4) \\ x & \equiv & 3 (\mathrm{mod}\, 6) \end{cases}$$

admite a solução $x_0 = 9$.

Exemplo

O sistema de congruências lineares

$$\begin{cases} x \equiv 3 (\mathrm{mod}\, 9) \\ x \equiv 2 (\mathrm{mod}\, 6) \end{cases}$$

não admite soluções inteiras.

Se admitirmos que x_0 é solução inteira do sistema, então existem $q_1, q_2 \in \mathbb{Z}$ tais que

$$x_0 = 9q_1 + 3 \quad \text{e} \quad x_0 = 6q_2 + 2.$$

Assim,

$$9q_1 + 3 = 6q_2 + 2,$$

i.e.,

$$9q_1 - 6q_2 = -1.$$

Portanto, a equação diofantina $9x - 6y = -1$ é solúvel, pelo que $3 = \text{m.d.c.}(9, 6) \mid -1$, o que é um absurdo.

Logo, o sistema não admite soluções.

Definição

Um sistema de congruências lineares que admite solução diz-se um **sistema solúvel**.

Dois sistemas de congruências lineares dizem-se **equivalentes** *se tiverem o mesmo conjunto de soluções.*

Os sistemas de congruências lineares podem ser aplicados na resolução de congruências lineares.

Proposição

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

$$n = {p_1}^{m_1} {p_2}^{m_2} \dots {p_k}^{m_k}$$

a fatorização de n em fatores primos distintos $p_1, p_2 \dots, p_k$. *Então, para quaisquer a e b,* x_0 *é solução da congruência linear* $ax \equiv b (\mathrm{mod}\, n)$ *se e só se* x_0 *é solução do sistema*

$$(S) \quad \begin{cases} ax \equiv b (\mathrm{mod}\, {p_1}^{m_1}) \\ ax \equiv b (\mathrm{mod}\, {p_2}^{m_2}) \\ \vdots \\ ax \equiv b (\mathrm{mod}\, {p_k}^{m_k}) \end{cases}$$

Demonstração.

Admitamos que x_0 é solução de $ax \equiv b (\mathrm{mod}\, n)$. Então, $n \mid (ax_0 - b)$.

Como, para cada $i \in \{1, 2, \ldots, k\}$, ${p_i}^{m_i} \mid n$ temos que ${p_i}^{m_i} \mid (ax_0 - b)$.

Logo, x_0 é solução das congruências lineares $ax \equiv b (\mathrm{mod}\, {p_i}^{m_i})$, com $i \in \{1, 2, \ldots, k\}$.

Reciprocamente, suponhamos que x_0 é solução do sistema (S).

Então, para cada $i \in \{1, 2, \ldots, k\}$, ${p_i}^{m_i} \mid (ax_0 - b)$.

Como ${p_1}^{m_1}, {p_2}^{m_2}, \ldots, {p_k}^{m_k}$ são todos primos entre si dois a dois, segue que

$$n = {p_1}^{m_1} {p_2}^{m_2} \ldots {p_k}^{m_k} \mid (ax_0 - b).$$

Logo, x_0 é solução da congruência linear $ax \equiv b (\mathrm{mod}\, n)$. □

Exemplo

Consideremos a congruência linear

$$13x \equiv 71 (\mathrm{mod}\, 380).$$

Fatorizando 380 num produto de números primos, obtemos

$$380 = 2^2 \times 5 \times 19.$$

Uma vez que m.d.c.$(13, 380) = 1$ e $1 \mid 71$, a congruência linear é solúvel.
Pelo teorema anterior, as soluções da congruência linear
$13x \equiv 71 (\mathrm{mod}\, 380)$ são as soluções do sistema

$$(S) \quad \begin{cases} 13x \equiv 71 (\mathrm{mod}\, 2^2) \\ 13x \equiv 71 (\mathrm{mod}\, 5) \\ 13x \equiv 71 (\mathrm{mod}\, 19) \end{cases}$$

Exemplo (continuação):

Uma vez que o sistema anterior é solúvel, cada uma das conguências lineares que o forma também é solúvel. Recorrendo ao teorema estabelecido na página 143, prova-se que o sistema indicado é equivalente ao sistema seguinte

$$(S) \quad \begin{cases} x \equiv 3 (\mathrm{mod}\, 2^2) \\ x \equiv 2 (\mathrm{mod}\, 5) \\ x \equiv 4 (\mathrm{mod}\, 19) \end{cases}$$

Se (S) é um sistema de congruências solúvel, todas as congruências lineares que formam (S) são também solúveis, pelo que cada uma das congruências lineares é equivalente a uma congruência linear cujo coeficiente da incógnita é 1. Assim, todo o sistema de congruências (S) que seja solúvel é equivalente a um sistema do tipo

$$(S') \quad \begin{cases} x & \equiv & c_1 \pmod{m_1} \\ x & \equiv & c_2 \pmod{m_2} \\ & \vdots & \\ x & \equiv & c_r \pmod{m_r} \end{cases}$$

onde, para cada $i \in \{1, 2, \ldots, r\}$, $c_i \in \mathbb{Z}$ e $m_i \in \mathbb{N}$.

Assim, todo o sistema pode ser resolvido recorrendo à resolução de um sistema do tipo (S').

Teorema (Teorema Chinês dos Restos)

Sejam $k \in \mathbb{N} \setminus \{1\}$, $a_1, a_2, \ldots a_k \in \mathbb{Z}$ *e* $n_1, n_2, \ldots, n_k \in \mathbb{N}$ *tais que*

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

Então o sistema de congruências lineares

$$(S') \quad \begin{cases} x & \equiv & a_1 (\text{mod } n_1) \\ x & \equiv & a_2 (\text{mod } n_2) \\ & \vdots & \\ x & \equiv & a_k (\text{mod } n_k) \end{cases}$$

tem uma e uma só solução módulo $n_1 n_2 \ldots n_k$.

Demonstração:

existência

Seja $n = n_1 n_2 \ldots n_k$.

