1. Determine o quociente e o resto na divisão de :

(a) 149 por $-23$;

(b) 310156 por 197;

(c) 32 por 45;

(d) 0 por 28;

(e) $-19$ por 6;

(f) $-234$ por $-9$.

Teorema (teorema do algoritmo da divisão)

Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q$ e $R \in \mathbb{Z}$ univocamente determinados tais que $a = bq + R$ e $0 \leq R < |b|$

a) $a = 149$ $b = -23$

Temos $149 = 6 \times 23 + 11$

$149 = (-6) \times (-23) + 11$ $q = -6$ e $R = 11$

$0 \leq R < |-23|$

b) $a = 310156 \qquad b = 197$

$$\begin{array}{r|l} 310156 & 197 \\ \cline{2-2} 1131 & 1574 \\ 1465 & \\ 866 & \\ 78 & \end{array}$$

$310 = 197 + 113$

$1131 = 5 \times 197 + 146$

$1465 = 7 \times 197 + 86$

$866 = 4 \times 197 + 78$

Assim: $310156 = 1574 \times 197 + 78$

$q = 1574$

$r = 78$

$0 \leq r < |197|$

c) $32$ por $45$

$32 = 0 \times 45 + 32$

$q = 0 \qquad r = 32$

$0 \leq r < |45|$

d) $0$ por $28$

$0 = 0 \times 28 + 0$

$q = 0 \qquad r = 0$

e) $-19$ por $-6$

$$19 = 3 \times 6 + 1$$
$$-19 = 3 \times (-6) - 1$$
$$-19 = 3 \times (-6) - 1 + 6 - 6$$
$$-19 = 4 \times (-6) + 5$$

$q = 4$ $r = 5$

$0 \leq r < |-6|$

f) $-234$ por $-9$

$$234 = 26 \times 9 \iff -234 = 26 \times (-9)$$

$q = 26$

$r = 0$

2. Utilizando o Algoritmo da Divisão, mostre que

(a) o quadrado de um inteiro é da forma $3k$ ou $3k+1$, para certo inteiro não negativo $k$;

(b) $3a^2-1$ não é um quadrado perfeito, para todo o inteiro $a$.

a) Seja $n$ um quadrado. Então $n = a^2$.

Para $a \in \mathbb{Z}$ temos que $a = 3q + r$ com $r \in \{0,1,2\}$

Assim $n = a^2 = (3q+r)^2 = 9q^2 + 6qr + r^2$

Se $r = 0$: $\quad n = 9q^2 = 3(3q^2)$

logo $n = 3k$ com $k = 3q^2$

Se $r = 1$: $\quad n = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$

logo $n = 3k' + 1$ com $k' = 3q^2 + 2q$

Se $r = 2$: $\quad n = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$

logo $n = 3k'' + 1$ com $k'' = 3q^2 + 2q$

Conclusão: Se $n = a^2$ então o resto da divisão de $n$ por 3 ou é 0 ou é 1, não pode ser 2.

b) Queremos mostrar que $3a^2 - 1$ não é um quadrado

Usando a alínea a) basta mostrar que o resto da divisão de $n = 3a^2 - 1$ por 3 é igual a 2.

Temos $n = 3a^2 - 1 = 3a^2 - 3 + 2 = 3(a^2 - 1) + 2$

Logo $n = 3q + 2$ com $q = a^2 - 1$, ou seja, pela unicidade no teorema do algoritmo da divisão, o resto da divisão de $n$ por 3 é 2. Assim, $n = 3a^2 - 1$ não pode ser um quadrado.

