Ficha 2 - EPTN

12. Sejam a e b inteiros não simultaneamente nulos. Mostre que:

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

    (b) Se $\text{m.d.c.}(a,b) = d$, então $\text{m.d.c.}(\frac{a}{d},\frac{b}{d}) = 1$.

12)

a) Basta notar que os divisores de a e $-a$ são os mesmos, assim como os divisores de b e $-b$. Logo, o m.d.c também vai ser comum.

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

$\Leftrightarrow \frac{a}{d}x + \frac{b}{d}y = 1 \Rightarrow m.d.c(\frac{a}{d}, \frac{b}{d}) = 1$

13. Verifique que, dados um inteiro positivo n e um inteiro a, $\text{m.d.c.}(a, a+n)$ divide n.
    Conclua que dois inteiros consecutivos são primos entre si.

a) Sabemos que, seja $d = m.d.c(a, a+n)$, $d \mid a \wedge d \mid a+n$ e

$d \mid ax + (a+n)y$ então,

seja $x = -1$ e $y = 1$, $d \mid -a + a + n \Leftrightarrow d \mid n$ c.q.m

b) n e $n+1$ são primos entre si, ou seja, $m.d.c(n, n+1) = 1$

$n+1 \,\underline{|\ n\quad}$ quociente 1, resto $\textcircled{1}$; $\quad n \,\underline{|\ 1\quad}$ resto 0

então, $m.d.c(n, n+1) = 1$

14. Sejam $a, b \in \mathbb{Z}$ tais que $\text{m.d.c.}(a,4) = \text{m.d.c.}(b,4) = 2$. Mostre que $\text{m.d.c.}(a+b,4) = 4$. ⟷ Máximo divisor comum!

14)

Temos de primeiro ter em conta que $2y \mid 4$, para todo y que seja par.

Como $m.d.c(a,4) = 2$ e $m.d.c(b,4) = 2$

$\downarrow$ $2 \mid a$ mas $4 \nmid a$ $\to$ $2x = a$ $\to$ da forma $2n+1$

$\downarrow$ $2 \mid b$ e $4 \nmid b$ $\to$ $2m = b$ → m é da forma $2k+1$

$a + b = 2(x + y) = 2(2n + 1 + 2k + 1) = 2 \times 2(n + k + 1) = 4(n+k+1)$

então, $m.d.c(a+b, 4) = m.d.c(4(n+k+1), 4) = 4$

$4 \leq 4(n+k+1)$ c.q.m.

15. Mostre que se k é um inteiro positivo, então $\underbrace{3k+2 \text{ e } 5k+3 \text{ são números primos entre}}$ si.

$\downarrow$

$m.d.c(3k+2, 5k+3) = 1$

Seja $d = m.d.c(3k+2, 5k+3)$,

$d \mid 3k+2$ e $d \mid 5k+3 \Rightarrow d \mid (3k+2)x + (5k+3)y$, $x, y \in \mathbb{Z}$

$d = (3k+2)x + (5k+3)y$, se $x = 5$ e $y = -3$,

$d = 15k + 10 - 15k - 9 = 1$, ou seja, $m.d.c(3k+2, 5k+3) = 1$, pois existem x e y inteiros que tornam a equação $1 = (3k+2)x + (5k+3)y$ possível

16. Sejam a e b números inteiros. Mostre que se x e y são inteiros tais que $ax + by =$ m.d.c.(a, b), então m.d.c.$(x, y) = 1$.

$m.d.c(a, b) = d$

16) $ax + by = d \Leftrightarrow$

$\Leftrightarrow \frac{a}{d}x + \frac{b}{d}y = 1 \longrightarrow$ ou seja, $m.d.c(x, y) = 1$, pois existem inteiros $\frac{a}{d}$ e $\frac{b}{d}$ que tornam a equação possível.

ⓘ $\Rightarrow$ ⓘⓘ

17. Mostre que m.d.c.$(a, b) = 1 =$ m.d.c.(a, c) se e só se m.d.c.$(a, bc) = 1$.

$i \Rightarrow ii$

$$\begin{cases} 1 = ax + by \\ 1 = am + ct \end{cases} \Leftrightarrow 1 \times 1 = (ax + by) \times (am + ct) \Leftrightarrow$$

$\Leftrightarrow 1 = ax \times am + ax \times ct + am \times by + by \times ct \Leftrightarrow$

$\Leftrightarrow a^2(xm + xt + my) + bc(t\, y) = 1$, logo,

como existem $\mathbb{Z}$ que tornam a equação possível, então, $m.d.c(a, bc) = 1$

18. 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) $a = 1001$, $b = 33$.

$m.d.c(1001, 357) = 7$

18. 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) $a = -2860,\ b = -2310.$

18)

a) 1001 | 357 → 287, 2   357 | 287 → 70, 1   287 | 70 → 7, 4   70 | 7 → $\boxed{0}$, 10

m.d.c (1001, 357) = 7

b) 1001 | 33 → 11, 30   33 | 11 → 0, 3   m.d.c(1001, 33) = 11

c) 126 | 56 → 14, 2   56 | 14 → 0, 4   m.d.c(56, 126) = 14

d) 1386 | 90 → 36, 15   90 | 36 → 18, 2   36 | 18 → 0, 2   m.d.c (1386, -90) = 18

e) 2860 | 2310 → 750, 1   2310 | 750 → 60, 3   750 | 60 → 30, 12   60 | $\boxed{30}$ → 0, 2

m.d.c (-2860, - 2310) = 30

19. Determine, usando o Algoritmo de Euclides, inteiros x e y que satisfaçam:

(a) $\text{m.d.c.}(56, 72) = 56x + 72y$; → 16
(b) $\text{m.d.c.}(24, 138) = 24x + 138y.$

