# EULERO

$$\mathbb{Z}_N^\times = \{[a]_N \mid \exists [b]_N \in \mathbb{Z}_N \text{ t.c. } [a]_N[b]_N = [1]_N\} =$$
$$= \{[a]_N \mid \mathrm{MCD}(a,N) = 1\} =$$
$$= \{[a]_N \mid \langle [a]_N \rangle = \mathbb{Z}_N\}$$

$\varphi(N) = |\mathbb{Z}_N^\times|$ funzione di Eulero

- Se $N = p$ primo $\Longrightarrow$ $\varphi(N) = p-1$
- Se $N = p^2$

$\cancel{\overline{0}}, \overline{1}, \dots, \cancel{\overline{p}}, \overline{p+1}, \dots, \cancel{\overline{2p}}, \dots, \cancel{\overline{(p-1)p}}, \overline{p^2-1}$ in $\mathbb{Z}_{p^2}$

scartiamo i multipli di $p$

$|\mathbb{Z}_{p^2}^\times| = p^2 - \underbrace{p}_{\text{multipli di } p} = p(p-1)$ $\qquad$ $\varphi(p^2) = p(p-1)$

- Se $N = p^e$, $e$ = elemento neutrale qualsiasi

$\overline{0}, \overline{1}, \dots, \overline{p}, \overline{p+1}, \dots, \overline{(p^{e-1}-1)p}, \dots, \overline{p^e-1}$

multipli di $\overline{p}$ : $\overline{p^{e-1}}$

non multipli di $\overline{p}$ : $\overline{p^e - p^{e-1}}$

$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ se $p$ e' primo

Esempio $\quad \varphi(64) = \varphi(2^6) = 2^5(2-1) = 2^5 = 32$

$\varphi(81) = \varphi(3^4) = 3^3(3-1) = 27 \cdot 2 = 54$

Proposizione

Se $n,m \in \mathbb{Z}_{>1}$ e $\mathrm{MCD}(m,n) = 1$

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

Dimostrazione

Abbiamo provato che se $\mathrm{MCD}(m,n) = 1$ allora

$\theta : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ e' un isomorfismo

$[a]_{mn} \longmapsto ([a]_m, [a]_n)$

$\Theta$ è anche un isomorfismo di monoidi rispetto alla moltiplicazione.

$\Theta$ si restringe ad una biezione:

$$\mathbb{Z}^{\times}_{mn} \longrightarrow (\mathbb{Z}_m \times \mathbb{Z}_n)^{\times} = \mathbb{Z}^{\times}_m \times \mathbb{Z}^{\times}_n$$

$$\Longrightarrow |\mathbb{Z}^{\times}_{mn}| = |\mathbb{Z}^{\times}_m| \cdot |\mathbb{Z}^{\times}_n|$$

$$= \varphi(nm) = \varphi(m)\varphi(n)$$

per fare tutto ciò, n e m devono essere co-primi

## Corollario

Se $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ $\quad p_i$ primi distinti

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}) = \boxed{\prod_{i=1}^{k}} p_i^{e_i - 1}(p_i - 1)$$

produttoria

FORMULA GENERALE PER CALCOLARE $\varphi(N)$

## Esercizio $\quad \varphi(59825) = ?$

$59825 = 3^2 \cdot 5 \cdot 11^3$

$\varphi(3^2) = 3(3-1) = 6$

$\varphi(5) = 5 - 1 = 4$

$\varphi(11^3) = 11^2(11-1) = 121 \cdot 10 = 1210$

$\Longrightarrow \varphi(5925) = 6 \cdot 4 \cdot 1210 = 29040$

## Esercizio $\quad N = 3^5 \cdot 7^{12} \cdot 11$

$\varphi(N) = 3^4 \cdot (3-1) \cdot 7^{11} \cdot (7-1) \cdot (11-1) = \underline{\underline{\text{CALCOLATELO}}}$

IMPORTANTE

$\varphi(nm) = \varphi(m)\varphi(n)$ vale $\iff$ m e n sono co-primi

Esempio $4 = 2 \cdot 2$ $\varphi(4) = 2$ $\varphi(2) = 1$

$\varphi(4) \neq \varphi(2)\varphi(2)$ !

**CONGRUENZE** = equazioni della forma $\underline{ax \equiv b}$ mod N

Risolvere la congruenza = trovare tutte le $x \in \mathbb{Z}$ che soddisfano

## Esempi

$5x \equiv 2 \mod 3$

$[5]_3 [x]_3 = [2]_3$

$\|$

$[2]_3 [x]_3 = [2]_3$ $\quad$ $[2]_3$ e' invertibile

rappresent. canonico

$[x]_3 = [1]_3 \implies x \equiv 1 \mod 3$

$\implies x \in \{1 + 3k \mid k \in \mathbb{Z}\}$ o $x \in [1]_3$ (non e' una singola soluzione !)

