Lista de Exercícios 09

1. Prove que, se x é um inteiro impar, então x^3 é impar.

   Prova: Suponha n ímpar, isto é, $n = 2k + 1$ para algum $k \in \mathbb{Z}$. Temos:

   $$x^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$$

   Então $x^3 = 2k' + 1$, onde k' é o inteiro $4k^3 + 6k^2 + 3k$. Portanto, x^3 é impar.

2. Suponha $x, y \in \mathbb{Z}$. Prove que se x e y são impares, então xy é impar.

   Prova: Suponha x e y impares, isto é, $x = 2k + 1$ e $y = 2k' + 1$, para $k, k' \in \mathbb{Z}$. Temos:

   $$xy = (2k + 1)(2k' + 1) = 4kk' + 2k + 2k' + 1 = 2(2kk' + k + k') + 1$$

   Então $xy = 2k'' + 1$, onde k'' é o inteiro $2kk' + k + k'$. Portanto, xy é impar.

3. Prove que, se n é impar, então $3n + 9$ é par.

   Prova: Suponha n ímpar, isto é, $n = 2k + 1$ para algum $k \in \mathbb{Z}$. Temos

   $$3n + 9 = 3(3k + 1) + 9 = 6k + 12 = 2(3k + 4)$$

   Então, $3n + 9 = 2k'$, onde $k' = 3k + 4$. Portanto, $3n + 9$ é par.

4. Prove que, se a soma de dois inteiros é par, então sua diferença também é par.

   Prova: Sejam $n, m \in \mathbb{Z}$ e suponha $n + m$ par, isto é, $n + m = 2k$ para algum $k \in \mathbb{Z}$. Temos

   $$n - m = (n + m) - 2m = 2k - 2m = 2(k - m)$$

   Então $n - m = 2k'$, onde k' é o inteiro $k - m$ e, portanto, $n - m$ é par. Note que $m - n = -(n - m)$ e, portanto, $m - n$ é também par.

5. Suponha $a, b \in \mathbb{Z}$. Prove que, se $a|b$ então $a^2|b^2$.

   Prova: Suponha $a|b$, isto é $b = k.a$ para algum $k \in \mathbb{Z}$. Temos que$b^2 = (k.a)^2 = k^2.a^2$, ou seja, $b^2 = ma^2$, onde m é o inteiro k^2, e, portanto, $a^2|b^2$.

6. Prove que, se n e m são quadrados perfeitos, então $(n\,m)$ é um quadrado perfeito.

   Prova: Sejam $n, m \in \mathbb{Z}$ e suponha que n e m são ambos quadrados perfeitos, isto é $n = p^2$ e $m = q^2$, onde $p, q \in \mathbb{Z}$. Temos

   $$n\,m = p^2\,q^2 = (p\,q)^2$$

   Então $n\,m = k^2$, onde $k = p\,q$ e, portanto, $n\,m$ é um quadrado perfeito.

7. Prove que, se a e b são números racionais, então $(a + b)$ é um número racional.

   Prova: Sejam a e b racionais, isto é, $a = n/m$ e $b = p/q$, onde $n, m, p, q \in \mathbb{Z}$ e $m, q \neq 0$. Temos que

   $$a + b = \frac{n}{m} + \frac{p}{q} = \frac{nq + pm}{mq}$$

   Então $a + b = r/s$, onde $r = nq + pm \in \mathbb{Z}$ e $s = mq \in \mathbb{Z}$, já que o produto e a soma de números inteiros é um número inteiro; além disso $s \neq 0$, pois $m \neq 0$ e $q \neq 0$. Portanto, $(a + b)$ é racional.

8. Sejam $a, b, c \in \mathbb{Z}$. Prove que se $a|b$ e $a|c$ então $a|(b + c)$.

   Prova: Sejam $a, b, c \in \mathbb{Z}$ e suponha $a|b$ e $a|c$. Temos que

   $$\frac{b + c}{a} = \frac{b}{a} + \frac{c}{a}$$

   Como $a|b$ e $a|c$, temos que (b/a) e (c/a) são ambos inteiros e, então, $(b/a)+(c/a)$ é um inteiro. Portanto, $a|(b + c)$.

