Aula 13. Revisão

13.1 Indução finita

Exercício 13.1

Mostre que

$$1 \cdot 2 + 2 \cdot 3 + \ldots + n \cdot (n+1) = \frac{n \cdot (n+1) \cdot (n+2)}{3}$$

para todos $n \geq 1$.

Solução 13.1

Vamos prosseguir pela indução finita.

Base $n = 1$.

$$1 \cdot 2 = \frac{1 \cdot 2 \cdot 3}{3}$$

Assim afirmação é verdadeira.

Hipótese $n = k$.

Suponha que para $n = k$ afirmação é verdadeira ou seja

$$1 \cdot 2 + 2 \cdot 3 + \ldots + k(k+1) = \frac{k \cdot (k+1) \cdot (k+2)}{3}$$

Hipótese $n = k+1$.

Vamos provar afirmação no caso $n = k+1$, ou seja precisamos provar que

$$1 \cdot 2 + 2 \cdot 3 + \ldots + k(k+1) + (k+1)(k+2) = \frac{(k+1) \cdot (k+2) \cdot (k+3)}{3}$$

Usando hipótese temos

$$\begin{aligned} 1 \cdot 2 + 2 \cdot 3 + \ldots + k \cdot (k+1) + (k+1) \cdot (k+2) &= \frac{k \cdot (k+1) \cdot (k+2)}{3} + (k+1) \cdot (k+2) \\ &= \frac{(k+1) \cdot (k+2)}{3} \cdot [k+3] \\ &= \frac{(k+1) \cdot (k+2) \cdot (k+3)}{3} \end{aligned}$$

Aplicando o (PIF) a afirmação vale para todos $n \geq 1$.

Exercício 13.2

Mostre que $8 \mid 3^{2n} - 1$, para todos $n \geq 0$.

Solução 13.2

Vamos prosseguir pela indução finita.

Base $n = 0$. Neste caso temos

$$8 \mid 3^0 - 1 = 1 - 1 = 0.$$

Assim afirmação é verdadeira.

Para $n = k$, suponha $8 \mid 3^{2k} - 1$ e vamos provar para caso $n = k + 1$.

$$\begin{aligned} 3^{2(k+1)} - 1 = 3^2 \cdot 3^{2k} - 1 = 9 \cdot 3^{2k} - 1 \qquad (13.1) \\ = 8 \cdot 3^{2k} + 3^{2k} - 1 \qquad (13.2) \end{aligned}$$

Como 8 divide ambos $8 \cdot 3^{2k}$ e $3^{2k} - 1$, assim 8 divide $3^{2(k+1)} - 1$ tmb. Pelo (PIF) afirmação vale para todos n.

Exercício 13.3

Mostre que

$$11 \mid 6^{2n-2} + 3^{n+1} + 3^{n-1},$$

para todos $n \geq 1$.

Solução 13.3

De novo, vamos prosseguir pela indução finita.

Base $n = 1$. Neste caso temos

$$6^{2 \cdot 1 - 2} + 3^{1+1} + 3^{1-1} = 1 + 9 + 1 = 11,$$

e afirmação é verdadeira.

Proseguido, vamos supor que para $n = k$, temos que

$$11 \mid 6^{2k-2} + 3^{k+1} + 3^{k-1},$$

e provaremos afirmação no caso $n = k + 1$. Neste caso temos

$$\begin{aligned} 6^{2(k+1)-2} + 3^{k+1+1} + 3^{k+1-1} &= 6^2 \cdot 6^{2k-2} + 3 \cdot 3^{k+1} + 3 \cdot 3^{k-1} \\ &= 33 \cdot 6^{2k-2} + 3 \cdot \left[6^{2k-2} + 3^{k+1} + 3^{k-1}\right] \end{aligned}$$

Agora notamos que 11 divide $33 \cdot 6^{2k-2}$ e divide o segundo somando pelo hipótese. Assim a afirmação vale pelo (PIF).

