IL TEOREMA DI FERMAT-EULERO

DEF. 13.1 DEFINIAMO LA FUNZIONE $\phi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}$, detta FUNZIONE "phi" di EULERO, ponendo

$$\phi(n) := \underbrace{\left|\{a \in \mathbb{Z} \mid 1 \le a \le n, (a,n)=1\}\right|}_{\text{cardinalità}}$$

= "numero di interi a compresi tra 1 e n inclusi che sono coprimi con n"

$\forall n \in \mathbb{N} \setminus \{0\}$.

OSSERVAZIONE 13.2

(1) $\phi(1) = |\{a \in \mathbb{Z} \mid 1 \le a \le 1, (a,1)=1\}| = |\{1\}| = 1$, $\phi(2) = |\{1\}| = 1$, $\phi(4) = |\{1, \cancel{2}, 3, \cancel{4}\}| = |\{1,3\}| = 2$, $\phi(8) = |\{1,3,5,7\}| = 4$

(2) È VERO CHE ϕ È MOLTIPLICATIVA? $\phi(nm) = \phi(n)\phi(m)$ $\forall n,m \in \mathbb{N}\setminus\{0\}$

NO, infatti se $n=2$ e $m=4 \Rightarrow \phi(2\cdot 4) = \phi(8) = 4$; $\phi(2)\phi(4) = 1 \cdot 2$

(3) La funzione $\phi : \mathbb{N}\setminus\{0\} \longrightarrow \mathbb{N}$ è MOLTIPLICATIVA SULLE COPPIE COPRIME, ovvero

$$\phi(n\cdot m) = \phi(n)\,\phi(m) \qquad \forall\, n,m \in \mathbb{N}\setminus\{0\} \text{ t.c. } (n,m)=1. \qquad (*0)$$

Ciò può essere dimostrato usando il teorema cinese del resto (DIMOSTRAZIONE OMESSA)

SCHEMI, ALGEBRETTA,

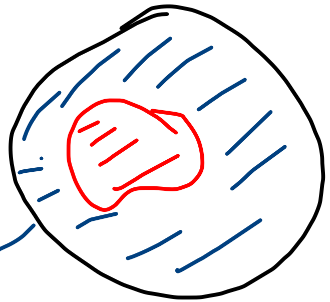
(4) Sia p un numero primo e sia $m \in \mathbb{N}\setminus\{0\}$. Considero $n = p^m$.

Calcoliamo $\phi(n) = \phi(p^m)$. Vale:

$$\phi(p^m) = \left|\{a\in\mathbb{Z} \mid 1\le a\le p^m,\ (a,p^m)=1\}\right| =$$
$$= \left|\{a\in\mathbb{Z} \mid 1\le a\le p^m,\ (a,p)=1\}\right| =$$
$$= \left|\{1,2,\dots,p^m\} \setminus \{a\in\mathbb{Z} \mid 1\le a\le p^m,\ (a,p)\neq 1\}\right| =$$

$$= \left| \{1, 2, \dots, p^m\} \setminus \{1 \cdot p, 2 \cdot p, 3 \cdot p, \dots, p^{m-1} \cdot p\} \right| =$$

$$= \left| \{1, 2, \dots, p^m\} \right| - \left| \underbrace{\{1 \cdot p, 2 \cdot p, 3 \cdot p, \dots, p^{m-1} \cdot p\}} \right| =$$



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

$$\Rightarrow \boxed{\phi(p^m) = p^m - p^{m-1} \qquad \forall p \text{ primo e } \forall m \in \mathbb{N} \setminus \{0\}} \quad (*)$$

$$\Rightarrow \phi(p) = p^1 - p^0 = p - 1$$

$$\Updownarrow$$

$$\boxed{\phi(p) = p - 1 \qquad \forall p \text{ primo}} \quad (*')$$

ESERCIZIO Calcolare:

- $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$
- $\phi(81) = \phi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$

- $\phi(7) \underset{(*')}{=} 7 - 1 = 6$; $\overset{(*)}{=} 7^1 - 7^0 = 7 - 1 = 6$
- $\phi(19) = 19 - 1 = 18$

- $\phi(36) = \cancel{\phi(6^2) = 6^2 - 6^1}$? ?