Para cada $i \in \{1, 2, \ldots, k\}$, seja

$$N_i = \frac{n}{n_i} = n_1 \ldots n_{i-1} n_{i+1} \ldots n_k$$

e consideremos a congruência linear

$$N_i x \equiv 1 (\mathrm{mod}\, n_i).$$

Como, para quaisquer $i, j \in \{1, \ldots, k\}$,

$$i \neq j \Rightarrow n_i \text{ e } n_j \text{ são primos entre si } \Rightarrow \text{m.d.c.}(N_i, n_i) = 1,$$

a congruência linear $N_i x \equiv 1 (\mathrm{mod}\, n_i)$ admite uma única solução módulo n_i. Seja x_i essa solução.

Demonstração (continuação):

Provamos seguidamente que o inteiro

$$\overline{x} = x_1 N_1 a_1 + x_2 N_2 a_2 + \ldots + x_k N_k a_k$$

é solução de (S).

De facto, para quaisquer $r, i \in \{1, 2, \ldots, k\}$ tais que $r \neq i$, tem-se $N_r \equiv 0 (\mathrm{mod}\, n_i)$, pois $n_i \,|N_r$. Logo,

$$\overline{x} = x_1 N_1 a_1 + x_2 N_2 a_2 + \ldots + x_k N_k a_k \equiv x_i N_i a_i (\mathrm{mod}\, n_i).$$

Como x_i é solução de $N_i x \equiv 1 (\mathrm{mod}\, n_i)$, obtemos

$$\overline{x} \equiv a_i (\mathrm{mod}\, n_i).$$

Logo, o sistema (S) admite a solução $\overline{x}$.

Demonstração (continuação):

unicidade

Admitamos que x' é outra solução do sistema (S'). Então

$$\overline{x} \equiv x' (\mathrm{mod}\, n_i),$$

para qualquer $i \in \{1, 2, \ldots, k\}$ e, portanto,

$$n_i \,|\, \overline{x} - x'.$$

Como, para quaisquer $i, j \in \{1, 2, \ldots, k\}$ tais que $i \neq j$, tem-se m.d.c.$(n_i, n_j) = 1$, segue que

$$n_1 n_2 \ldots n_k \,|\, \overline{x} - x'.$$

Assim,

$$\overline{x} \equiv x' (\mathrm{mod}\, n).$$

□

Exemplo

O problema colocado pelo matemático Sun-Tsu consiste em determinar um inteiro que tenha resto 2, 3 e 2 na divisão por 3, 5 e 7, respetivamente. Este problema é modelado pelo seguinte sistema de congruências lineares

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 3) \\ x \equiv 3 (\mathrm{mod}\, 5) \\ x \equiv 2 (\mathrm{mod}\, 7) \end{cases}$$

Como $\mathrm{m.d.c.}(3,5) = \mathrm{m.d.c.}(3,7) = \mathrm{m.d.c.}(5,7) = 1$, o sistema admite uma única solução módulo $n = 3 \times 5 \times 7 = 105$.

Sejam

$$N_1 = \frac{n}{3} = 35, \quad N_2 = \frac{n}{5} = 21, \quad N_3 = \frac{n}{7} = 15.$$

Exemplo (continuação):

Como m.d.c.$(35, 3)$ = m.d.c.$(21, 5)$ = m.d.c$(15, 7) = 1$, cada uma das congruências lineares

$$35x \equiv 1 (\mathrm{mod}\, 3), \quad 21x \equiv 1 (\mathrm{mod}\, 5), \quad 15x \equiv 1 (\mathrm{mod}\, 7),$$

admite uma e uma só solução módulo 3, 5 e 7, respetivamente, sendo essas soluções

$$x_1 = 2, \quad x_2 = 1 \quad \text{e} \quad x_3 = 1,$$

Então, pelo Teorema Chinês dos Restos,

$$\overline{x} = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233$$

é uma solução do sistema. Logo, a única solução do sistema módulo 105 é

$$x' = 233 \equiv 23 (\mathrm{mod}\, 105).$$

Exemplo

Um turista espanhol e um guia subiram a correr os degraus da pirâmide Keops perseguidos por um leão! O turista conseguia subir cinco degraus de uma só vez, o guia seis degraus e o leão sete degraus. A dada altura, o turista estava a um degrau do topo da pirâmide, o guia a nove degraus e o leão a dezanove degraus. Quantos degraus pode ter a pirâmide?

Representando por n o número de degraus da pirâmide, pretende-se determinar os valores possíveis de n tais que

$$\begin{cases} 5x + 1 = n \\ 6y + 9 = n \\ 7z + 19 = n \end{cases}$$

Exemplo (continuação):

O problema anterior pode, então, ser modelado pelo sistema de congruências

$$\begin{cases} n \equiv 1 (\mathrm{mod}\, 5) \\ n \equiv 9 (\mathrm{mod}\, 6) \\ n \equiv 19 (\mathrm{mod}\, 7) \end{cases}$$

o qual é equivalente a

$$\begin{cases} n \equiv 1 (\mathrm{mod}\, 5) \\ n \equiv 3 (\mathrm{mod}\, 6) \\ n \equiv 5 (\mathrm{mod}\, 7) \end{cases}$$

Uma vez que $\mathrm{m.d.c.}(5,6) = \mathrm{m.d.c.}(5,7) = \mathrm{m.d.c.}(6,7) = 1$, o sistema admite uma única solução módulo $n = 5 \times 6 \times 7 = 210$.

