Teoria de Números

1. Divisibilidade de números inteiros
2. Equações Diofantinas
3. Números primos
4. Congruências módulo um inteiro n
5. Congruências Lineares
6. Teorema de Fermat e Teorema de Euler

1 - Divisibilidade de números inteiros

Exemplo

Se dividirmos 171 objectos por caixas com capacidade para 14 objectos, quantas caixas conseguimos completar e quantos objectos sobram?

Queremos determinar o quociente e o resto da divisão de 171 por 14 :

$$\begin{array}{r|l} 171 & 14 \\ \cline{2-2} 31 & 12 \\ 3 & \end{array} \qquad \text{e portanto} \qquad 171 = 12 \times 14 + 3$$

pelo que o quociente da divisão é 12 e o resto é igual a 3.

Exemplo

Também podemos resolver este problema usando a recta real.

A partir da origem vamos avançando 14 unidades obtendo os inteiros $14, 28, 42, \cdots$ até obtermos o inteiro mais próximo de 171 que não excede 171, neste caso o inteiro 168.

O número de vezes que avançamos 14 unidades indica-nos o valor do quociente e o número de unidades necessárias para atingir o inteiro 171, a partir do inteiro 168, indica-nos o valor do resto.

$$0 \underset{14}{\longrightarrow} 14 \underset{14}{\longrightarrow} 28 \underset{14}{\longrightarrow} 42 \underset{14}{\longrightarrow} \cdots \underset{14}{\longrightarrow} 168 \underset{3}{\longrightarrow} 171$$

Exemplo

Vejamos uma forma mais interessante de ver o problema na recta real:

A partir do inteiro 171 vamos avançando 14 unidades na direção da origem da recta real, até atingirmos um inteiro positivo inferior a 14.

Esse inteiro será o valor do resto e o número de vezes que nos deslocamos 14 unidades indica-nos o valor do quociente .

Neste exemplo, a partir do inteiro 171 vamos obtendo os inteiros: $157, 143, 129, 115, \cdots$ que têm a particularidade de todos eles darem resto 3, quando divididos por 14.

$$0 \quad \underset{3}{\longleftarrow} \quad 3 \quad \underset{14}{\longleftarrow} \quad 17 \quad \underset{14}{\longleftarrow} \quad \cdots \quad \underset{14}{\longleftarrow} \quad 143 \quad \underset{14}{\longleftarrow} \quad 157 \quad \underset{14}{\longleftarrow} \quad 171$$

Exemplo

Assim, para calcular o resto da divisão de 171 por 14, em vez de efectuarmos a divisão, podemos subtrair a 171 múltiplos de 14 até obter um inteiro entre 0 e 13.

$$171 - 140 = 31 \qquad 31 - 28 = 3$$

Da primeira vez subtraímos, 10×14 e da segunda vez, 2×14. No total, subtraímos 12 vezes 14.

Logo o quociente da divisão de 171 por 14, é 12 e o resto é 3.

Algoritmo da divisão (para inteiros positivos)

Dados $a, b \in \mathbb{N}$ existem inteiros únicos, $q, r \in \mathbb{N}_0$, tais que:

$$a = q \times b + r \quad \text{com} \quad 0 \leq r < b$$

Este resultado pode ser generalizado para inteiros (positivos ou negativos):

Algoritmo da divisão (para inteiros)

Dados $a, b \in \mathbb{Z} \backslash \{0\}$, existem inteiros únicos, $q, r \in \mathbb{Z}$, tais que:

$$a = q \times b + r \quad \text{com} \quad 0 \leq r < |b|$$

Exemplos (inteiros negativos)

1. Vamos calcular o quociente e o resto da divisão de 171 por -14:

Sabemos que: $171 = 12 \times 14 + 3$
pelo que, $171 = (-12) \times (-14) + 3$
Logo

$$q = -12 \quad \text{e} \quad r = 3$$

2. Vamos calcular o quociente e o resto da divisão de -171 por 14:

Sabemos que: $171 = 12 \times 14 + 3$
pelo que, $-171 = -12 \times 14 - 3 = -12 \times 14 - 14 + 14 - 3 =$
$= -13 \times 14 + 11$
Logo

$$q = -13 \quad \text{e} \quad r = 11$$

Exemplos (inteiros negativos)

