Funzione di Eulero : $\varphi(N) = |\mathbb{Z}_N^*|$

↓

$\varphi(N)$ = quanti $n \in \mathbb{Z}_N$ co-primi con N
$n < N$

Sia p primo :

- $\varphi(p) = p-1$
- $\varphi(p^2) = p(p-1)$
- $\varphi(p^e) = p^{e-1}(p-1)$

$e \in \mathbb{N}$ esponente qualunque

Se $n, m \in \mathbb{Z}_{>1}$ e $MCD(n,m) = 1$ ovvero co-primi

$\Rightarrow$ $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Se N non primo , lo scompongo in prodotto di numeri primi

$N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ $e_i \in \mathbb{N}$

$$\Longrightarrow \boxed{\varphi(N) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)}$$ IN GENERALE

Congruenze

$a x \equiv b \mod N$

incognita $x \in \mathbb{Z}$

calcolare $ax \equiv b \mod N$ significa calcolare $ax - kN = b$
equazione diofantina

Come si risolve :

1) $\exists$ soluzione $\Longleftrightarrow$ $MCD(a,N) \mid b$

$\Rightarrow$ calcolo MCD con algoritmo di Eulero

2) risolvo l'identità di Bézout $1 = A \cdot a - B \cdot b$

3) trovo $x \equiv$ rappresentante canonico mod N