Sejam

$$N_1 = \frac{n}{5} = 42, \quad N_2 = \frac{n}{6} = 35, \quad N_3 = \frac{n}{7} = 30.$$

Exemplo (continuação):

Como m.d.c.$(42, 5)$ = m.d.c.$(35, 6)$ = m.d.c$(30, 7) = 1$, cada uma das congruências lineares

$$42x \equiv 1 (\mathrm{mod}\, 5), \quad 35x \equiv 1 (\mathrm{mod}\, 6), \quad 30x \equiv 1 (\mathrm{mod}\, 7),$$

admite uma e uma só solução módulo 5, 6 e 7. Estas congruências lineares são equivalentes às congruências lineares

$$2x \equiv 1 (\mathrm{mod}\, 5), \quad 5x \equiv 1 (\mathrm{mod}\, 6), \quad 2x \equiv 1 (\mathrm{mod}\, 7),$$

e admitem, respetivamente, as seguintes soluções

$$x_1 = 3, \quad x_2 = 5 \quad \text{e} \quad x_3 = 4,$$

Então, pelo Teorema Chinês dos Restos,

$$\overline{x} = 1 \times 42 \times 3 + 3 \times 35 \times 5 + 5 \times 30 \times 4 = 1251$$

é uma solução do sistema. Logo, a única solução do sistema módulo 210 é

$$x' = 1251 \equiv 201 (\mathrm{mod}\, 210).$$

Congruências módulo n

Num exemplo anterior, observámos que o sistema

$$\begin{cases} x \equiv 3 (\mathrm{mod}\, 9) \\ x \equiv 2 (\mathrm{mod}\, 6) \end{cases}$$

não é solúvel. A este sistema não pode ser aplicado o Teorema Chinês dos Restos, uma vez que 9 e 6 não são primos entre si.

O resultado seguinte, provado no séc. VII d.C. por Yih-Hing, generaliza o Teorema Chinês dos Restos. Este resultado estabelece em que condições são solúveis os sistemas de congruências lineares

$$(S) \quad \begin{cases} x & \equiv & a_1 (\mathrm{mod}\, n_1) \\ x & \equiv & a_2 (\mathrm{mod}\, n_2) \\ & \vdots & \\ x & \equiv & a_k (\mathrm{mod}\, n_k) \end{cases}$$

onde os naturais n_i não são necessariamente primos entre si.

Teorema

Sejam $k \in \mathbb{N} \setminus \{1\}$, $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ e $n_1, n_2, \ldots, n_k \in \mathbb{N}$. Então o sistema de congruências lineares

$$(S') \quad \begin{cases} x & \equiv & a_1 (\mathrm{mod}\, n_1) \\ x & \equiv & a_2 (\mathrm{mod}\, n_2) \\ & \vdots & \\ x & \equiv & a_k (\mathrm{mod}\, n_k) \end{cases}$$

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

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

Se o sistema tiver solução, ela é única módulo n onde n é o mínimo múltiplo comum de $n_1, n_2, \ldots, n_k$.

Demonstração:

Suponhamos que existe uma solução x_0 do sistema dado. Então

$$x_0 \equiv a_i (\mathrm{mod}\, n_i),$$

para qualquer $i \in \{1, 2, \ldots, k\}$ e, portanto,

$$n_i \mid (x_0 - a_i).$$

Para quaisquer $i, j \in \{1, 2, \ldots, k\}$ tais que $i \neq j$, sejam

$$n_{ij} = \mathrm{m.d.c.}(n_i, n_j).$$

Então

$$n_{ij} \mid n_i \quad \text{e} \quad n_{ij} \mid n_j$$

e, portanto, $n_{ij} \mid (x_0 - a_j) - (x_0 - a_i)$, ou seja $n_{ij} \mid a_i - a_j$.

Demonstração (continuação):

Reciprocamente, admitamos que m.d.c.$(n_i, n_j) \mid (a_i - a_j)$. Pretendemos provar que o sistema dado admite solução.

A prova passa pela construção, a partir do sistema dado, de um sistema nas condições do Teorema Chinês dos Restos.

Para obter tal sistema, começamos por substituir cada congruência linear $x \equiv a_i (\mathrm{mod}\, n_i)$ $(i \in \{1, 2, \ldots, k\})$ por uma coleção de congruências lineares em que toda a congruência é da forma $x \equiv a_i (\mathrm{mod}\, p^r)$, onde $r \in \mathbb{N}$ e p é um dos primos que ocorrem na fatorização de n_i em primos.

Demonstração (continuação):

Para cada $i \in \{1, 2, \ldots, k\}$, se $n_i = {p_{i_1}}^{m_{i_1}} {p_{i_2}}^{m_{i_2}} \ldots {p_{i_r}}^{m_{i_r}}$ é a fatorização de n_i em fatores primos, substituímos a congruência linear $x \equiv a_i (\mathrm{mod}\, n_i)$ pelo sistema de congruências lineares

$$(S') \quad \begin{cases} x & \equiv & a_i (\mathrm{mod}\, {p_{i_1}}^{m_{i_1}}) \\ x & \equiv & a_i (\mathrm{mod}\, {p_{i_2}}^{m_{i_2}}) \\ & \vdots & \\ x & \equiv & a_i (\mathrm{mod}\, {p_{i_k}}^{m_{i_k}}) \end{cases}$$

que, como já sabemos, é equivalente à congruência linear $x \equiv a_i (\mathrm{mod}\, n_i)$.

Demonstração (continuação):

Assim, obtemos um sistema equivalente ao primeiro, no qual os naturais que definem as congruências são potências de primos; estes naturais não são, necessariamente, primos entre si.

Seguidamente, para cada primo p da lista de números primos obtidos na decomposição de todos os naturais n_i ($i \in \{1, 2, \ldots, k\}$), procede-se do seguinte modo:

- escolhe-se $j \in \{1, 2, \ldots, k\}$ tal que n_j seja divisivel pela maior potência de p; seja p^e essa potência;
- eliminam-se do sistema todas as congruências lineares $x \equiv a_i (\mathrm{mod}\, p^f)$ ($i \in \{1, 2, \ldots, k\}$), com exceção da congruência linear $x \equiv a_j (\mathrm{mod}\, p^e)$.