Exercício 13.4

Mostre que para todo $n \geq 1$, temos que

$$F_n \cdot F_{n+2} - (F_{n+1})^2 = (-1)^{n+1},$$

onde F_n é sequencia de Fibonacci, com $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, ...

$$F_{n+2} = F_{n+1} + F_n.$$

Solução 13.4

De novo prosseguimos por indução. Para $n = 1$ temos

$$F_1 \cdot F_3 - F_2^2 = 1 \cdot 2 - 1 = 1 = (-1)^{1+1}$$

Assim base da indução vale. Suponha que para $n = k$, temos que

$$F_k \cdot F_{k+2} - (F_{k+1})^2 = (-1)^{k+1}$$

Agora,

$$\begin{aligned} F_{k+1} \cdot F_{k+3} - (F_{k+2})^2 &= F_{k+1}(F_{k+1} + F_{k+2}) - (F_{k+2})^2 \\ &= F_{k+1}F_{k+1} + F_{k+1}F_{k+2} - (F_{k+2})^2 \\ &= (F_{k+1})^2 - F_{k+2}(F_{k+2} - F_{k+1}) \\ &= (F_{k+1})^2 - F_{k+2} \cdot F_k = (-1) \cdot (-1)^{k+1} = (-1)^{k+2}. \end{aligned}$$

Assim a formula vale para todos $n \geq 1$.

13.2 *Divisibilidade e primos*

Exercício 13.5

Mostre que todo inteiro da forma $6k+5$ é também da forma $3 \cdot k + 2$. Mas o contrario é falso.

Solução 13.5

Temos,

$$6k + 5 = 3 \cdot 2k + 3 + 2 = 3 \cdot (2k + 1) + 2 = 3 \cdot K + 2,$$

com $K = 2k + 1$, assim a afirmação é correto.

Por outro lado $8 = 3 \cdot 2 + 2$ ou seja $8 = 3k + 2$, com $k = 2$,

mas $8 \neq 6k+5$ para todos k inteiros, pois 8 tem o resto 2 quando divide por 6.

Exercício 13.6

Mostre que $30 \mid a^5 - a$ para todo $a \in \mathbb{Z}$

Solução 13.6

Como $2, 3, 5$ são primos entre si, basta mostrar que $2 \mid a^5 - a$, $3 \mid a^s - a$ e $5 \mid a^5 - a$. Temos que

$$\begin{aligned} a^5 - a &= a \cdot \left(a^4 - 1\right) \\ &= a \cdot \left(a^2 - 1\right) \cdot \left(a^2 + 1\right) \\ &= (a-1) \cdot a \cdot (a+1) \cdot (a^2+1). \end{aligned}$$

Temos que $(a-1) \cdot a$ e um numero par para todo a, pois este produto é produto de 2 inteiros consecutivos, logo 2 divide $a^5 - a$ para todo a.

Semelhante, $(a-1) \cdot a \cdot (a+1)$ é múltiplo de 3, pois é produto de 3 inteiros consecutivos. Assim e $3 \mid a^5 - a$ para todo a.

Agora, aplicando algoritmo da divisão temos uqe $a = 5q + r$, com $0 \leq r < 5$. Analizando os restos, temos:

$$\begin{array}{lll} r = 0 & \Rightarrow a = 5q + 0 & \Rightarrow 5 \mid a, \quad 5 \mid a^5 - a \\ r = 1 & \Rightarrow a = 5q + 1 & \Rightarrow 5 \mid a - 1, \quad 5 \mid a^5 - a \\ r = 4 & \Rightarrow a = 5q + 4 & \Rightarrow 5 \mid a + 1, \quad 5 \mid a^5 - a \end{array}$$

Se $r = 2$, assim $a = 5q + 2$, neste caso, temos

$$\begin{aligned} a^2 + 1 &= (5q+2)^2 + 1 \\ &= 25q^2 + 20q + 4 + 1 \\ &= 25q^2 + 20q + 5, \end{aligned}$$

Finalmente, se $r = 3$, assim $a = 5q + 3$, neste caso, temos

$$\begin{aligned} a^2 + 1 &= (5q+3)^2 + 1 \\ &= 25q^2 + 30q + 9 + 1 \\ &= 25q^2 + 30q + 10, \end{aligned}$$

logo $5 \mid a^2 + 1$ e assim $5 \mid a^5 - a$ neste caso.

Resumindo $5 \mid a^5 - a$ para todos a.

Exercício 13.7

Exescicio 8) Mostre que se $7 \mid a^2 + b^2$ assim $7 \mid a$ ou $7 \mid b$.

