Monitoria:

Nas monitorias passadas: exs 4, 6, 7, 9, 10, 11, 12, 14 16, 21, 22, 23, 24.

—//—

TFA: Seja a um inteiro diferente de 0, 1 e -1. Então, existem primos positivos $p_1 < p_2 < \dots < p_r$ e inteiros positivos $n_1, \dots, n_r$ tais que $a = E\, p_1^{n_1} \dots p_r^{n_r}$, em que $E = \pm 1$ conforme a seja positivo ou negativo. Além disso essa decomposição é única.

Lema 2.6.10 (pág 83): Seja $a = p_1^{n_1} \cdots p_t^{n_t}$ e $d = p_1^{m_1} \cdots p_t^{m_t}$ inteiros positivos, onde $p_1, \ldots, p_t$ são primos positivos e n_i, m_i, $1 \leq i \leq t$ são inteiros não negativos. Então, $d \mid a \iff m_i \leq n_i$ $1 \leq i \leq t$.

Teorema: Sejam $a = p_1^{n_1} \cdots p_t^{n_t}$ e $b = p_1^{m_1} \cdots p_t^{m_t}$ inteiros nas condições do lema 2.6.10. Então $d = mdc(a,b) = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ em $\alpha_i = \min(n_i, m_i)$, $1 \leq i \leq t$

$$m = mmc(a,b) = p_1^{\beta_1} \cdots p_t^{\beta_t}, \quad \beta_i = \max\{n_i, m_i\}$$

$1 \le i \le t$

— // —

Ex: $a = 2^2 \cdot 3^4 \cdot 5^2$ / $b = 2^1 \cdot 3^7 \cdot 5^0$

$$\begin{cases} mdc(a,b) = 2^1 \cdot 3^4 \\ mmc(a,b) = 2^2 \cdot 3^7 \cdot 5^2 \end{cases}$$

Prop 2.6.12 (pg 85)

Seja $a = p_1^{n_1} \cdots p_t^{n_t}$ a decomp de $a > 1$ nas condições do T.F.A. Então o número de divisores positivos de a é:

$$n(a) = (n_1 + 1) \cdots (n_t + 1)$$

Dem:

Temos que $a = p_1^{n_1} \cdots p_t^{n_t}$ e pelo lema 2.6.10, um divisor de a é da forma

$$x = p_1^{\alpha_1} \cdots p_t^{\alpha_t}, \quad 0 \leq \alpha_i \leq n_i, \quad 1 \leq i \leq t$$

$x = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, $0 \le \alpha_i \le n_i$, $1 \le i \le t$.

$p_i^{\alpha_i} \in \{p_i^0, p_i^1, \ldots, p_i^{n_i}\}$. Repare,

$|\{p_i^0, \ldots, p_i^{n_i}\}| = (n_i + 1)$. Então,

temos que $n(a) = (n_1 + 1) \cdots (n_t + 1)$.

□

(...)

Ex 4 (pág 94): Demonstrar que existem infinitos primos da forma $3n+2$, $n \in \mathbb{Z}$

Dem:

Note que $\forall \in \mathbb{N}$ pode ser escrito como

$\forall = 3n + r$, $r \in \{0, 1, 2\}$. $\underline{3n}$, $3n+1$, $3n+2$

Veja que um primo ou é 3, ou é de uma das seguintes formas: $3n+1$ ou $3n+2$

Vamos supor que existe uma quantidade finita de primos da forma $3n+2$, são eles,

$\{p_1 = 2, p_2, \dots, p_k\}$

Considere $N = 3p_2 \cdots p_k + 2$.

Note que se $2 \mid N$, então $2 \mid 3p_2 \cdots p_k$ ($3n$ ($n=1$)), e, como $mdc(2,3) = 1$, pelo teo. euclides $2 \mid p_2 \cdots p_k \Rightarrow$ $2 \mid p_i$ (porque?), absurdo.

Suponha que $p_i \mid N$, como $p_i \mid 3p_2 \cdots p_k$ temos que $p_i \mid 2$, contradição pois $p_i \neq 2$ ($2 \leq i \leq k$)

Assim, concluímos que nenhum dos primos da forma $3n+2$ divide N. Então na decomp. de N ainda podem aparecem primos da forma $3n+1$

ou aparece 3 (pode aparecer ambos).