  $\phi(36) = \phi(2^2 \cdot 3^2) =$

$$\boxed{= \phi(2^2)\,\phi(3^2) \overset{(*)}{=} \\ = (2^2 - 2^1)(3^2 - 3^1) = \\ = 2 \cdot 6 = 12} \quad (*0)$$

(5) FORMULA GENERALE $(\phi(1)=1)$

Sia $n \geq 2$ e sia $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ per qualche numero primo $p_1, \dots, p_k$ con $p_i \neq p_j \ \forall i \neq j$, e $m_1, \dots, m_k \in \mathbb{N} \setminus \{0\}$

Allora

$$\phi(n) = \phi(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) \overset{(*0)}{=} \phi(p_1^{m_1})\,\phi(p_2^{m_2}) \cdots \phi(p_k^{m_k}) \overset{(*1)}{=}$$

$$= (p_1^{m_1} - p_1^{m_1-1})(p_2^{m_2} - p_2^{m_2-1}) \cdots (p_k^{m_k} - p_k^{m_k-1})$$

$$\Rightarrow \boxed{\phi(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) = (p_1^{m_1} - p_1^{m_1-1})(p_2^{m_2} - p_2^{m_2-1}) \cdots (p_k^{m_k} - p_k^{m_k-1}).} \quad (*2)$$

ESERCIZIO Calcolare:

- $\phi(24) = \phi(2^3 \cdot 3) = \phi(2^3)\,\phi(3) = (2^3 - 2^2)(3-1) = (8-4) \cdot 2 = 4 \cdot 2 = 8,$
- $\phi(21) \cancel{=} 21 - 1 \rightsquigarrow \phi(21) = \phi(3 \cdot 7) = \phi(3)\,\phi(7) = (3-1)(7-1) = 2 \cdot 6 = 12.$
- $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\,\phi(5^2) = (2^2 - 2^1)(5^2 - 5^1) = 2 \cdot 20 = 40.$ $\blacksquare$

Lemma 13.3 (Prop. 13.8 sulle dispense)

Dato $n>0$, vale:

$$\underbrace{\left|(\mathbb{Z}/n\mathbb{Z})^*\right|}_{\text{"cardinalità dell'insieme degli interi modulo } n \text{ invertibile"} \,=\, \text{"numero degli interi modulo } n \text{ invertibili"}} = \underline{\phi(n)}.$$

DIM. Grazie alla Prop. 12.5 (volta scorsa e dispense),

$$\left|(\mathbb{Z}/n\mathbb{Z})^*\right| = \left|\{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid 0 \le a \le n-1,\ (a,n)=1\}\right| =$$

$[0]_n = [n]_n$

$$= \left|\{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid 1 \le a \le n,\ (a,n)=1\}\right| =$$

$$= \left|\{a \in \mathbb{Z} \mid 1 \le a \le n,\ (a,n)=1\}\right| = \phi(n) \qquad \boxed{}$$

la definizione di "phi" di Eulero

Lemma 13.4 Dati $\alpha, \beta \in (\mathbb{Z}/n\mathbb{Z})^*$, valgono:

$n > 0$

(1) $\alpha\beta \in (\mathbb{Z}/n\mathbb{Z})^*$, $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$;

(2) $\alpha^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$, $(\alpha^{-1})^{-1} = \alpha$.

DIM. (1) $(\alpha\beta)(\beta^{-1}\alpha^{-1}) = \alpha(\beta\beta^{-1})\alpha^{-1} = (\alpha\,[1]_n)\alpha^{-1} = \alpha\alpha^{-1} = [1]_n$

$\Rightarrow \alpha\beta \in (\mathbb{Z}/n\mathbb{Z})^*$ e $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} = \alpha^{-1}\beta^{-1}$.

(2) Vale: $\alpha(\alpha^{-1}) = [1]_n \Rightarrow \alpha^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$ e $(\alpha^{-1})^{-1} = \alpha$. $\square$

TEOREMA 13.5 (TEOREMA DI FERMAT – EULERO, TEOREMA 13.9 sulle dispense)

Sia $n > 0$. Per ogni $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$, vale:

$$\alpha^{\phi(n)} = [1]_n \quad \text{in } \mathbb{Z}/n\mathbb{Z}. \qquad (*3)$$

Equivalentemente, per ogni $a \in \mathbb{Z}$ t.c. $(a, n) = 1$,

$$a^{\phi(n)} \equiv 1 \pmod{n}. \qquad (*4)$$

Dim. Sia $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Consideriamo la seguente funzione

$$L_\alpha : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*, \text{ ovvero } L_\alpha(\beta) := \alpha\beta \quad \forall \beta \in (\mathbb{Z}/n\mathbb{Z})^*.$$