Solução 13.7

Suponha que $7 \nmid a$ e $7 \nmid b$. Assim $a = 7q_1 + r_1$, com $1 \leq r_1 < 7$ e $b = 7q_2 + r_2$, com $1 \leq r_2 < 7$. Agora, temos

$$\begin{aligned} a^2 + b^2 &= (7q_1 + r_1)^2 + (7a_2 + r_2)^2 \\ &= 49\left(q_1^2 + q_2^2\right) + 14\left(q_1 r_1 + q_2 r_2\right) + r_1^2 + r_2^2, \end{aligned}$$

Como $7 \mid (a^2 + b^2)$ assim $7 \mid (r_1^2 + r_2^2)$. Sem perda generalidade suponha que $r_1 \leq r_2$. Analizando os restos possíveis, temos os seguintes pares (r_1, r_2)

$$\begin{array}{cccccc} (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\ & & (3,3) & (3,4) & (3,5) & (3,6) \\ & & & (4,4) & (4,5) & (4,6) \\ & & & & (5,5) & (5,6) \\ & & & & & (6,6) \end{array}$$

Para cada par (r_1, r_2) vamos calcular $r_1^2 + r_2^2$ colocando os valores na tabela parecida:

$$\begin{array}{cccccc} 1^2 + 1^2 = 2 & 1^2 + 2^2 = 5 & 10 & 17 & 26 & 37 \\ & 2^2 + 2^2 = 8 & 13 & 20 & 29 & 40 \\ & & 18 & 25 & 34 & 45 \\ & & & 32 & 41 & 52 \\ & & & & 50 & 61 \\ & & & & & 72 \end{array}$$

Assim temos que $r_1^2 + r_2^2$ nao é múltiplo de 7 para todos opções! Contradição, ou seja $7 \mid a$ ou $7 \mid b$.

Exercício 13.8

Suponha que $p, p+2$ dois primos (tais primos chamam-se, primos gêmeos). Mostre que se $p > 5$, assim $12 \mid p + (p+2)$.

Solução 13.8

Basta ver que $4 \mid p + (p+2)$ e $3 \mid p + (p+2)$.

Como $p > 5$ e primo, assim o é um numero impar, logo $p = 2k + 1$ para algum k. Agora $p + 2 = 2k + 3$, logo

$$p + (p+2) = 2k + 1 + 2k + 3 = 4k + 4 = 4(k+1),$$

assim $4 \mid p + (p+2)$,

Aplicando algoritmo da divisão de o por 3, temos que

$$p = 3 \cdot q + r,$$

com $0 \leq r < 3$. Como $p > 5$ é um primo logo $r \neq 0$. Se $r = 1$, assim $p + 2 = 3q + 3 = 3(s+1)$ é um multiplo de 3 que é impossivel, pois $p+2$ e primo tmb. Assim unico opção possivel é $r = 2$. Neste caso temos

$$p = 3q + 2, \quad p + 2 = 3c + 2 + 2.$$

Logo $p + (p+2) = 3a + 2 + 3y + 4 = 6(q+1)$, portanto $3 \mid p + (p+2)$.

13.3 MDC e MMC

O que precisamos lembrar sobre mdc e mmc?

(a) **Definições**.
Um inteiro não-negativo d é *máximo divisor comum* de a e b se:

i) $d \mid a$ e $d \mid b$.

ii) se c é divisor comum de a e b, assim $c \mid d$.

Um inteiro não-negativo c é *minimo multiplo comum* de a e b se:

i) $a \mid c$ e $b \mid c$.

ii) se e é multiplo comum de a e b, assim $c \mid e$.