4. Verifique que, para todo o inteiro $n \geq 1$, $\frac{n(n+1)(2n+1)}{6}$ é um inteiro.

Queremos mostrar que $6 \mid n(n+1)(2n+1)$

Basta mostrar que $2 \mid n(n+1)(2n+1)$ e $3 \mid n(n+1)(2n+1)$

- Vejamos que $2 \mid n(n+1)(2n+1)$

Temos $n = 2q + r$ com $r \in \{0, 1\}$

- se $r = 0$ $n = 2q$

Logo $n(n+1)(2n+1) = 2q(2q+1)(4q+1) = 2[q(2q+1)(4q+1)]$

- se $r = 1$ $n = 2q+1$

Logo $n(n+1)(2n+1) = (2q+1)(2q+2)(4q+3) = 2[(2q+1)(q+1)(4q+3)]$

- Vejamos que $3 \mid n(n+1)(2n+1)$

Temos $n = 3q + r$ com $r \in \{0, 1, 2\}$

- se $r = 0$ $\quad n = 3q$

$$n(n+1)(2n+1) = 3q(3q+1)(6q+1) = 3[q(3q+1)(6q+1)]$$

- se $r = 1$ $\quad n = 3q+1$

$$n(n+1)(2n+1) = (3q+1)(3q+2)(6q+3) = 3[(3q+1)(3q+2)(2q+1)]$$

- se $r = 2$ $\quad n = 3q+2$

$$n(n+1)(2n+1) = (3q+2)(3q+3)(6q+5) = 3[(3q+2)(q+1)(6q+5)]$$

Como $2 \mid n(n+1)(2n+1)$ e $3 \mid n(n+1)(2n+1)$ então

$$6 \mid n(n+1)(2n+1)$$

8. Mostre que, para todo o inteiro $a$, um dos inteiros $a$ e $a+2$ ou $a+4$ é divisível por 3.

Pelo Teorema do Algoritmo da divisão, existem $q$ e $r$ únicos tais que $a = 3q + r$ com $r \in \{0, 1, 2\}$

- Se $r = 0$ então $a = 3q$ e $3 \mid a$
- Se $r = 1$ então $a = 3q+1$

  logo $a+2 = 3q+3 = 3(q+1)$ e $3 \mid a+2$
- Se $r = 2$ então $a = 3q+2$

  logo $a+4 = 3q+6 = 3(q+2)$ e $3 \mid a+4$.

10. Utilizando o Algoritmo de Euclides, determine o máximo divisor comum de cada par de inteiros $a$ e $b$ e escreva-o como combinação linear de $a$ e $b$:

(a) $a = 1001$, $b = 357$;

(b) $a = 1001$, $b = 33$;

(c) $a = 56$, $b = 126$;

(d) $a = -90$, $b = 1386$;

(e) $a = -2860$, $b = -2310$.

**Lema** (Algoritmo de Euclides)

Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Sejam $q$ e $r \in \mathbb{Z}$ tais que $a = bq + r$ então $m.d.c(a, b) = m.d.c(b, r)$

**Nota:** $m.d.c(a, b) = m.d.c(|a|, |b|)$

**Teorema** Dados $a, b \in \mathbb{Z}$ existem $x, y \in \mathbb{Z}$ tais que

$$m.d.c(a, b) = ax + by.$$

a) $a = 1001$ $\quad b = 357$ $\qquad m.d.c(1001, 357) = ?$

Aplicando a algoritmo da divisão, temos

$$1001 = 2 \times \underline{357} + \underline{287}$$

$$357 = 1 \times \underline{287} + \underline{70}$$

$$287 = 4 \times \underline{70} + \underline{7}$$

$$70 = 10 \times 7 + \underline{0}$$

Aplicando o lema de Euclides

$$m.d.c(1001, 357) = m.d.c(357, 287) = m.d.c(287, 70) =$$

$$= m.d.c(70, 7) = 7$$

"Andamos para trás" e temos

$7 = 287 - 4 \times 70 =$

$= 287 - 4 \times (357 - 287) =$

$= 5 \times 287 - 4 \times 357 =$

$= 5 \times (1001 - 2 \times 357) - 4 \times 357 =$

$= 5 \times \underline{1001} - 14 \times \underline{357}$

Logo $7 = m.d.c(1001, 357) = x\, 1001 + y\, 357$

com $x = 5$ e $y = -14$.

b) $a = 1001$ e $b = 33$

$1001 = 30 \times 33 + 11$ $\quad m.d.c(1001, 33) = 11$

$33 = 3 \times 11 + 0$ $\quad 11 = \underline{1001} - 30 \times \underline{33}$

c) $a = -90$ e $b = 1386$

$$m.d.c(-90, 1386) = m.d.c(90, 1386)$$

$$90 = 0 \times \underline{1386} + \underline{90}$$

$$1386 = 15 \times \underline{90} + \underline{36}$$

$$90 = 2 \times \underline{36} + \underline{18}$$

$$36 = 2 \times 18 + 0$$

$$m.d.c(1386, 90) = 18$$

$$18 = 90 - 2 \times 36$$

$$= 90 - 2 \times (1386 - 15 \times 90) =$$

$$= -2 \times \underline{1386} + 31 \times \underline{90}$$

12. Determine o menor inteiro positivo $k$ da forma $k = 22x + 55y$, onde $x$ e $y$ são inteiros.

$$T = \{22x + 55y : x, y \in \mathbb{Z}\}$$

é o conjunto dos múltiplos de m.d.c$(22, 55)$

Portanto o menor inteiro positivo da forma $22x + 55y$ é o m.d.c$(22, 55)$.

$$\left.\begin{aligned} 55 &= 2 \times 22 + 11 \\ 22 &= 2 \times 11 + 0 \end{aligned}\right\} \Rightarrow \text{m.d.c}(22, 55) = 11.$$

$11 = 55 - 2 \times 22$ $\quad x = -2$ e $y = 1$.