NUMBER THEORY

NOTAÇÃO

* N: Inteiro positivo
* p: Primo

ARITMÉTICA MODULAR

$$\begin{array}{r|l} 17 & 12 \\ -12 & 1 \\ \boxed{5} & \end{array}$$

Exemplo: $N = 12$

17 mod 12

$9 + 8 = 5$ em $\mathbb{Z}_{12}$

$5 \times 7 = 11$ em $\mathbb{Z}_{12}$

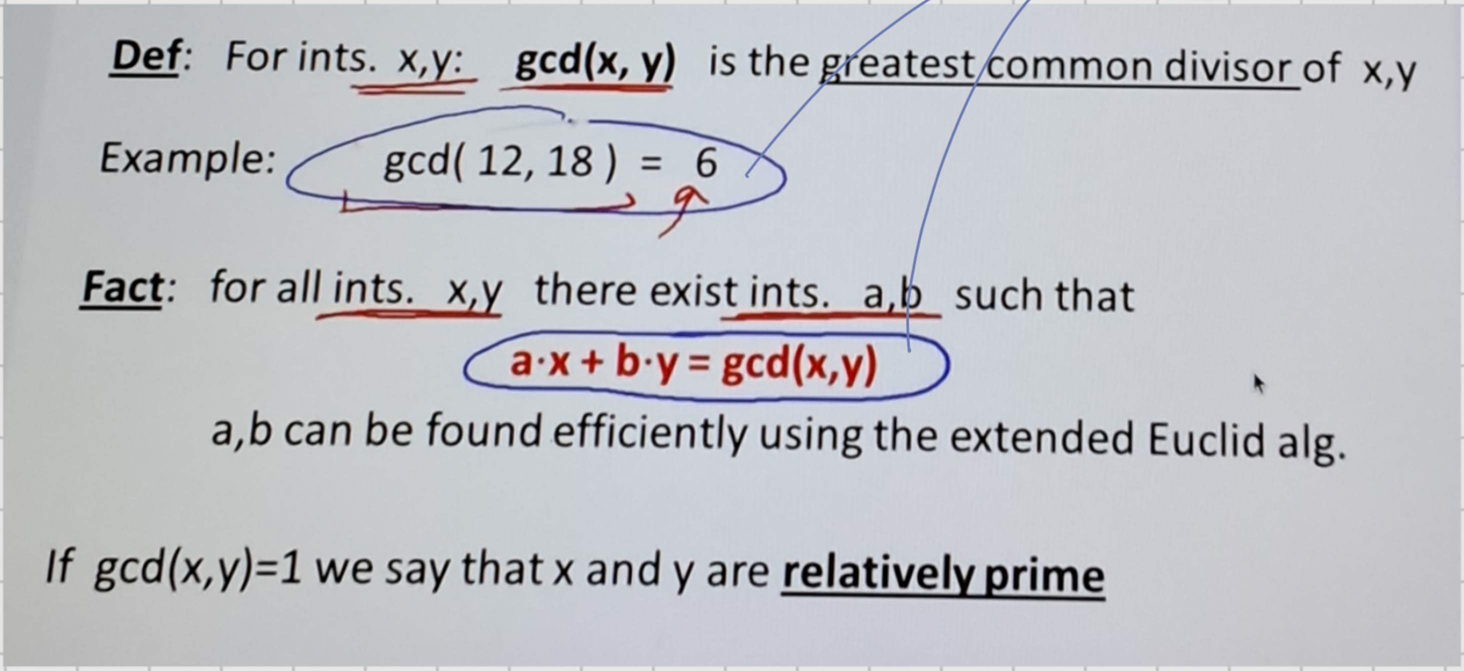
$5 - 7 = 10$ em $\mathbb{Z}_{12}$

* Resultado padrão dividido por N o resultado será o resto.

MAIOR DIVISOR COMUM

↪ gcd

$2.12 - 1.18 = 6$



Def: For ints. x,y: **gcd(x, y)** is the greatest common divisor of x,y

Example: gcd(12, 18) = 6

Fact: for all ints. x,y there exist ints. a,b such that

a·x + b·y = gcd(x,y)

a,b can be found efficiently using the extended Euclid alg.

If gcd(x,y)=1 we say that x and y are **relatively prime**