Demonstração (continuação):

O sistema obtido após a eliminação das congruências lineares indicadas é equivalente ao sistema inicial. De facto, se $p^f \mid n_i$, para algum $i \in \{1, 2, \ldots, k\}$, tem-se $f \leq e$ e, portanto, $p^f \mid n_j$. Então $p^f \mid \text{m.d.c.}(n_i, n_j)$ e, portanto, $p^f \mid (a_i - a_j)$. Logo, se x_0 é solução de $x \equiv a_j (\text{mod}\, p^e)$, também será solução de $x \equiv a_j (\text{mod}\, p^f)$ e de $x \equiv a_i (\text{mod}\, p^f)$.

No sistema que é obtido por aplicacão do processo descrito anteriormente, todas as congruências são da forma $x \equiv a_i (\text{mod}\, p^s)$, para algum $i \in \{1, 2, \ldots, k\}$, algum primo p e algum $s \in \mathbb{N}$; os números primos que ocorrem nestas congruências são distintos dois a dois. Logo, o Teorema Chinês dos Restos garante que este sistema é solúvel.

Demonstração (continuação):

Por último, provamos que, se o sistema for solúvel, a sua solução é única módulo minímo múltiplo comum de $n_1, n_2, \ldots, n_k$.

Seja x_0 uma solução do sistema.

Se x é outra solução do sistema, tem-se $x \equiv x_0 (\mathrm{mod}\, n_i)$, para cada $i \in \{1, 2, \ldots, k\}$, i.e.,

$$n_i \,|\, x - x_0,$$

para cada $i \in \{1, 2, \ldots, k\}$.

Logo, sendo n o mínimo múltiplo comum de $n_1, n_2, \ldots, n_k$,

$$n \,|\, x - x_0$$

e, portanto,

$$x \equiv x_0 (\mathrm{mod}\, n).$$

□

Exemplo

Consideremos o seguinte sistema de congruências lineares

$$(S) \quad \begin{cases} x \equiv 11 (\mathrm{mod}\, 36) \\ x \equiv 7 (\mathrm{mod}\, 40) \\ x \equiv 32 (\mathrm{mod}\, 75) \end{cases} .$$

Sejam $a_1 = 11$, $a_2 = 7$, $a_3 = 32$, $n_1 = 36$, $n_2 = 40$ e $n_3 = 75$. Então

$$n_{12} = \text{m.d.c.}(36, 40) = 4, \qquad n_{13} = \text{m.d.c.}(36, 75) = 3,$$
$$n_{23} = \text{m.d.c.}(40, 75) = 5.$$

Uma vez que

$$a_1 - a_2 = 11 - 7 = 4, \qquad a_1 - a_3 = 11 - 32 = -21,$$
$$a_2 - a_3 = 7 - 32 = -25,$$

as condições $n_{ij} \mid a_i - a_j$ são satisfeitas e, portanto, o sistema tem uma única solução módulo $\text{m.m.c.}(36, 40, 75) = 1800$.

Exemplo (continuação):

O sistema (S) é equivalente a

$$(S_1) \begin{cases} x & \equiv & 11 (\mathrm{mod}\, 2^2) \\ x & \equiv & 11 (\mathrm{mod}\, 3^2) \\ x & \equiv & 7 (\mathrm{mod}\, 2^3) \\ x & \equiv & 7 (\mathrm{mod}\, 5) \\ x & \equiv & 32 (\mathrm{mod}\, 3) \\ x & \equiv & 32 (\mathrm{mod}\, 5^2) \end{cases}$$

sendo este último equivalente ao sistema

$$(S_2) \begin{cases} x & \equiv & 11 (\mathrm{mod}\, 3^2) \\ x & \equiv & 7 (\mathrm{mod}\, 2^3) \\ x & \equiv & 32 (\mathrm{mod}\, 5^2) \end{cases} .$$

Exemplo (continuação):

Considerando que $11 \equiv 2 (\mathrm{mod}\, 9)$ e $32 \equiv 7 (\mathrm{mod}\, 25)$, o sistema (S_2) é equivalente ao sistema

$$(S_3) \quad \begin{cases} x & \equiv & 7 (\mathrm{mod}\, 8) \\ x & \equiv & 2 (\mathrm{mod}\, 9) \\ x & \equiv & 7 (\mathrm{mod}\, 25) \end{cases} .$$

Os naturais 9, 8 e 25 são primos entre si dois a dois, pelo que o sistema (S_3) pode ser resolvido aplicando o Teorema Chinês dos Restos.

Exemplo (continuação):

Sejam $n = 8 \times 9 \times 25 = 1800$,

$$N_1 = \frac{1800}{8} = 225, \quad N_2 = \frac{1800}{9} = 200, \quad N_3 = \frac{1800}{25} = 72.$$

Como m.d.c.(n, N_1) = m.d.c.(n, N_2) = m.d.c.$(n, N_3) = 1$, as congruências lineares

$$225x \equiv 1 (\mathrm{mod}\, 8), \quad 200x \equiv 1 (\mathrm{mod}\, 9), \quad 72x \equiv 1 (\mathrm{mod}\, 25)$$

são solúveis e têm uma única solução módulo 8, 9 e 25, respetivamente. As congruências lineares anteriores são equivalentes às congruências lineares

$$x \equiv 1 (\mathrm{mod}\, 8), \quad 2x \equiv 1 (\mathrm{mod}\, 9), \quad 22x \equiv 1 (\mathrm{mod}\, 25)$$

e admitem, respetivamente, as soluções $x_1 = 1$, $x_2 = 5$ e $x_3 = 8$.

Exemplo (continuação):

Assim,

$$\overline{x} = 7 \times 225 \times 1 + 2 \times 200 \times 5 + 7 \times 72 \times 8 = 7607$$

é uma solução do sistema (S_3).