Repare que $3 \nmid N$. Caso $3 \mid N$ como

$3 \mid 3 p_2 \cdots p_k$ então $3 \mid 2$ (contradição)

Com isso, 3 não aparece na decomp. de N

em fatores primos. Logo, N deve ser um produto

de primos da forma $3n+1$.

Considere $S = \{ 3n+1 : n \in \mathbb{Z} \}$. veja que

S é fechado para multiplicação. De fato,

$$(3n+1)(3l+1) = 9nl + 3n + 3l + 1 = 3(3nl + n + l) + 1 \in S.$$

Assim, chegamos a uma contradição pois

N deveria ser da forma $3n+1$, mas

por construção ele é da forma $3n+2$

→ Lista de Revisão:

(17) Se $a|b$ e $mdc(b,c)=1 \Rightarrow mdc(a,c)=1$

Dem: Seja $d = mdc(a,c) \Rightarrow d|a$ e $d|c$.

Como $a|b$, segue que $d|b$. Logo,

$d \mid mdc(b,c)=1 \Rightarrow d=1$. ∎

(ii) $mdc(a,c) = mdc(b,c)=1 \Leftrightarrow mdc(ab,c)=1$

Dem

($\Leftarrow$) Seja $d = mdc(a,c) \Rightarrow d|a$ e $d|c \Rightarrow$

$d|ab$ e $d|c \Rightarrow d \mid mdc(ab,c)=1 \Rightarrow d=1$

($\Rightarrow$) Agora considere $mdc(a, c) = mdc(b, c) = 1$

Seja $d = mdc(ab, c) \Rightarrow d \mid ab$ e $d \mid c$. Vamos mostrar que $mdc(d, b) = x = 1$. Temos que $x \mid d$ e $x \mid b$. Como $d \mid c \Rightarrow x \mid c$. Daí,

$x \mid c$ e $x \mid b \Rightarrow x \mid mdc(c, b) = 1 \Rightarrow x = 1$.

Feito isso, temos que $d \mid ab$ e $mdc(d, b) = 1$ então, pelo teo. de Euclides, $d \mid a$. Assim, $d \mid a$, $d \mid c \Rightarrow d \mid mdc(a, c) = 1 \Rightarrow d = 1$ ∎

Ex 18 $\left[\begin{array}{l} d \mid (a+b)^2 \text{ e } d \mid (a+b)^2 - ab \Rightarrow \\ d \mid (a+b)^2 - [(a+b)^2 - ab] = ab \end{array}\right]$

(i) $mdc(a+b, a^2+ab+b^2) = 1$

Dem: Seja $d = mdc(a+b, a^2+ab+b^2) \Rightarrow$

$d \mid a+b$, $d \mid (a+b)^2 - ab \Rightarrow d \mid (a+b)^2$ e

$d \mid (a+b)^2 - ab \Rightarrow d \mid ab$. Vou mostrar

que $mdc(d, b) = x = 1$. Temos $x \mid d$, $x \mid b$.

Como $d \mid a+b \Rightarrow x \mid (a+b)$. Usando que

$x \mid a+b$ e $x \mid b \Rightarrow x \mid a$. Logo $x \mid mdc(a,b) = 1$.

Portanto, $x = 1$.

Assim, obtemos que $d \mid ab$ e $mdc(d, b) = 1$,

logo, pelo teo. de Euclides, $d \mid a$.

Desse modo, $d \mid \underbrace{a+b \text{ e } d \mid a}_{} \Rightarrow d \mid b$ e,

portanto, $d \mid mdc(a, b) = 1 \Rightarrow d = 1$.

obs/ $d \mid a+b$ e $d \mid a \Rightarrow d \mid (a+b) - a = b$

(ii) $mdc(a+b, a^2 - ab + b^2) = 1$ ou 3

Dem: Seja $d = mdc(a+b, a^2 - ab + b^2) \Rightarrow$

$d | (a+b)$ e $d | (a+b)^2 - 3ab \Rightarrow$

$d | 3ab$. Seja $x = mdc(d, b) \Rightarrow x | d$ e $x | b$.