3. Vamos calcular o quociente e o resto da divisão de -171 por -14:

Sabemos que: $171 = 12 \times 14 + 3$

pelo que, $-171 = 12 \times (-14) - 3 = 12 \times (-14) - 14 + 14 - 3 =$

$= 13 \times (-14) + 11$

Logo

$$q = 13 \quad \text{e} \quad r = 11$$

4. Vamos calcular o resto da divisão de 1351 por -14:

Basta subtrair múltiplos de 14 a 1351 até obter um inteiro entre 0 e 13

$$1351 - 1400 = -49 \qquad -49 + 56 = 7$$

Logo o resto da divisão de 1351 por -14 é igual a 7.

Nota: $q = -100 + 4 = -96$.

A relação de divisibilidade

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, quando o resto da divisão de a por b é zero, temos que $a = q \times b$ e nesse caso escrevemos $b|a$, isto é

$$b|a \qquad \Longleftrightarrow \qquad \exists\, q \in \mathbb{Z} \;:\; a = q \times b$$

Dizemos então que:

- b divide a
- b é um divisor de a
- a é divisível por b
- a é um múltiplo de b

Exemplo : $3|18$ uma vez que $18 = 6 \times 3$

Logo 3 é um divisor de 18, ou seja, 18 é um múltiplo de 3.

Propriedades da relação de divisibilidade

Sejam $a, b, c, d \in \mathbb{Z}\backslash\{0\}$. Então:

1. $a|a$
2. $a|b \quad \wedge \quad b|a \quad \Rightarrow \quad a = \pm\, b$
3. $a|b \quad \wedge \quad b|c \quad \Rightarrow \quad a|c$

4. $a|b \quad \Rightarrow \quad a|-b \quad \wedge \quad -a|b \quad \wedge \quad -a|-b$
5. $a|b \quad \wedge \quad c|d \quad \Rightarrow \quad ac|bd$

6. $a|b \quad \wedge \quad a|c \quad \Rightarrow \quad a|b+c$
7. $a|b \quad \wedge \quad a|c \quad \Rightarrow \quad a|b-c$
8. $a|b+c \quad \wedge \quad a|b \quad \Rightarrow \quad a|c$
9. $a|b \quad \wedge \quad a|c \quad \Rightarrow \quad a|bx+cy \quad \forall x, y \in \mathbb{Z}$

Propriedades da relação de divisibilidade

Demonstração 9.

Como $a|b$ temos que $b = q_1\ a$ com $q_1 \in \mathbb{Z}$
Como $a|c$ temos que $c = q_2\ a$ com $q_2 \in \mathbb{Z}$

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

$$bx + cy = (aq_1)x + (aq_2)y = a(q_1x + q_2y)$$

e como $q_1x + q_2y \in \mathbb{Z}$ temos que $a|bx + cy$

Exemplo

Como $7|28$ e $7|56$ então $7|28 + 56$

Dado $b \in \mathbb{Z}$, se $7|28 + b$ como $7|28$ então $7|b$

Máximo divisor comum

Definição

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, chama-se máximo divisor comum entre a e b, e representa-se por m.d.c.(a, b), ao maior inteiro positivo que é simultaneamente divisor de a e divisor de b.

Exemplo   Vamos calcular m.d.c.$(36, 45)$:

divisores positivos de 36 : $1, 2, 3, 4, 6, 9, 12, 18, 36$

divisores positivos de 45 : $1, 3, 5, 9, 15, 45$

Logo,   m.d.c.$(36, 45) = 9$.

Nota :   m.d.c.$(-36, 45)$ = m.d.c.$(-36, -45)$ = m.d.c.$(36, -45) = 9$

Máximo divisor comum

Vamos agora calcular m.d.c.$(36, 45)$, por outro processo:

$36 = 2 \times 2 \times 3 \times 3 \qquad 45 = 3 \times 3 \times 5$

Logo, m.d.c.$(36, 45) = 3 \times 3 = 9$.

Definição

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, se m.d.c.$(a, b) = 1$, dizemos que os inteiros a e b são primos entre si .

Nota : Se m.d.c.$(a, b) = c > 1$ então $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros e são primos entre si.