Como $7607 \equiv 407 (\mathrm{mod}\, 1800)$ temos que x' é solução do sistema (S_3) se e só se $x' \equiv 407 (\mathrm{mod}\, 1800)$. Considerando que o sistema (S_3) é equivalente ao sistema (S), o conjunto das soluções do sistema (S) é

$$\{407 + 1800t : t \in \mathbb{Z}\}.$$

Exemplo

Resolver o seguinte sistema

$$(S) \begin{cases} x & \equiv & 2 (\mathrm{mod}\, 4) \\ x & \equiv & 4 (\mathrm{mod}\, 6) \\ x & \equiv & 1 (\mathrm{mod}\, 3) \end{cases}.$$

Como 4 e 6 não são primos entre si, não podemos resolver o sistema pelo Teorema Chinês dos Restos. No entanto, dado que

$$m.d.c.(6,4) = 2 \,|\, 2 = 4 - 2,$$

$$m.d.c.(6,3) = 3 \,|\, 3 = 4 - 1$$

$$m.d.c.(4,3) = 1 \,|\, 2 = 2 - 1,$$

o sistema tem uma única solução módulo m.m.c.$(4,6,3) = 12$.

Exemplo (continuação):

O sistema (S) é equivalente a

$$(S_1)\ \begin{cases} x & \equiv & 2 (\mathrm{mod}\, 2^2) \\ x & \equiv & 4 (\mathrm{mod}\, 2) \\ x & \equiv & 4 (\mathrm{mod}\, 3) \\ x & \equiv & 1 (\mathrm{mod}\, 3) \end{cases}$$

que é equivalente ao sistema

$$(S_2)\ \begin{cases} x & \equiv & 2 (\mathrm{mod}\, 4) \\ x & \equiv & 1 (\mathrm{mod}\, 3) \end{cases}.$$

Exemplo (continuação):

O sistema (S_2) pode ser resolvido aplicando o Teorema Chinês dos Restos.

Sejam $n = 12$, $N_1 = \frac{12}{4} = 3$ e $N_2 = \frac{12}{3} = 4$.

- $3x \equiv 1 (\mathrm{mod}\, 4)$ tem uma e uma só solução módulo 4, sendo essa solução $x_1 = 3$.
- $4x \equiv 1 (\mathrm{mod}\, 3)$ tem uma e uma só solução módulo 3, sendo essa solução $x_2 = 1$.

Assim,

$$x_0 = 2 \times 3 \times 3 + 1 \times 4 \times 1 = 22$$

é uma solução do sistema (S_2). Como $22 \equiv 10 (\mathrm{mod}\, 12)$ temos que x' é solução do sistema (S_2) se e só se $x' \equiv 10 (\mathrm{mod}\, 12)$. Logo o conjunto das soluções do sistema (S) é

$$\{10 + 12t : t \in \mathbb{Z}\}.$$

Alguns 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 divide $a^{p-1} - 1$."

carta de Fermat a Bessy (1640)

(sem demonstação por ser muito longa)

Quase 100 anos mais tarde, Euler (1707-1783) prova essa afirmação.

Teorema (Pequeno Teorema de Fermat)

Se p é primo e a é um inteiro não divisível por p, então $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Demonstração:

Consideremos os seguintes $p-1$ múltiplos de a:

$$a, 2a, 3a, \ldots, (p-1)a.$$

Como p não divide a, então, para quaisquer $r, s \in \{1, 2, \ldots, p-1\}$ tais que $r \neq s$,

$$ra \not\equiv sa (\mathrm{mod}\, p) \quad \text{e} \quad ra \not\equiv 0 (\mathrm{mod}\, p).$$

De facto, se admitirmos que

$$ra \equiv sa (\mathrm{mod}\, p), \text{ com } 1 \leq r < s \leq p-1,$$

seria possível cancelar a (pois m.d.c.$(a, p) = 1$), obtendo-se $r \equiv s (\mathrm{mod}\, p)$, o que é impossível.

Logo, os $p-1$ inteiros indicados são incongruentes dois a dois módulo p; portanto, $a, 2a, 3a, \ldots, (p-1)a$ são congruentes módulo p como um e um só dos números $1, 2, 3, \ldots, p-1$.

Demonstração (continuação):

Assim,

$$a \times 2a \times 3a \times \ldots \times (p-1)a \equiv 1 \times 2 \times 3 \times \ldots \times (p-1) (\mathrm{mod}\, p),$$

i.e.,

$$a^{p-1}(p-1)! \equiv (p-1)! (\mathrm{mod}\, p).$$

Como m.d.c.$(p, (p-1)!) = 1$, temos que

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Corolário

Se p é primo, então $a^p \equiv a (\mathrm{mod}\, p)$, para qualquer inteiro a.

Demonstração.

Por um lado, se $p \mid a$, então $a \equiv 0 (\mathrm{mod}\, p)$, pelo que $a^p \equiv 0 (\mathrm{mod}\, p)$. Logo, $a^p \equiv a (\mathrm{mod}\, p)$.

Por outro lado, se $p \nmid a$, então pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, donde $a^p \equiv a (\mathrm{mod}\, p)$. □

Apresentam-se de seguida alguns exemplos de aplicação do Pequeno Teorema de Fermat.

Exemplo

Provar que $5^{38} \equiv 4 (\mathrm{mod}\, 11)$.

Como 11 é primo e $11 \nmid 5$, obtemos, pelo Pequeno Teorema de Fermat, que

$$5^{10} \equiv 1 (\mathrm{mod}\, 11).$$

Assim,

$$5^{38} = (5^{10})^3 \times 5^8 \equiv 5^8 (\mathrm{mod}\, 11).$$

Como $5^2 = 25 \equiv 3 (\mathrm{mod}\, 11)$, temos $5^8 \equiv 3^4 (\mathrm{mod}\, 11)$. Mas $3^4 = 81 \equiv 4 (\mathrm{mod}\, 11)$ e, portanto, $5^8 \equiv 4 (\mathrm{mod}\, 11)$. Logo

$$5^{38} \equiv 4 (\mathrm{mod}\, 11).$$

Exemplo

Determinar o resto de 24^{1947} na divisão por 17.