Como $d | (a+b) \Rightarrow x | (a+b)$. Daí, usando

$x | (a+b)$ e $x | b \Rightarrow x | a$. Logo $x | mdc(a, b) = 1 \Rightarrow$

$x = 1$.

Agora, de posse do fato de que $d | 3ab$ e $mdc(d, b) = 1$, usando o T.E, $d | 3a$.

Agora, precisamos mostrar $mdc(d, a) = x = 1$.

Assim, $x \mid d$ e $x \mid a$. Como $d \mid a+b$, segue que $x \mid a+b$. Daqui usando que $x \mid a$, vem que $x \mid b$. Com isso, $x \mid a$ e $x \mid b \Rightarrow x \mid mdc(a, b) = 1 \Rightarrow x = 1$.

Portanto, temos que $d \mid 3a$ e $mdc(d, a) = 1$, daí pelo T. E, $d \mid 3 \Rightarrow d = 1$ ou 3

Ex 28) (ii) $97 \mid 2^{48} - 1$

Dem:

obs: Seja $d \neq 0$ um divisor próprio de $a > 0$

Então, $a = d \cdot c$, $c > 1$. Observe que se $d, c > \sqrt{a}$ então $dc > \sqrt{a}\sqrt{a} = a$, contradição.

Então, se a não possui um divisor menor ou igual a $\sqrt{a}$ (diferente de ± 1), a deve ser um primo.

$\sqrt{97} < \sqrt{100} = 10$. Daí, concluímos que 97 é primo.

Agora veja que

$$2^{48} - 1 = (2^{24})^2 - 1^2 = (2^{24} - 1)(2^{24} + 1) =$$

$$((2^{12})^2 - 1^2)(2^{24} + 1) = (2^{12} - 1)(2^{12} + 1)(2^{24} + 1)$$

Note que $97 \mid 2^{48} - 1 \iff 97 \mid (2^{12} - 1)$ ou $97 \mid (2^{12} + 1)$ ou $97 \mid (2^{24} + 1)$.

$2^{12} = 4096$. "É fácil ver que",

$97 \mid (2^{12}-1)$ e $97 \mid (2^{12}+1)$. Daí,

$$97 \mid 2^{48}-1 \iff 97 \mid 2^{24}+1$$

Precisamos mostrar que $2^{24} \equiv -1 \pmod{97}$.

Veja que $2^{12} \equiv 22 \pmod{97}$ (faça as contas :))

Logo $(2^{12})^2 \equiv (22)^2 \pmod{97} \Rightarrow 2^{24} \equiv 484 \pmod{97}$

e $484 \equiv 96 \equiv -1 \pmod{97}$ ∎

(obs: Nesse ex precisamos fazer contas mesmo)

13)

(viii) $mdc(-a, b) = mdc(a, -b) = mdc(a, b)$

Dem: Sejam $d = mdc(-a, b)$, $d' = mdc(a, -b)$ e $d'' = mdc(a, b)$. A ideia é mostrar que $d = d'$ e $d' = d''$.

Como $d \mid (-a)$ e $d \mid b \Rightarrow d \mid a$ e $d \mid (-b)$.

(*) Logo $\underline{d \mid d'}$. Analogamente, como $d' \mid a$ e $d' \mid (-b) \Rightarrow d' \mid (-a)$ e $d' \mid b \Rightarrow \underline{d' \mid d}$.

Comissão $d = d'$.

Analogamente, prova-se que $d = d''$

(*)

Seja $d = mdc(a,b) \Rightarrow \exists\, r, s \in \mathbb{Z}$ tq $ar + bs = d$. Seja d' um divisor de a e b, então $d' | a$ e $d' | b \Rightarrow d' | ar + bs = d$.

□

(ii) Dica: mostre que p/ $mdc(mdc(a,b),c) = x$ $x | a, b, c$ e use (*). Além disso, mostre que para $mdc(a, mdc(b,c)) = y$, $y | a, b$ e c e use (*)