

LIBRA DE EXERCÍCIO 3

NOME: GABRIEL ALMEIDA MENDES

PNE: 352204959

③ TEOREMA: SEJA $m > m \in \mathbb{Z}_+^*$. SE $m|n = r$, ENTÃO $2^m - 1 | 2^n - 1$.

PROVA:

SE $n = mq + r$ e $0 \leq r < m$, QUEREMOS

$$2^m - 1 = (2^m - 1)q + 2^n - 1 \wedge 0 \leq 2^n - 1 < 2^m - 1.$$

SE ESTAS EQUAÇÕES SE SATISFAZEM ENTÃO O RESTO É $2^n - 1$ POR CAUSA DA UNICIDADE DO RESTO DA DIVISÃO, DEVIDO AO FATO QUE:

$0 \leq r < m$, ENTÃO $2^0 \leq 2^n < 2^m$ DONDE SE CONCLUI QUE $0 \leq 2^n - 1 < 2^m - 1$. TAMBÉM.

④ a) SENDO $2^{2^m+1} - 1 = (2^{2^m} + 1)(2^{2^m} - 1)$, MOSTRE QUE $2^{2^m} - 1$ É MÚLTIPLO DE $2^{2^m} + 1$ QUANDO $m > m$. QUEM O QUOCIENTE?

PROVA: SENDO MÚLTIPLOS ENTRE SI ENTÃO SUA DIVISÃO É INTEIRA COM RESTO 0. EXISTE INTEIRO q TAL QUE $b = q \cdot q_1$.

$$\text{OU } q = \frac{b}{a} \text{ ENTRE } q = \frac{b}{a} \text{ ENTÃO } \downarrow$$

ENTÃO $\frac{2^{2^m} - 1}{2^{2^m} + 1}$ DA RESTO 0, JÁ QUE PELA

PRA UNICIDADE DO QUOCIENTE DO RESTO,
 $\frac{2^m}{2^{m+1}}$ DA RESTO 0 TAMBÉM. ASSIM EXISTE q TAL QUE:

$$b = aq$$

$$2^{2^m} - 1 = (2^{2^m+1} - 1)Q$$

$$Q = \frac{2^{2^m} - 1}{(2^{2^m} + 1)(2^{2^m} - 1)} = \frac{1}{2^{2^m} + 1} = Q$$

→ AQUI PROVA QUE $2^{2^m} - 1$ E $2^{2^m} + 1$ SÃO
MULTIPLO PORQUE ELES SÃO DIVISIVEIS

OBSS: OS CÍRCULOS USADOS AQUI FORAM MUITO
LÓGICOS MAS SE NÉCESSARIO POSSO ENVIA-LOS.

⑥ ENCONTRE TODOS OS INTEIROS POSITIVOS
M TAIIS QUE $2m^2 + 1 | m^3 + 9m - 57$

RESUMÃO: REDUZINDO O DENOMINADOR DE $m^3 + 9m - 57$
UTILIZANDO $2m^2 + 1$ COM O LEMA DE EUCLIDES

$$2m^2 + 1 | (m^3 + 9m - 57)2$$

$$2m^2 + 1 | 2m^3 + 18m - 114 - m(2m^2 + 1)$$

$$2m^2 + 1 | 2m^3 + 18m - 114 - 2m^3 - m$$

$$2m^2 + 1 | 17m - 114$$

↓

COMO $2m^2 + 1 > 17m - 34$ ENTÃO PODEMOS
PEGAR UMA LISTA FINITA PARA N, ASSIM:

$$17m - 34 = 0$$

$$m = \frac{34}{17} \rightarrow m = 2$$

$$|2m^2 + 1| \leq |17m - 34|$$

$$\Delta = -17^2 - 4 \cdot 2 \cdot 35$$

$$\Delta = 289 - 280 = 9$$

$$2m^2 + 1 \leq 17m - 34$$

$$m_1 = \frac{17+3}{2 \cdot 2} = \frac{20}{4} = 5$$

$$2m^2 - 17m + 35 \leq 0$$

$$m_2 = \frac{17-3}{4} = \frac{14}{4} = \frac{7}{2}$$

A PENAS 2 E 5 SÃO SOLUÇÕES.

- ② a) PROVA: TOMANDO OS NÚMEROS COMO a E b É O PRODUTO ENTRE ELES AB. PELA PROPRIEDADE DA DIVISIBILIDADE $m/a \wedge m/b \rightarrow m/(a \cdot b)$, OU SEJA O RESTO DA DIVISÃO DE UM PRODUTO DE DOIS INTEIROS POR UM NÚMERO M É O MESMO QUE O RESTO DE CADA NÚMERO DIVIDIDO INDIVIDUALMENTE POR M.
NESSE CASO: $(a \% 7 = 7) \wedge (b \% 7 = 7) \Rightarrow ((a \cdot b) \% 7 = 7)$

(11)

a) SEJAM $a, b \in \mathbb{C}$ INTEIROS.