Tem-se

$$24 \equiv 7 (\mathrm{mod}\, 17),$$

logo

$$24^{1947} \equiv 7^{1947} (\mathrm{mod}\, 17).$$

Como 17 é primo e $17 \nmid 7$, pelo Pequeno Teorema de Fermat,

$$7^{16} \equiv 1 (\mathrm{mod}\, 17).$$

Assim,

$$7^{1947} = 7^{16 \times 121 + 11} = (7^{16})^{121} \times 7^{11} \equiv 1^{121} \times 7^{11} (\mathrm{mod}\, 17).$$

Exemplo (continuação)

Mas $7^2 = -2 (\mathrm{mod}\, 17)$ e, portanto,

$$7^{11} = (7^2)^5 \times 7 \equiv (-2)^5 \times 7 (\mathrm{mod}\, 17).$$

Como

$$(-2)^5 = -32 \equiv 2 (\mathrm{mod}\, 17),$$

obtem-se

$$-32 \times 7 \equiv 2 \times 7 (\mathrm{mod}\, 17).$$

Assim, considerando que $2 \times 7 = 14$ e $0 \leq 14 < 17$, o resto de 2^{1947} na divisão por 17 é 14.

Exemplo

Provar que $a^{21} \equiv a \pmod{15}$, para todo o inteiro a.

Fatorizando 15 em números primos, tem-se $15 = 3 \times 5$.

Uma vez que 3 é um número primo, pelo Corolário do Pequeno Teorema de Fermat,

$$a^3 \equiv a \pmod{3}.$$

Logo,

$$a^{21} = (a^3)^7 \equiv a^7 \pmod{3}.$$

Por sua vez,

$$a^7 = (a^3)^2 \times a \equiv a^2 \times a \pmod{3}.$$

Então, como $a^{21} \equiv a^7 \pmod{3}$, $a^7 \equiv a^3 \pmod{3}$ e $a^3 \equiv a \pmod{3}$, tem-se $a^{21} \equiv a \pmod{3}$.

Exemplo (continuação)

Considerando que 5 é primo, pelo Corolário do Pequeno Teorema de Fermat, tem-se

$$a^5 \equiv a \pmod 5.$$

Logo,

$$a^{21} = (a^5)^4 \times a \equiv a^4 \times a \pmod 5.$$

Como $a^{21} \equiv a^5 \pmod 5$ e $a^5 \equiv a \pmod 5$, então $a^{21} \equiv a \pmod 5$.

Assim, $a^{21} \equiv a \pmod 3$ e $a^{21} \equiv a \pmod 5$. Como 3 e 5 são primos entre si, segue que $a^{21} \equiv a \pmod{3 \times 5}$, ou seja, $a^{21} \equiv a \pmod{15}$.

Alguns teoremas relevantes na teoria de números

Usando o contra-recíproco do Pequeno Teorema de Fermat

$$(\exists_{a\in\mathbb{Z}}\ a^{p-1} \not\equiv 1 (\mathrm{mod}\, p)) \Rightarrow (p \text{ não é primo} \vee p \mid a)$$

ou o contra-recíproco do seu corolário

$$(\exists_{a\in\mathbb{Z}}\ a^{p} \not\equiv a (\mathrm{mod}\, p)) \Rightarrow p \text{ não é primo},$$

é possível verificar se um dado número natural é ou não primo.

Exemplo

Mostremos que 117 não é um número primo.

Consideremos $a = 2$ e vejamos que $2^{117} \not\equiv 2 (\mathrm{mod}\, 117)$. A potência de 2 mais próxima de 117 é 2^7. Então, considerando que

$$2^{117} = 2^{7\times 16+5} = (2^7)^{16} \times 2^5 \quad \text{e} \quad 2^7 = 128 \equiv 11 (\mathrm{mod}\, 117),$$

temos

$$2^{117} \equiv (11)^{16} \times 2^5 \equiv 121^8 \times 2^5 (\mathrm{mod}\, 117) \equiv 4^8 \times 2^5 (\mathrm{mod}\, 117) \equiv 2^{21} (\mathrm{mod}\, 117).$$

Uma vez que $2^{21} = (2^7)^3$, segue-se que

$$2^{21} \equiv 11^3 (\mathrm{mod}\, 117) \equiv 121 \times 11 (\mathrm{mod}\, 117) \equiv 4 \times 11 (\mathrm{mod}\, 117) \equiv 44 (\mathrm{mod}\, 117).$$

Como $2^{117} \equiv 44 (\mathrm{mod}\, 117)$ e $44 \not\equiv 2 (\mathrm{mod}\, 117)$, então $2^{117} \not\equiv 2 (\mathrm{mod}\, 117)$. Portanto, 117 não é primo.

O recíproco do Pequeno Teorema de Fermat não é verdadeiro: existem inteiros a e p para os quais $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ e p não é primo.

Exemplo

Como $4^2 = 16 \equiv 1 (\mathrm{mod}\, 15)$, temos que $4^{14} \equiv 1^7 (\mathrm{mod}\, 15)$, ou seja, $4^{15-1} \equiv 1 (\mathrm{mod}\, 15)$. No entanto, 15 não é um número 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

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

Demonstração.

Sejam p e q números primos distintos tais que

$$a^p \equiv a \pmod{q} \quad \text{e} \quad a^q \equiv a \pmod{p}.$$

De $a^p \equiv a \pmod{q}$, obtemos $a^{pq} \equiv a^q \pmod{q}$. Então, como $a^q \equiv a \pmod{q}$, tem-se $a^{pq} \equiv a \pmod{q}$. De modo análogo, concluímos que $a^{pq} \equiv a \pmod{p}$. Logo, como p e q são primos entre si,

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

□

Teorema de Euler

Uma das funções mais importantes no estudo da teoria de números é a Função de Euler.

Definição

Para cada $n \geq 1$, seja $\phi(n)$ o número de inteiros positivos k tais que $k \leq n$ e m.d.c.$(k, n) = 1$. *À função $\phi : \mathbb{N} \to \mathbb{N}$ definida por $n \mapsto \phi(n)$ chama-se* **Função de Euler**.

Exemplo

- $\phi(1) = \phi(2) = 1$, $\phi(3) = \phi(4) = \phi(6) = 2$ e $\phi(5) = 4$.
- $\phi(30) = 8$, pois existem 8 números menores ou iguais a 30 e primos com 30:

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Dado $n \geq 2$, temos que $\phi(n) \leq n - 1$.