Máximo divisor comum (propriedades)

Teorema

Dados $a, b \in \mathbb{Z}\backslash\{0\}$ *existem inteiros* $x, y \in \mathbb{Z}$ *tais que:*

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

Proposição

Dados $a, b, c \in \mathbb{Z}\backslash\{0\}$

$$a|c \quad \wedge \quad b|c \quad \wedge \quad \textit{m.d.c.}(a, b) = 1 \quad \Longrightarrow \quad ab|c$$

Proposição

(Lema de Euclides): Dados $a, b, c \in \mathbb{Z}\backslash\{0\}$

$$a|bc \quad \wedge \quad \textit{m.d.c.}(a, b) = 1 \quad \Longrightarrow \quad a|c$$

Nota : $4|12$ e $6|12$ mas no entanto $4 \times 6 \nmid 12$
Nota : $6|4 \times 9$ mas no entanto $6 \nmid 4$ e $6 \nmid 9$

Mínimo múltiplo comum

Definição

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, *chama-se* *mínimo múltiplo comum* *entre* a *e* b , *e representa-se por* *m.m.c.*(a, b) , *ao menor inteiro* *positivo* *que é simultaneamente múltiplo de* a *e múltiplo de* b .

Teorema

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, $\quad \text{m.m.c.}(a, b) = \dfrac{|\, a\, b\, |}{\text{m.d.c.}(a, b)}$

Exemplo

$$\text{m.m.c.}(36, 45) = \frac{|\, 36 \times 45\, |}{\text{m.d.c.}(36, 45)} = \frac{36 \times 45}{9} = 4 \times 45 = 180$$

Algoritmo de Euclides (250 a.c.)

Dados $a, b \in \mathbb{N}$ queremos calcular m.d.c.(a, b).
Supondo que $a > b$, pelo algoritmo da divisão existem $q, r \in \mathbb{N}_0$, únicos, tais que

$$a = qb + r \quad \text{com} \quad 0 \leq r < b$$

vamos mostrar que;

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

Seja $d \in \mathbb{N}$ tal que $d|a$ e $d|b$ então $d|a - qb = r$. Logo $d|b$ e $d|r$
Reciprocamente, se $d|b$ e $d|r$ então $d|qb + r = a$. Logo $d|a$ e $d|b$.

Algoritmo de Euclides

Assim, em vez de calcularmos m.d.c.(a, b) podemos calcular m.d.c.(b, r).

Como $b > r$, pelo algoritmo da divisão existem $q_1, r_1 \in \mathbb{N}_0$, tais que

$$b = q_1 r + r_1 \quad \text{com} \quad 0 \leq r_1 < r$$

Pelo que teremos

$$\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r) = \text{m.d.c.}(r, r_1)$$

Dividindo agora r por r_1 e repetindo sucessivamente este processo, como os restos obtidos são cada vez menores, a certa altura teremos que obter resto zero na divisão.
Nessa divisão de resto zero, o menor dos inteiros será o m.d.c. , ou seja, o m.d.c. será o último resto não nulo que obtivermos.

Algoritmo de Euclides - Exemplo

Vamos usar o algoritmo de Euclides para calcular m.d.c.$(340, 812)$

$812 = 2 \times 340 + 132$

$340 = 2 \times 132 + 76$

$132 = 1 \times 76 + 56$

$76 = 1 \times 56 + 20$

$56 = 2 \times 20 + 16$

$20 = 1 \times 16 + 4$

$16 = 4 \times 4 + 0$

Logo m.d.c.$(340, 812) = 4$

Vamos agora usar o algoritmo de Euclides para escrever o m.d.c.$(340, 812)$ como combinação linear de 340 e 812

$$4 = 20 - 1 \times 16 =$$

$$= 20 - 1 \times (56 - 2 \times 20) = -56 + 3 \times 20 =$$

$$= -56 + 3 \times (76 - 56) = 3 \times 76 - 4 \times 56 =$$

$$= 3 \times 76 - 4 \times (132 - 76) = -4 \times 132 + 7 \times 76 =$$

$$= -4 \times 132 + 7 \times (340 - 2 \times 132) = 7 \times 340 - 18 \times 132 =$$

$$= 7 \times 340 - 18 \times (812 - 2 \times 340) = -18 \times 812 + 43 \times 340$$

$$\text{m.d.c.}(340, 812) = 4 = 43 \times 340 - 18 \times 812$$