SE $\frac{a}{2x-3y} \in \frac{a}{4x-5y}$, ENTÃO $\frac{a}{y}$.

PROVA: SUPONDO QUE a/y SEJAM q, r INTEIROS
TAIS QUE $y = a \cdot q + r$.

QUEREMOS q INTEIRO TAL QUE $x - y = a \cdot q$.

MAS $x - y = aq_x - aq_y = a(q_x - q_y)$ SERÁ

LOGO $q = q_x = q_y$.

PELA UNICIDADE DO RESTO E DO QUOCIENTE

$$Q_1 = \frac{a}{2x-3y} = q = \frac{a}{4x-5y} = Q_2 \text{ ENTÃO}$$

$$q = Q_1 = Q_2.$$

b) SEJAM $a, b \in \mathbb{C}$ INTEIROS.

SE $\frac{b}{ac}$, ENTÃO $\frac{b}{c}$

PROVA: SUPONDO b/c SEJAM q, r INTEIROS.

TAL QUE $c = b \cdot q + r$, e $a = b \cdot q_a$

LOGO: $ac = b \cdot q_a \cdot b \cdot q$

$$ac = (b \cdot q) \cdot b$$

* SENO INTG 170

c) SEJA a UM INTEIRO

SE $a^2 - 2a + 7$ É PAR, ENTÃO a É IMPAR.

PROVA: PELA CONTA POSITIVA SE a É PAR ENTÃO $a^2 - 2a + 7$ É IMPAR, COM a INTEIRO. SUPONHAMOS a Ú PAR, ENTÃO $a = 2k$. VAMOS ANALISAR $a^2 - 2a + 7$:

$$a^2 - 2a + 7 =$$

$$(2k)^2 - 2(2k) + 7 =$$

$$4k^2 - 4k + 7 =$$

$$\underbrace{2(2k^2 - k)}_{2q} + 7 =$$

$$2q + 7 \rightarrow q = 2k^2 - k$$

ENTÃO $a^2 - 2a + 7$ É IMPAR

(3) c) SE a/b é RACIAL, ENTÃO a/c

PROVA: PELA DEFINIÇÃO DE TRANSITIVIDADE,

SE a/b , EXISTE $k \in \mathbb{Z}$ ($k \neq 0$) TAL QUE $b = ak$.

POR VERSE RACIAL, EXISTE $y \in \mathbb{Z} \setminus \{0\}$ TAL QUE $b = by$.

ENTÃO TENDO: $b = ak$ E $c = by$ TEMOS

$c = a \cdot k \cdot y$, OU a/c TENDO $K, Y \in \mathbb{Z}$ $\begin{cases} K \neq 0 \\ Y \neq 0 \end{cases}$

EM OUTRAS PALAVRAS, SIM a/c .

o) Se $a|b$ e $a|c$, então $a|(bx+cy)$,

QUAISQUER QUE SEJAM OS INTEIROS x, y .

Prova: Por hipótese $b = aq_1$ e $c = aq_2$.

ENTÃO $b \cdot x = (a \cdot q_1) \cdot x$ e $c \cdot y = (a \cdot q_2) \cdot y$, ou

$bx = a(x \cdot q_1)$ e $cy = a(y \cdot q_2)$.

Agora somamos $bx + cy$ que é

$a(x \cdot q_1) + a(y \cdot q_2) = a(x \cdot q_1 + y \cdot q_2)$, então

$bx + cy = a(x \cdot q_1 + y \cdot q_2)$.

Como $bx + cy$ é múltiplo de a , determinamos
que $a | bx + cy$.

l) Se $a|b$ e $b|a$, então $a = b$

Prova: Para $a|b$ existe q_1 que $b = aq_1$ e
Para $b|a$ existe q_2 que $a = b \cdot q_2$.

SUSTITUIMOS $b = aq_1$ em $a = b \cdot q_2$ FICANDO

$a = a \cdot q_1 \cdot q_2$, Sendo que $a \neq 0$ e $a = a$,

O PRODUTO DE q_1 E q_2 SÓ PODE SER 1.

DESSÉ MODO, $q_1 = q_2 = 1$ E POR TANTO, $a = b$.

f) se $a \leq b$;

Prova: Para $a \leq b$ existe q que $b = a \cdot q$,
TENDO QUE $q \in \mathbb{Z}$ e $q \geq 1$. Se para a se querer
que ele precise ser multiplicado por q .
Então é porque $a \leq b$.

g) Se $c = \phi$, então: $a \mid b$ se $a \mid bc$
(o que acontece no caso $c = 0$?).

Prova: Essa ai bugou a cabeça não?

⑯ b) $\text{mdc}(a, ca) = a$

Prova:

LISANDO UMA LISTA FINITA DE DIVISORES
EM COMUM PARA a E ca E \mathbb{Z} QUERIA CON-

$$D(a) = \{a\}$$

$$D(ca) = \{a, ca\}$$

AMOS TEM UM DIVISOR COMUM QUE É a .
ENTÃO SE CONFIRMA A PROPRIEDADE.