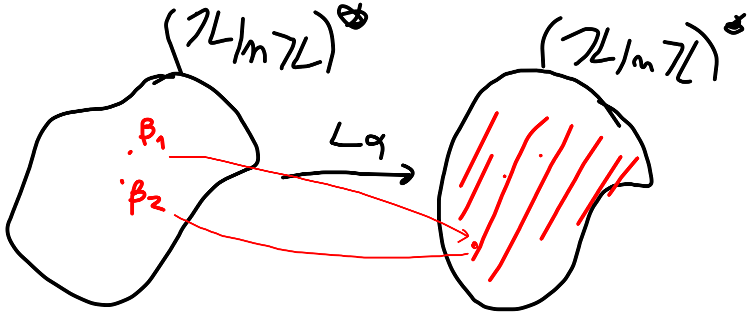
$$\beta \longmapsto \alpha\beta$$

OSSERVIAMO CHE L_α È BEN-DEFINITA grazie al precedente Lemma 13.4 (1).
Se riusciamo a provare che L_α è iniettiva, allora L_α sarà anche bigettiva in

quindi $(\mathbb{Z}/n\mathbb{Z})^{\otimes}$ è un insieme finito che coincide sia col dominio che con il codominio di L_α.

Proviamo che L_α è iniettiva. Siano $\beta_1, \beta_2 \in (\mathbb{Z}/n\mathbb{Z})^{\otimes}$

t.c. $L_\alpha(\beta_1) = L_\alpha(\beta_2)$. Dobbiamo provare che $\beta_1 = \beta_2$.



L_α iniettiva $\Rightarrow$ L_α surgettiva (bigettiva)

Vale:

$$L_\alpha(\beta_1) = L_\alpha(\beta_2) \iff \alpha\beta_1 = \alpha\beta_2$$

$$\Downarrow$$

$$\alpha^{-1}\alpha\beta_1 = \alpha^{-1}\alpha\beta_2$$

$$\Updownarrow$$

$$\beta_1 = [1]_n\beta_1 = [1]_n\beta_2 = \beta_2$$

$$\Updownarrow$$

$$\beta_1 = \beta_2$$

$\Rightarrow$ L_α è iniettiva $\Rightarrow$ L_α è bigettiva.

Segue che, se $k := \phi(n)$ e $(\mathbb{Z}/n\mathbb{Z})^* \overset{\text{Lemma 13.3 prec.}}{=} \{\beta_1, \beta_2, \dots, \beta_k\}$, allora

$L_\alpha(\beta_1), L_\alpha(\beta_2), \dots, L_\alpha(\beta_k)$ sono ancora tutti e soli gli elementi $\beta_1, \dots, \beta_k$ di $(\mathbb{Z}/n\mathbb{Z})^*$ eventualmente riordinati.

Poiché la moltiplicazione in $\mathbb{Z}/n\mathbb{Z}$ (e quindi anche in $(\mathbb{Z}/n\mathbb{Z})^*$) è associativa e commutativa, vale:

$$\begin{aligned}\beta_1 \cdots \beta_k &= L_\alpha(\beta_1) L_\alpha(\beta_2) \cdots L_\alpha(\beta_k) \quad \text{in } (\mathbb{Z}/n\mathbb{Z})^* \\ &= \alpha\beta_1 \alpha\beta_2 \cdots \alpha\beta_k \\ &= \alpha^k \beta_1 \beta_2 \cdots \beta_k\end{aligned}$$

$$\Updownarrow$$

$$\underline{\beta_1 \cdots \beta_k = \alpha^k \beta_1 \cdots \beta_k} \quad \text{in } (\mathbb{Z}/n\mathbb{Z})^*$$

Grazie al Lemma 13.4(1), $\gamma := \beta_1 \cdots \beta_k \in (\mathbb{Z}/n\mathbb{Z})^*$, $\Rightarrow \gamma = \alpha^k \gamma \Rightarrow \overbrace{\gamma^{-1}\gamma}^{[1]_n} = \overbrace{\alpha^k \gamma \gamma^{-1}}^{\alpha^k}$ (*3) ✓

Se $a \in \mathbb{Z}$ con $(a, m) = 1$, allora $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^*$ e $(\circledast 3)$ implica:

$$\begin{rcases} [a]_m^{\phi(m)} = \underline{[1]_m} \\ \shortparallel \\ \underline{[a^{\phi(m)}]_m} \end{rcases} \Leftrightarrow a^{\phi(m)} \equiv 1 \pmod{m} \quad (\circledast 4).$$

Corollario 13.6 (PICCOLO TEOREMA DI FERMAT)

Se p è un numero primo e $a \in \mathbb{Z}$ t.c. $p \nmid a$ (ovvero $(p, a) = 1$), allora

$$(\circledast 4) \text{ con } n = p \Rightarrow \underline{a^{p-1} \equiv 1 \pmod{p}.}$$

<u>Es.</u> $p = 7$, $a = 10$, $7 \nmid 10$

$$a^{p-1} = 10^6 \equiv 1 \pmod{7}$$
$$\Updownarrow$$
$$7 \mid 10^6 - 1 = 999999$$