9. Suponha $x, y \in \mathbb{R}$. Prove que se $x^2 + 5y = y^2 + 5x$, então $x = y$ ou $x + y = 5$.

   Prova: Suponha $x^2 + 5y = y^2 + 5x$, ou seja, $x^2 - y^2 = 5(x - y)$. Sabemos que $x^2 - y^2 = (x + y)(x - y)$. Então, $(x + y)(x - y) = 5(x - y)$. Portanto, temos que $x - y = 0$, isto é, $x = y$, ou $x + y = 5$.

10. Prove que, se $n \in \mathbb{Z}$, então $5n^2 + 3n + 7$ é impar.

    Prova: Considere os seguintes possíveis casos:

    (a) n é par: Então n^2 é par e, portanto, $5n^2$ é par. Além disso, $3n$ é par. Então, $5n^2 + 3n + 7$ é a soma de dois pares e um ímpar, que é ímpar.

    (b) n é impar: Então n^2 é impar e, portanto, $5n^2$ é impar, pois é o produto de dois impares. Do mesmo modo, $3n$ é impar. Então, $5n^2 + 3n + 7$ é a soma de três impares, que é ímpar.

11. Prove que, para todo $n \in \mathbb{N}$, $n^2 = 2\binom{n}{2} + \binom{n}{1}$

    Prova: Considere os seguintes possíveis casos:

    (a) $n = 0$: Temos que $\binom{0}{2} = \binom{0}{1} = 0$. Portanto $0^2 = 2\binom{0}{2} + \binom{0}{1}$.

    (b) $n = 1$: Temos que $\binom{1}{2} = 0$ e $\binom{1}{1} = 1$. Portanto, $1^2 = 2\binom{1}{2} + \binom{1}{1}$.

    (c) $n > 0$: Temos que

    $$\begin{aligned} 2\binom{n}{2} + \binom{n}{1} &= 2\tfrac{n!}{2!(n-2)!} + \tfrac{n!}{(n-1)!} \\ &= n(n-1) + n \\ &= n^2 \end{aligned}$$

12. Seja $n \in \mathbb{Z}$. Prove que se n^2 é par então n é par.

    Prova: (Contrapositivo). Suponha que n é ímpar, isto é, $n = 2k + 1$, para algum $k \in \mathbb{Z}$. Temos

    $$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

    Então $n^2 = 2k' + 1$, onde k' é o inteiro igual e $2k^2 + 2k$. Portanto, n^2 é ímpar.

13. Sejam $a, b \in \mathbb{Z}$. Prove que se $a^2(b^2 - 2b)$ é impar, então a e b são ambos impares.

    Prova: (Contrapositivo). Suponha que a é par ou b é par. Se a é par, temos que a^2 é par e, portanto $a^2(b^2 - 2b)$ é par. Por outro lado, se b é par, temos que b^2 é par e, então $(b^2 - 2b$ é par, pois é a diferença entre dois números pares. Então, $a^2(b^2 - 2b)$ é par. Portanto, se $a^2(b^2?2b)$ é impar, então a e b são ambos impares.

14. Suponha $x \in \mathbb{R}$. Prove que se $x^2 + 5x < 0$ então $x < 0$.

    Prova: (Contrapositivo). Sabemos que $x^2 \geq 0$. Supondo $x \geq 0$, temos que $5x \geq 0$ e, portanto $x^2 + 5x \geq 0$. Portanto, se $x^2 + 5x < 0$ então $x < 0$.

15. Prove que se r é um número irracional, então $\sqrt{r}$ é irracional. **Prova**: (Contrapositivo). Suponha que $\sqrt{r}$ é racional, isto é, $\sqrt{r} = n/m$, onde $n, m \in \mathbb{Z}$ e $m \neq 0$. Temos que

    $$n = (\sqrt{n})^2 = (\frac{n}{m})^2 = \frac{n^2}{m^2}$$

    Então $n = p/q$, onde $p = n^2 \in mathbbZ$ e $q = m^2 \in \mathbb{Z}$ e $q \neq 0$, já que $m \neq 0$. Ou seja, n é racional. Portanto, se n é irracional, então $\sqrt{n}$ é irracional.

