ALGORITMO DE EUCLIDES

- calcula o mdc de dois inteiros de modo eficiente, sem precisar encontrar suas fatorações primas.
* ele é baseado em 2 proposições que podemos provar:

① Prove que $mdc(a,b) = mdc(a,b-a)$

② Seja r o resto se dividimos B por A, então prove que $mdc(a,b) = mdc(a,r)$

① Prova:

$\underbrace{mdc(a,b)}_{X} = \underbrace{mdc(a,b-a)}_{Y}$

então, queremos provar que $X = Y$.

- primeira parte: provar que $X \leq Y$

1. $X = mdc(a,b) \rightarrow X|a \wedge X|b$
2. Se $X|a$, $X|-a$.
3. Se $X|-a \wedge X|b$, $X|b+(-a) \rightarrow X|b-a$
4. temos que $X|a$ e $X|(b-a)$
5. Se $Y = mdc(a,b-a)$, $Y|a \wedge Y|(b-a)$ → maior
6. Logo, $X \leq Y$.

- segunda parte da prova: $Y \leq X$

1. $Y = mdc(a,b-a)$, $Y|a \wedge Y|b-a$
2. Se (1), $Y|a+(+b-a) \rightarrow Y|b$
3. temos que $Y|a \wedge Y|b$, porém x é o maior divisor. Logo:
4. $Y \leq X$

Juntando 1- com 2-, temos que $X = Y$ //

② prova: Seja r o resto se dividirmos b por a, então $mdc(a,b) = mdc(a,r)$.

- quero provar que: $mdc(a,b) = mdc(a, b-a\cdot q)$ pois $b = aq + r$.
↳ aplicar o teorema provado em (1)

1. $mdc(a,b) = mdc(a, \underbrace{b-a}_{Y})$
2. $mdc(a,b-a) = mdc(a,b-a-a)$
3. $mdc(a,b-2a) = mdc(a,b-3a)$

⋮ depois de n vezes:

4. $mdc(a,b-q\cdot a)$, $q \in \mathbb{Z}$.

- Como funciona o algoritmo?
- quero achar o mdc entre a e b
1- dividir o maior ~~e mei~~ pelo menor;
2- pegar o resto;
3- dividir pelo resto ; (acaba com a=0)

exemplos:

a) $mdc(300,18)$

1- $\frac{300}{18} = \frac{50}{3}$ (resto 12) → (12, 18)

2- $\frac{18}{12}$ ⇒ resto 6 → (12, 6)

3- $\frac{12}{6}$ → resto → (0, 6) → mdc:

$mdc(300,18) = 6$

Teorema: identidade de Bezout:
→ dados inteiros a e b, não nulos, existem inteiros m e n, tais que:

$a\cdot m + b\cdot n = mdc(a,b)$

Ou seja, o mdc de a e b pode ser escrito como uma combinação linear com coeficientes a e b.

IDENTIDADE DE BEZOUT

$$a \cdot m + b \cdot n = mdc(a,b)$$

exemplo: sabemos que $mdc(300,18) = 6$,

Sabemos que podemos achar m e n

$$300 \cdot m + 18 \cdot n = 6$$

* por exemplo:

$$300 \cdot (-1) + 18 \cdot 17 = 6$$

Será que essa solução é única?

-> como achar m e n?

usando o algoritmo DE EUCLIDES!