$ax \equiv b \mod N$ significa $ax - b = kN$, $k \in \mathbb{Z}$

$\underbrace{ax - kN = b}_{\text{equazione diofantina}}$

ha soluzione $\iff$ MCD$(a, N)$ divide b

in questo caso possiamo determinare x con Bézout

# Esempi

- $5x \equiv 4 \mod 22$

  ha soluzione $\Leftrightarrow$ $\underbrace{MCD(5, 22)}_{1} \mid 4$

  - Calcolo MCD(5,22) con Euclide :
  $$22 = 5 \cdot 4 + 2$$
  $$5 = 2 \cdot 2 + 1$$
  $$2 = 1 \cdot 2$$

  - Bézout : $1 = 5 - 2 \cdot 2 = 5 \cdot 2(22 - 5 \cdot 4)$
  $$= 9 \cdot 5 - 2 \cdot 22$$
  $$\Longrightarrow 5 \cdot 9 - 22 \cdot 2 = 1$$

  $$5 \cdot \underbrace{36} - 22 \cdot 8 = 4$$

  per trovare il rappresent. canonico

  $$\Longrightarrow 5 \cdot 36 \equiv 4 \mod 22$$
  $$5 \cdot 14 \equiv 4 \mod 22 \quad \Longrightarrow \quad \boxed{x \equiv 14 \mod 22}$$

- $6x \equiv 15 \mod 26$

  ha soluzione $\Leftrightarrow$ $\underbrace{MCD(6, 26)}_{=2 \nmid 15} \mid 15$

  NON C'È SOLUZIONE perché $2 \nmid 15$

- $9x \equiv 12 \mod 51$

  $MCD(9, 51) \mid 12$ ?

  $MCD(9, 51) = 3 \Longrightarrow$ c'è soluzione

  $\rightarrow$ cerco k t.c. $9x - 51k = 12$ $\rightarrow$ tutti divisibili per 3
  $$3x - 17k = 4$$

  $\rightarrow$ MCD(3,17)?
  $$17 = 3 \cdot 5 + 2$$
  $$3 = 2 \cdot 1 + 1$$
  $$2 = 1 \cdot 2$$
  $$\Longrightarrow MCD(\underbrace{3, 17}_{\text{co-primi}}) = 1$$

  $\rightarrow$ Bézout : $1 = 3 - 2 \cdot 1 = 3 - (17 - 3 \cdot 5) = 3 \cdot 6 - 17$

  $$\Rightarrow 3 \cdot 6 - 17 \cdot 1 = 1 \quad \Rightarrow 3 \cdot (6 \cdot 4) - 17 \cdot 4 = 4$$
  $$\Rightarrow 3 \cdot 24 - 17 \cdot 4 = 4$$

  $$\Longrightarrow x \equiv 24 \mod 17$$

$\Rightarrow x \equiv 7 \mod 17$

$x \equiv 7, 24, \underbrace{41}_{24+17}, \underbrace{(41+17)}_{\text{mod } 7} \mod 51$

## Esercizio

a) Determinare l'inverso di $\overline{72}$ in $\mathbb{Z}_{125}$

b) Elencare le soluzioni in $\mathbb{Z}_{68}$ di $12x \equiv 8 \mod 68$

c) Dire quali sono le classi $\overline{x} \in \mathbb{Z}_{11}$ t.c. $\overline{5}^k = \overline{x}$ con $k \in \mathbb{N}$

(b) $MCD(12, 68) = 4 \mid 8 \Rightarrow \exists$ soluzione

$12x - 68k = 8$

$\hookrightarrow 3x - 17k = 2$ (cerco soluzione in mod 17)

$17 = 3 \cdot 5 + 2$

$3 = 2 + 1$ $\qquad 1 = 3 - 2 = 3 - (17 - 3 \cdot 5) = 3 \cdot 6 - 17$

$\Rightarrow 18 - 17 = 1$

$\Rightarrow 3 \cdot 12 - 17 \cdot 2 = 2$

trovo che $x \equiv 12 \mod 17 \Rightarrow$ $x \equiv 12, 29, 46, 63 \mod 68$

Ma in $\mathbb{Z}_{68}$ le soluzioni sono: $[12]_{68}, [29]_{68},$
$[46]_{68}, [63]_{68}$