16. Prove que, se o produto de dois números inteiros (xy) não é divisível por n, então x não é divisível por n e y não é divisível por n.

    Prova: (Contrapositivo). Suponha que x é divisível por n ou que y é divisível por n. Considere os seguintes possíveis casos:

    (a) x é divisível por n, isto é, $x = kn$, onde $k \in \mathbb{Z}$. Então $xy = (kn)y = (ky)n$. Ou seja, $xy = k'n$ onde k' é o inteiro (ky). Portanto, (xy) é divisível por n.

    (b) y é divisível por n, isto é, $y = kn$, onde $k \in \mathbb{Z}$. Então $xy = x(kn) = (kx)n$. Ou seja, $xy = k'n$ onde k' é o inteiro (kx). Portanto, (xy) é divisível por n.

17. Sejam a e b inteiros não nulos. Prove que $mdc(a, b) = mdc(a - b, b)$.

    Prova: (Direta) Sejam a e b inteiros não nulos e seja $d = mdc(a, b)$. Como d é um divisor de a e de b, temos que $a = dn$ e $b = dm$, para alguns inteiros n e m. Então $a-b = dn-dm = d(n-m)$ e, portanto, d é também um divisor de $a-b$. Como ele não pode ser maior que o máximo divisor comum de $a - b$ e b, temos que $d \leq mdc(a - b, b)$.

    Seja agora $e = mdc(a-b, b)$. Então, e é um divisor de $a-b$ e de b, isto é, $a-b = en$ e $b = em$, para alguns inteiros n e m. Então $a = (a - b) + b = en + em = e(n + m)$. Portanto, temos que e é um divisor tanto de a como de b. Mas e não pode ser maior do que o máximo divisor comum de a e b, isto é, $mdc(a - b, b) = e \leq mdc(a, b)$.

    Os dois parágrafos acima nos dão que $mdc(a, b) \leq mdc(a - b, b)$ e $mdc(a - b, b) \leq mdc(a, b)$. Portanto, $mdc(a, b) = mdc(a - b, b)$.

Definições úteis

Definição 1 *Seja $n \in \mathbb{Z}$. n é **par** se existe $k \in \mathbb{Z}$ tal que $n = 2k$; n é **impar** se existe $k \in \mathbb{Z}$ tal que $n = 2k + 1$.*

Definição 2 *Sejam $n, d \in \mathbb{Z}$. Dizemos que n é divisível por d (notação $d|n$) se existe $k \in \mathbb{Z}$ tal que $n = kd$.*

Definição 3 *Um número n é um **quadrado perfeito** se existe $k \in \mathbb{Z}$ tal que $n = k^2$.*

Definição 4 *Seja $n \in \mathbb{Z}$ e $n > 1$. n é **primo** se, para quaisquer $m, k \in \mathbb{Z}$ tais que $n = mk$, temos $m = 1$ ou $k = 1$; n é **composto** caso contrário, isto é, se existem $m, k \in \mathbb{Z}$ tais que $n = mk$ e $m \neq 1$ e $k \neq 1$.*

Definição 5 *Seja $r \in \mathbb{R}$. r é **racional** se existem $p, q \in \mathbb{Z}$ tais que $r = p/q$ e $q \neq 0$; r é irracional caso contrário.*

Definição 6 *O **Máximo divisor comum** de dois inteiros a e b, denotado como $mdc(a, b)$ é o maior inteiro que divide tanto a quanto b. O **mínimo múltiplo comum** de dois inteiros a e b, denotado como $mmc(a, b)$, é o menor inteiro que é múltiplo tanto de a quanto de b. **Observações:** $mdc(a, 0) = mdc(0, a) = |a|$ se $a \neq 0$; $mdc(0, 0) = \infty$.*