- Se n é um número primo, então $\phi(n) = n - 1$.
- Se n é um número composto, existe pelo menos um inteiro positivo $k < n$ tal m.d.c.$(n, k) \neq 1$, pelo que $\phi(n) \leq n - 2$.

Do que foi observado resulta o seguinte critério de primalidade.

Proposição

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

Proposição

Se p é primo e $k > 0$, então

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

Demonstração.

Dos elementos do conjunto $\{1, 2, 3, \ldots, p, \ldots, p^k\}$ existem $\frac{p^k}{p} = p^{k-1}$ elementos que são divisíveis por p, pelo que não são primos com p^k. Todos os outros elementos são primos com p^k. Assim,

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

□

Exemplo

- $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$; os seis inteiros menores do que 9 e primos com 9 são: 1,2,4,5,7,8.
- $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$; os oito inteiros menores do que 16 e primos com 16 são: 1,3,5,7,9,11,13,15.

Proposição

Sejam m e n inteiros positivos tais que m.d.c.$(m.n) = 1$. *Então* $\phi(mn) = \phi(m)\phi(n)$.

Exemplo

Os inteiros $m = 5$ e $n = 4$ são primos entre si, pelo que $\phi(20) = \phi(4)\phi(5) = 2 \times 4$.

Observação: A proposição anterior não é válida se os números considerados não forem primos entre si: por exemplo,

$$\phi(4) = 2 \neq 4 = \phi(2)\phi(2).$$

Alguns teoremas relevantes na teoria de números

Teorema

Se um inteiro $n > 1$ admite a factorização

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

onde $p_1, p_2, \dots, p_r$ são primos distintos dois a dois, então

$$\begin{aligned} \phi(n) &= ({p_1}^{k_1} - {p_1}^{k_1-1})({p_2}^{k_2} - {p_2}^{k_2-1}) \dots ({p_r}^{k_r} - {p_r}^{k_r-1}) \\ &= n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \dots (1 - \tfrac{1}{p_r}). \end{aligned}$$

Exemplo

Calculemos $\phi(360)$. Fatorizando 360 em números primos, temos $360 = 2^2 \times 3^2 \times 5$. Então, pelo teorema anterior, obtem-se

$$\phi(360) = 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 96.$$

Lema

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

Demonstração.

Comecemos por observar que, para quaisquer $i, j \in \{1, 2, \ldots, \phi(n)\}$ com $i \neq j$, $ar_i \not\equiv ar_j \pmod{n}$. De facto, se admitirmos que existem $i, j \in \{1, 2, \ldots, \phi(n)\}$ com $i \neq j$ tais que $ar_i \equiv ar_j \pmod{n}$, então, como $\text{m.d.c.}(a, n) = 1$, obtem-se $r_i \equiv r_j \pmod{n}$, o que é um absurdo.

Além disso, considerando que $\text{m.d.c.}(r_i, n) = 1$, para cada $i \in \{1, 2, \ldots, \phi(n)\}$, e $\text{m.d.c.}(a, n) = 1$, tem-se $\text{m.d.c.}(ar_i, n) = 1$.

Para cada $i \in \{1, 2, \ldots, \phi(n)\}$, existe $0 \leq b < n$ tal que $ar_i \equiv b \pmod{\text{n}}$. Como

$$\text{m.d.c.}(b, n) = \text{m.d.c.}(ar_i, n) = 1,$$

b tem de ser um dos inteiros $r_1, r_2, \ldots, r_{\phi(n)}$. □

Alguns teoremas relevantes na teoria de números

Em 1760, Euler estabeleceu a seguinte generalização do Pequeno Teorema de Fermat.

Teorema (Teorema de Euler)

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

Demonstração.

Sejam $r_1, r_2, \ldots, r_{\phi(n)}$ os $\phi(n)$ inteiros positivos menores do que n e primos com n.

Como m.d.c.$(a, n) = 1$, temos que, para cada $i \in \{1, 2, \ldots, \phi(n)\}$, existe $j \in \{1, 2, \ldots, \phi(n)\}$ tal que $ar_i \equiv r_j (\mathrm{mod}\, n)$.

Além disso, para quaisquer $i, j \in \{1, 2, \ldots, \phi(n)\}$ com $i \neq j$, $ar_i \not\equiv ar_j (\mathrm{mod}\, n)$.

Assim,

$$ar_1 \times ar_2 \times \ldots \times ar_{\phi(n)} \equiv r_1 \times r_2 \times \ldots \times r_{\phi(n)} (\mathrm{mod}\, n),$$

ou seja,

$$a^{\phi(n)} r_1 r_2 \ldots r_{\phi(n)} \equiv r_1 r_2 \ldots r_{\phi(n)} (\mathrm{mod}\, n).$$

Como $r_1, r_2, \ldots, r_{\phi(n)}$ são primos com n, podem ser sucessivamente cancelados obtendo-se $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$. □

A demonstração do teorema anterior pode ser ilustrada com inteiros específicos.

Exemplo

Sejam $n = 9$ e $a = -4$.

Os inteiros positivos menores do que 9 e primos com 9 são: $1, 2, 4, 5, 7, 8$. Considerando a multiplicação destes inteiros por a, tem-se

$$\begin{aligned} -4 \times 1 &= -4, \quad & -4 \times 2 &= -8, \quad & -4 \times 4 &= -16, \\ -4 \times 5 &= -20, \quad & -4 \times 7 &= -28, \quad & -4 \times 8 &= -32 \end{aligned}$$

sendo estes inteiros congruentes módulo 9, respetivamente, com $5, 1, 2, 7, 8, 4$.