(b) **Como procurar**. Atraves lemma de Euclides: se $a = b \cdot q + r$ pare algum q, assim

$$\text{mdc}(a,b) = \text{mdc}(b,r)$$

e

$$\text{mdc}(a,b) \cdot \text{mmc}(a,b) = |a| \cdot |b|.$$

Através os primos: sejam

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha},$$
$$b = p_1^{\beta_1} \ldots p_t^{\beta_t}$$

inteiros nas condições acima. Então,

$$\text{mdc}(a,b) = p_1^{\gamma_1} \ldots p_t^{\gamma_t}, \text{ em que } \gamma_j = \min(\alpha_i, \beta_i).$$
$$\text{mmc}(a,b) = p_1^{\delta_1}, \ldots p_t^{\delta_t}, \text{ em que } \delta_i = \max(\alpha_i, \beta_i)$$

(c) **Teorema de Bezout:** existem $r, s \in \mathbb{Z}$, tais que

$$\text{mdc}(a,b) = a \cdot r + b \cdot s.$$

Exercício 13.9

Encontre mdc e mmc entre 119 e 279. Escreva $\text{mdc}(279, 119)$ como $279 \cdot x + 119 \cdot y$.

Solução 13.9

Aplicando algoritmo de Euclides, temos

$$\begin{aligned} 279 &= (2) \cdot 119 + 41 && \Rightarrow 41 = 279 - (2) \cdot 119 \\ 119 &= (2) \cdot 41 + 37 && \Rightarrow 37 = 119 - (2) \cdot 41 \\ 41 &= (1) \cdot 37 + 4 && \Rightarrow \quad 4 = 41 - (1) \cdot 37 \\ 37 &= (9) \cdot 4 + (1) && \Rightarrow 1 = 37 - (9) \cdot 4 \end{aligned}$$

Assim

$$\text{mdc}(279, 119) = 1$$

Agora aplicando formula

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = |a| \cdot |b|,$$

temos

$$\text{mmc}(279, 119) = 279 \cdot 119 = 33201$$

$$\begin{aligned} 1 &= 37 - (9) \cdot 4 = 37 - (9) \cdot (41 - (1) \cdot 5+) - \\ &= (10) \cdot 37 - (9) \cdot 41 = (10)(119 - (2) \cdot 41) - (9) \cdot 41 \\ &= (10) \cdot 119 - (29) \cdot 41 = (10) \cdot 119 - (25)(279 - (2) \cdot 119) \\ &= (68) \cdot 119 - (29) \cdot 279 \end{aligned}$$

Ou seja

$$- \quad 279 \cdot (-29) + 119 \cdot 68 = 1 = \text{mdc}(279, 119).$$

Exercício 13.10

Mostre que $\text{mdc}(2^n, 3^m) = 1$ para todos n, m.

Solução 13.10

Sejam $a = 2^n$ e $b = 3^m$. Temos que

$$a = 2^n \cdot 3^0, \qquad b = 2^0 \cdot 3^m,$$

assim calculando mdc através os primos temos

$$\text{mdc}(2^n, 3^m) = 2^0 \cdot 3^0 = 1.$$

Exercício 13.11

Sejam a, b, c tais que $a \mid b$ e $\text{mdc}(b, c) = 1$. Mostre que

$$\text{mdc}(a, c) = 1,$$

Solução 13.11

Temos que

$$\text{mdc}(a, b) = 1 \quad \Longleftrightarrow \quad ax + by = 1.$$

Como $\text{mdc}(b, c) = 1$ assim

$$b \cdot x_0 + c \cdot y_0 = 1,$$

para alguns x_0, y_0. Agora

$$\begin{aligned} 1 = b \cdot x_0 + c \cdot y_0 &= (a \cdot q) \cdot x_0 + c \cdot y_0 \\ &= a \cdot (q_i x_0) + c \cdot y_0 \\ &= a \cdot x_0' + c \cdot y_0 = 1 \end{aligned}$$

Assim $\text{mdc}(a, c) = 1$.

Exercício 13.12

Assumindo $\text{mdc}(a, b) = 1$ mostre que

$$\text{mdc}(2a + b, a + 2b) = 1 \quad ou \quad 3.$$

Solução 13.12

Seja $d = \text{mdc}(2a + b, a + 2b)$, assim

$$d \mid (2a + b) \quad d \mid (a + 2b),$$

portanto d também divide

$$(2a + b) \cdot 2 - (a + 2b) = 3a.$$

Na mesma maneira $d \mid 3b$ mas $\text{mdc}(a, b) = 1$, assim $d \mid 3$, logo $d = 1$ ou $d = 3$.

Exercício 13.13

Mostre que $\text{mdc}(m, n) = \text{mdc}(m - n, n)$ para todos inteiros m, n.