56 = 16×3 + 8

16 = 2 × 8

19) a) 72 | 56 → 16, 1   56 | 16 → 8, 3   16 | 8 → 2

16 = 72 - 56

$8 = 56 - 16\times3 = 56 - (72-56)\times3 = 56\times\underline{4} - 72\times\underline{3}$

x = 4
y = -3

b) 138 | 24 → 18, 5   24 | 18 → 6, 1   18 | 6 → 0, 3

$6 = 24 - 18 = 24 - (138 - 24\times5) =$
$= 24\times6 - 138\times1$ x = 6
y = -1

20. Determine o menor inteiro positivo k da forma $\underbrace{k = 22x + 55y,}$ onde x e y são inteiros.

m.d.c = $\boxed{11}$

21. Prove que

(a) todo o primo da forma $3n + 1$ é da forma $6m + 1$ $(m, n \in \mathbb{N})$;
(b) o único primo da forma $n^3 - 1$ é o 7 $(n \in \mathbb{N})$;
[Sugestão: Escreva $n^3 - 1$ como $(n - 1)(n^2 + n + 1)$.]
(c) todo o inteiro da forma $n^4 + 4$, em que $n > 1$, é composto.

21)

a) Seja p um primo qualquer da forma $\underline{3n+1}$, e $\underline{6m+1}$

Tem resto 1 na divisão por 3.   resto 1 por 6

p ≥ 7, pq n e m são naturais

{não pode ser 2, 3, 5 pq aí m ou n teriam de ser negativos}

1) $6m$ ✗

2) $6m+1 \longrightarrow$ única alternativa que sobra.

3) $6m+2$ ✗ $\longrightarrow 2(3m+1)$

4) $6m+3$ ✗ $\longrightarrow 3(2m+1)$

5) $6m+4$ ✗ $\longrightarrow 2(3m+2)$

6) $6m+5 \longrightarrow 6m+3+2 \longrightarrow 3(2m+1)+2$

↳ como tem resto 2, não pode ser

b) $n^3-1 \longrightarrow$ único primo é 7.

$$n^3-1 = \overset{\geq 0}{(n-1)}\,\overset{>1}{(n^2+n+1)}$$

para $n=1$, $(1-1)(3)=0$ não é primo

$n=2 \quad 8-1=7$

para $n>2$, $\underset{>1}{(n-1)}\,\underset{>1}{(n^2+n+1)} \longrightarrow$ ou seja, este nº será exprimido por nºs primos e não primos, ou seja, será divisível pelos mesmos, então, não será primo.

c.q.d.

c) n^4+4 é composto para todo $n>1$

$$(n^2+2)^2 - 4n^2 = n^4+4 \iff$$

$$\iff (n^2+2-2n)(n^2+2+2n) = n^4+4$$

Ou seja, terá n^2-2n+2 e n^2+2n+2 como divisores, então, será composto e não primo.

22. Usando a fatorização de 507 e 1287 em fatores primos, determine m.d.c.(507, 1287) e m.m.c.(507, 1287).

$$\begin{array}{r|l} 507 & 3 \\ 169 & 13 \\ 13 & 13 \\ 1 & \end{array} \quad = 13^2 \times 3 \quad = 13 \times 39$$

$$\begin{array}{r|l} 1287 & 3 \\ 429 & 3 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array} \quad = 3^2 \times 11 \times 13 = 3 \times 11 \times 39$$

m.d.c = 39

$$m \cdot \text{——} \cdot c = \frac{507 \times 1287}{m \cdot m \cdot c} = \frac{13 \times \cancel{39} \times 3 \times 11 \times 39}{\cancel{39}} =$$

$$= 39 \times 39 \times 11 = 1521 \times 11 = 1521 + 15210 =$$

$$= 16731$$

23. Verifique que 701 é um número primo, testando todos os primos $p \leq \sqrt{701}$ como possíveis divisores.

$$26 < \sqrt{701} < 27$$

Ver se 2, 3, 5, 7, 11, 13, 17, 19 e 23 são divisores de 701

24) comprova-se por contradição. (Supomos que p é primo tal que $\sqrt{p}$ é natural/racional → vamos chegar a um absurdo que nos diz que p tem mais divisores além de 1 e p.)

25. Mostre que há uma infinidade de primos da forma $6n + 5$.

Vamos supor que há uma finidade de primos da forma 6n+5

$$p_1 < p_2 < \ldots < p_n$$

Seja $N = 6\, p_1 \times p_2 \times p_3 \times \ldots \times p_n + 5$ → ao dividirmos N por p_i, $i \in \{1, \ldots, n\}$, obtemos sempre resto 5.

$N > p_n$, N é o composto.

De acordo com o Teorema Fundamental da Aritmética, todo nº é escrito pelo produto de primos e potências de primos.

Como N não pode ser escrito da forma de produto de primos da forma 6n+5, só nos restam primos da forma 6n+1 ($\overline{pq}$ se for com os outros restos da divisão de 6, obtemos um nº composto). Porém, entramos outra vez numa contradição, $\overline{pq}$ N, quando dividido por 6, deixa resto 5 e não 1.

$$(6k+1)(6n+1)(6q+1)\ldots = \underbrace{6k(6n+1)(6q+1)}_{\downarrow} + \underbrace{(6n+1)(6q+1)}_{\downarrow}\ldots =$$

O produto vai ser da forma 6m+1, logo, entramos

O produto vai ser da forma 6n+1, logo, entramos numa contradição. Ou seja, obrigatoriamente, há uma infinidade de primos da forma 6n+3. ^w^