Exemplo

Por conseguinte,

$$(-4)(-8)(-16)(-20)(-28)(-32) \equiv 5 \times 1 \times 2 \times 7 \times 8 \times 4 (\mathrm{mod}\, 9),$$

ou seja,

$$(-4)^6(1 \times 2 \times 4 \times 5 \times 7 \times 8) \equiv (1 \times 2 \times 4 \times 5 \times 7 \times 8)(\mathrm{mod}\, 9).$$

Uma vez que 1,2,4,5,7,8 são primos com 9 podem ser cancelados na congruência linear anterior e obtemos $(-4)^6 \equiv 1(\mathrm{mod}\, 9)$.

Teorema de Wilson

Em 1770, Edward Waring anunciou, na obra "Meditationes Algebraicae", diversos teoremas novos. Entre esses teoremas está enunciada uma conjetura que lhe foi apresentada pelo seu aluno John Wilson, a qual estabelece a seguinte propriedade sobre números primos: se p é primo, então p divide $(p+1)!+1$. Wilson baseou a sua conjetura em cálculos numéricos, mas nem ele nem Waring apresentaram uma prova desta conjetura. Este resultado veio a ser provado, em 1771, por Lagrange e ficou conhecido como Teorema de Wilson.

Teorema (Teorema de Wilson)

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

Demonstração:

A condição verifica-se para $p = 2$ e $p = 3$. De facto,

$$(2-1)! = 1 \equiv -1 (\mathrm{mod}\, 2)$$

e

$$(3-1)! = 2 \equiv -1 (\mathrm{mod}\, 3).$$

Verifiquemos que também se tem

$$(p-1)! \equiv -1 (\mathrm{mod}\, p), \text{ para } p > 3.$$

Demonstração (continuação):

Seja $a \in \{1, 2, 3 \ldots, p-1\}$ e consideremos a congruência linear

$$ax \equiv 1 (\mathrm{mod}\, p).$$

Como m.d.c.$(a, p) = 1$, existe uma e uma só solução módulo p desta congruência linear. Então existe um único inteiro a' tal que

$$1 \leq a' \leq p-1 \quad \text{e} \quad aa' \equiv 1 (\mathrm{mod}\, p).$$

Sendo p primo, tem-se $a = a'$ se e só se $a = 1$ ou $a = p-1$. De facto, se $a = a'$, tem-se

$$a^2 \equiv 1 (\mathrm{mod}\, p).$$

Além disso,

$$\begin{aligned} a^2 \equiv 1 (\mathrm{mod}\, p) &\Leftrightarrow p \,|\, a^2 - 1 \\ &\Leftrightarrow p \,|\, (a-1)(a+1) \\ &\Leftrightarrow p \,|\, a-1 \text{ ou } p \,|\, a+1 \\ &\Leftrightarrow a = 1 \text{ ou } a = p-1 \end{aligned}$$

Demonstração (continuação):

Se $a \neq a'$, temos

$$a \in \{2, 3, 4, \ldots, p-3, p-2\}.$$

Os $p-3$ elementos deste conjunto podem ser agrupados em pares (a, a') tais que $a \neq a'$ e $aa' \equiv 1 (\mathrm{mod}\, p)$. Das $\frac{p-3}{2}$ congruências $aa' \equiv 1 (\mathrm{mod}\, p)$, obtem-se

$$2 \times 3 \times \ldots \times (p-3) \times (p-2) \equiv 1 (\mathrm{mod}\, p),$$

i.e.,

$$(p-2)! \equiv 1 (\mathrm{mod}\, p).$$

Logo

$$(p-1)! = (p-1)(p-2)! \equiv p-1 (\mathrm{mod}\, p)$$

e, portanto,

$$(p-1)! \equiv -1 (\mathrm{mod}\, p).$$

Alguns teoremas relevantes na teoria de números

O exemplo seguinte ilustra a demonstração do Teorema de Wilson.

Exemplo

Pretende-se provar que o resto da divisão de $12!$ *por* 13 *é* 12*, ou seja, que* $12! \equiv -1 (\mathrm{mod}\, 13)$*. Da lista* $2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ *podemos formar* $\frac{13-3}{2} = 5$ *pares de números* (a, a') *tais que* $a \neq a'$ *e* $aa' \equiv 1 (\mathrm{mod}\, 13)$*:*

$$\begin{aligned} 2 \times 7 &\equiv 1 (\mathrm{mod}\, 13), & 3 \times 9 &\equiv 1 (\mathrm{mod}\, 13), \\ 4 \times 10 &\equiv 1 (\mathrm{mod}\, 13), & 5 \times 8 &\equiv 1 (\mathrm{mod}\, 13), \\ 6 \times 11 &\equiv 1 (\mathrm{mod}\, 13). \end{aligned}$$

Então

$$2 \times 7 \times 3 \times 9 \times 4 \times 10 \times 5 \times 8 \times 6 \times 11 \equiv 1 (\mathrm{mod}\, 13),$$

i.e.,

$$11! \equiv 1 (\mathrm{mod}\, 13).$$

Logo $12! = 12 \times 11! \equiv 12 \times 1 (\mathrm{mod}\, 13)$*, i.e.,* $(13-1)! \equiv -1 (\mathrm{mod}\, 13)$.

O recíproco do Teorema de Wilson é também verdadeiro.

Teorema

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

Demonstração.

Admitamos que n não é primo. Então existe um inteiro d tal que $1 < d \leq n-1$ e $d \mid n$. Uma vez que $1 < d \leq n-1$, tem-se que $d \mid (n-1)!$. Atendendo a que $d \mid n$ e que, por hipótese, $n \mid (n-1)! + 1$, concluímos que $d \mid (n-1)! + 1$. Logo

$$d \mid (n-1)! + 1 - (n-1)!,$$

ou seja, $d \mid 1$, o que contradiz o facto de $1 < d$. Logo, n é primo. □

Alguns teoremas relevantes na teoria de números

Dos teoremas anteriores obtem-se, assim, uma caraterização para os números primos: um número inteiro positivo n é primo se e só se $(n-1)! \equiv -1 (\mathrm{mod}\, n)$.

Note-se, porém, que esta caracterização tem mais interesse teórico do que aplicação prática, pois à medida que n cresce, $(n-1)!$ aumenta muito rapidamente.