Solução 13.13

Sejam $d = \text{mdc}(m, n)$ e $d' = \text{mdc}(m - n, n)$. Assim

$$\begin{cases} d \mid m \\ d \mid n \end{cases} \Rightarrow \begin{cases} d \mid m - n \\ d \mid n \end{cases} \Rightarrow d \mid d'$$

Semelhante,

$$\begin{cases} d' \mid m - n \\ d' \mid n \end{cases} \Rightarrow \begin{cases} d' \mid m \\ d' \mid n \end{cases} \Rightarrow d' \mid d$$

Como $d \mid d'$ e $d' \mid d$ assim $d = d'$ (pois ambos são positivos).

Exercício 13.14

Sejam a, m, n inteiros positivos, com

$$\text{mdc}(a, n) = 1 = \text{mdc}(a, m) = 1.$$

Mostre que $\text{mdc}(a, m \cdot n) = 1$.

Solução 13.14

Como $\text{mdc}(a, n) = 1$ assim

$$a \cdot x_1 + n \cdot y_1 = 1$$

para alguns x_1, y_1. Semelhante

$$a \cdot x_2 + m \cdot y_2 = 1,$$

para alguns x_2, y_2. Agora:

$$\begin{aligned} 1 = a \cdot x_1 + n \cdot y_1 &= a \cdot x_1 + 1 \cdot n \cdot y_1 \\ &= a \cdot x_1 + (a \cdot x_2 + m \cdot y_2) \cdot ny_1 \\ &= ax_1 + ax_2 \cdot n \cdot y_1 + mnay_1y_2 \\ &= a \cdot (x_1 + x_2ny_1) + m \cdot (ny_1y_2) = 1. \end{aligned}$$

Logo,

$$a \cdot x' + m \cdot n \cdot y' = 1,$$

e $\text{mdc}(a, mn) = 1$.

Exercício 13.15

Suponha que $a + b = c^2$, mostre que

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

Solução 13.15

Sejam

$$d = \text{mdc}(a, c) \qquad e = \text{mdc}(b, c)$$

Mostremos que $d|e$ e $e|d$.

Como $d \mid a$ e $d \mid c$ assim $\quad d \mid c^2$, e $d \mid (c^2 - a)$, mas $c^2 - a = b$, logo $d \mid b$. Agora

$$\begin{cases} d \mid b \\ d \mid c \end{cases} \Rightarrow d \mid e$$

Semelhante, Como $e \mid b$ e $e \mid c$ assim $\quad e \mid c^2$, e $e \mid (c^2 - b)$, mas $c^2 - b = a$, logo $e \mid a$. Agora

$$\begin{cases} e \mid a \\ e \mid c \end{cases} \Rightarrow e \mid d$$

Assim $d = e$.

Exercício 13.16

Seja $\text{mdc}(a, b) = p$ um primo. O que pode ser dito $\text{mdc}\left(a^2, b\right)$ e $\text{mdc}\left(a^2, b^2\right)$?

Solução 13.16

Como $\text{mdc}(a, b) = p$ assim, aplicando T.de Bezout temos que

$$a \cdot r + b \cdot s = p,$$

para algum r, s inteiros. Levando ambos os lados ao quadrado, temos

$$\begin{aligned} a^2 \cdot r^2 + 2a \cdot r \cdot b \cdot b + b^2 \cdot s^2 &= a^2 \cdot r^2 + b\left(2a \cdot r \cdot s + bs^2\right) \\ &= p^2. \end{aligned}$$

Assim $\text{mdc}\left(a^2, b\right) \mid p^2$, por outro lado $\text{mdc}(a, b) \mid \text{mdc}\left(a^2, b\right)$ ou seja $p \mid \text{mdc}\left(a^2, b\right)$ assim $\text{mdc}\left(a^2, b\right) = p$ ou $\text{mdc}\left(a^2, b\right) = p^2$, e ambas possibilidade possíveis, pois se, por exemplo, $a = p$, $b = p$, assim

$$\text{mdc}(a^2, b) = \text{mdc}(p^2, p) = p.$$

Por outro lado, se $a = p$ e $b = p^2$, assim

$$\text{mdc}(a^2, b) = \text{mdc}(p^2, p^2) = p^2.$$