TEORIA DOS NÚMEROS

Conceitos básicos:

① Sejam a e b dois inteiros dizemos que a divide b ou b é múltiplo de a se existe um inteiro m tal que $m \cdot a = b$.

- notação: $a|b$ → divisor
- notação: $a \nmid b$ → não divisor

a → menor sempre (é o divisor)

Teoremas:

a) se $a|b$ e $a|c$, então $a|(b+c)$

* Prova direta:

1. Se $a|b \Rightarrow a \cdot k_1 = b$, $k_1 \in \mathbb{Z}$ (1)
2. $\wedge$ $a|c \Rightarrow a \cdot k_2 = c$ (2)
3. $a \cdot k_1 + a \cdot k_2 = b + c$ (1)+(2)
4. $a(k_1 + k_2) = b + c$, logo $a|(b+c)$ //

($k_1 + k_2 \rightarrow k$)

b) Se $a|b$ então $a|bk$, para qualquer inteiro k //

c) Se $a|b$ e $b|c$ então $a|c$ //

Teorema (algoritmo da divisão)

$a \mid b \rightarrow$ div. Seja um inteiro $b \neq 0$,

r → resto; q → quociente. existem inteiros únicos q e r, de forma que $a = b \cdot q + r$

$r < b$ (resto vai de 0 até b-1) //

algoritmo: $a = b \cdot q + r$

O resto é único!!!

Módulo (mod)

* definição: Sejam a e b inteiros positivos. Nós denotamos a mod b como o resto quando a é dividido por m //.

- exemplo: 15 mod 12 = 3 mod 12 = 3

operador %

* notação: conjunto de divisores de a

$D(a) = \{n \in \mathbb{Z}, n|a\}$ ex:

$D_+(a)$ = divisores positivos

$D_-(a)$ = divisores negativos

* definição (maior divisor comum)

Sejam a e b inteiros, de forma que apenas um deles pode ser 0. O maior inteiro d do conjunto $D(a) \cap D(b)$ é o MDC de a e b. Denotado por mdc(a,b).

* Primos entre si, se mdc(a,b) = 1 //

primos: não podem ser escritos como o produto de 2 inteiros positivos menores do que ele.

só é divisível por 1 e ele mesmo //.

TESTE DE PRIMALIDADE

Teorema fundamental da Aritmética

→ Todo inteiro positivo pode ser escrito como um produto de primos e essa fatoração é única a menos da ordem dos primos.

TFA //

TEOREMA FUNDAMENTAL DA ARTMÉTICA

exemplo: prove que $\sqrt{2}$ é irracional.

-> por contradicção:

1. Supomos $\sqrt{2}$ racional.

2. De (1) temos: $\sqrt{2} = a/b$

3. De (2) temos $2b^2 = a^2$

* usar quantidade de vezes que 2 aparece na fatoração prima de a e b para chegar em uma contradição.

exemplo: prove que se p é um primo, a e b são inteiros e $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$ ou ambos.

$p = p$ ocorre na fatoração prima de $a \cdot b$, logo, ele deve ocorrer na F. p de a ou de b ou de ambos.