

Abbiamo visto che un elemento  $[a]_m$  in  $\mathbb{Z}_m$  con

$[a]_m \neq [0]_m$  si dice invertibile se esiste

$[b]_m$  in  $\mathbb{Z}_m$  con  $[a]_m \cdot [b]_m = [1]_m = [b]_m \cdot [a]_m$

Inoltre per  $m > 1$  abbiamo due  $[a]_m$  e'

invertibile & e solo se  $(a, m) = 1$ . Supponiamo

anche come si trova l'inverso di  $[a]_m$ : dalla

identità di Bezout ricaviamo  $s, t \in \mathbb{Z}$  con

$$as + tm = 1$$

e pertanto

$$[a]_m^{-1} = [s]_m$$

FUNZIONE DI EULERO

$$\varphi: \mathbb{N}^* \rightarrow \mathbb{N}^*$$

$$\varphi(1) = 1$$

$$\varphi(m) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq m-1 \text{ e } (m, k) = 1\}|$$

per  $m > 1$

ESEMPIO

$$m=6 \quad \varphi(6) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq 5 \text{ e } (k, 6) = 1\}|$$

$$= |\{1, 5\}| = 2$$

# PROPRIETA' DELLA FUNZIONE DI EULERO

1. Se  $p$  è un numero primo allora

$$\varphi(p) = p - 1$$

2. se  $p$  è un numero primo e  $m \in \mathbb{N}^*$  allora

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

$$= p^{m-1}(p-1)$$

prova

$$\varphi(p^m) = |\{k \in \mathbb{N}^+ \mid 1 \leq k \leq p^m\} \setminus \{k, p^m\}| = |\{k \in \mathbb{N}^+ \mid 1 \leq k \leq p^m\}| - |\{k, p^m\}|$$

$$= p^m - p$$

$$= p^{m-1}(p-1)$$

$$= p^{m-1}(p-1)$$

$$\{1, 2, \dots, p^m\} \setminus \{p, 2p, \dots, p^{m-1} \cdot p\}$$

3. La funzione di Eulero è molt. plicativa cioè

se  $m, n \in \mathbb{N}^*$  con  $\text{C.M.D.}(m, n) = 1$  allora

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

Dalle proprietà 1, 2, e 3. segue che possiamo calcolare  $\varphi(n)$  per un qualsiasi  $n \in \mathbb{N}^*$ . Infatti se

$$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$$

con  $p_i \neq p_j$   $i \neq j$  e  $p_i$  primo per  $i = 1, \dots, t$

allora

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}) = \varphi(p_1^{e_1}) \varphi(p_2^{e_2}) \dots \varphi(p_t^{e_t}) \\ &= p_1^{e_1-1} p_2^{e_2-1} \dots p_t^{e_t-1} (p_1-1) \dots (p_t-1) \quad \boxed{2}\end{aligned}$$

ESEMPIO  $m=12 = 2^2 \cdot 3$  dunque

$$\begin{aligned}\varphi(12) &= \varphi(2^2 \cdot 3) = \varphi(2^2) \cdot \varphi(3) \\ &= 2^{2-1} \cdot (2-1) \cdot (3-1) = 4\end{aligned}$$

OSSERVAZIONE

Per  $n > 1$ ,  $\varphi(n)$  è uguale al numero di invertibili in  $\mathbb{Z}_n$ .

TEOREMA DI EULERO

Siano  $a \in \mathbb{Z}$  e  $m \in \mathbb{N}^+$  con  $m > 1$  e  $(a, m) = 1$ .

Allora

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

(ovvero  $[a]_m^{\varphi(m)} = [1]_m$ ).

Dim.

Fatti: 1) se  $a, b, c \in \mathbb{Z}$  allora  $(ab, c) = 1$  se e solo se

$$(a, c) = 1 \text{ e } (b, c) = 1$$

2)  $a, b, c \in \mathbb{Z}$   $\wedge$   $a|bc$  e  $(a, b) = 1$  allora  
 $a|c$ .

3) se  $[a]_m \in [b]_m$  suo elementi invertibili

in  $Z_n$  allora anche  $[a]_n [b]_n = [ab]_n$   
 è invertibile infatti  $(a, n) = 1 = (b, n)$  con  
 $(ab, n) = 1$ . L'inverso di  $[a]_n \cdot [b]_n$  è  
 $[a]_n^{-1} \cdot [b]_n^{-1}$ .

$$5) [a]_n^m = \underbrace{[a]_n \cdot [a]_n \cdot \dots \cdot [a]_n}_m = [a^m]_n$$

per  $m \geq 0$ .

Sia  $A_m = \{k \in \mathbb{N} \mid 1 \leq k \leq m-1 \text{ e } (m, k) = 1\}$ .

Diciamo che  $|A_m| = r$  e scriviamo

$$A_m = \{k_1, k_2, \dots, k_r\}$$

cost  $\varphi(m) = |A_m| = r$ . Considero gli insiemi

$$X = \{[k_1]_m, [k_2]_m, \dots, [k_r]_m\}$$

$$e \quad Y = \{[ak_1]_m, [ak_2]_m, \dots, [ak_r]_m\}$$

Vogliamo far vedere che  $X = Y$ . Supponiamo di averlo provato allora

$$[k_1]_m [k_2]_m \dots [k_r]_m = [ak_1]_m [ak_2]_m \dots [ak_r]_m$$

da cui

[3]

$$[k_1 k_2 \dots k_r]_m = [a^r k_1 k_2 \dots k_r]_m$$

ovvero

$$[k_1 k_2 \dots k_r]_m = [a]_m^r [k_1 k_2 \dots k_r]_r$$

Per il fatto 3) se indichiamo con  $[c]_m^r = [k_1 \dots k_r]_m$  abbiamo che  $[c]_m^r$  è invertibile in  $\mathbb{Z}_m$ .

Moltiplico l'ultima uguaglianza per  $[c]_m^{-1}$  e trovo

$$[a]_m^r = [1]_m$$

ovvero

$$a^r \equiv 1 \pmod{m}, \text{ dove } r = \varphi(m).$$

Devo far vedere che  $X = Y$ . Ora  $X$  è l'insieme di tutti e soli gli elementi invertibili in  $\mathbb{Z}_m$ .

Considero  $[a k_1]_m$ . Siccome  $(a, m) = 1$  e  $(k_1, m) = 1$  risulta  $(a k_1, m) = 1$ . Dunque  $[a k_1]_m$  è un elemento invertibile in  $\mathbb{Z}_m$ . Lo stesso è vero per gli altri elementi di  $Y$  cioè  $Y \subseteq X$ .

Poi non può essere  $[a k_1]_m = [a k_2]_m$  perché se fosse avrei  $a k_1 \equiv a k_2 \pmod{m}$  cioè  $m \mid a(k_1 - k_2)$ . Ità  $(a, m) = 1$  cioè  $m \mid k_1 - k_2$ , ovvero  $[k_1]_m = [k_2]_m$ , un assurdo.

Con lo stesso argomento si mostra che non può essere  $[a k_i]_m = [a k_j]_m$  per  $i \neq j$ .

Quindi  $Y \subseteq X$  e  $|Y| = r = |X|$  da cui  $Y = X$ .  $\square$