φ di Eulero

Note Title 10/12/2017

(PEOPLE.DM.UNIPI.IT/LOMBARDO)

DEF Sia n un intero >0. Si pone

$$\varphi(n) = \#\left\{ k \in \mathbb{N} \text{ t.c. } \begin{matrix} 1 \le k \le n \\ (k,n)=1 \end{matrix} \right\}$$

Esempi $\varphi(4) = 2$

1 ~~2~~ 3 ~~4~~

$\varphi(12) = 4$

1 ~~2~~ 3 ~~4~~ 5 ~~6~~

7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~

$= 12 - 6 - 4 + 2$

$$\varphi(p^k) = p^k - \#\left\{ m \quad \begin{matrix} 1 \le m \le p^k \\ (m, p^k) > 1 \end{matrix} \right\}$$

$$= p^k - \#\left\{ m \quad \begin{matrix} 1 \le m \le p^k \\ p \mid m \end{matrix} \right\}$$

$$= p^k - \frac{1}{p} \cdot p^k = p^{k-1}(p-1)$$

$$= p^k \cdot \left(1 - \frac{1}{p}\right)$$

$$\varphi(p^a q^b) = p^a q^b - \frac{1}{p} p^a q^b - \frac{1}{q} p^a q^b + \frac{1}{pq} p^a q^b$$

$a, b \ge 1$

principio di INCLUSIONE-ESCLUSIONE

$$= p^a q^b \left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right)$$

$$= p^a q^b \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$$

$$\varphi(\underbrace{p_1^{e_1} p_2^{e_2} p_3^{e_3}}_{n}) = p_1^{e_1} p_2^{e_2} p_3^{e_3} \left(1 - \frac{1}{p_1}\right)\left(1 - 1/p_2\right)\left(1 - 1/p_3\right)$$

$$A_{p_1} = \{m \quad 1 \le m \le n,\ p_1 \mid m\}$$

$$A_{p_2} = \{m \quad 1 \le m \le n,\ p_2 \mid m\}$$

p_1, p_2 primi distinti

$$A_{p_1 p_2} = \{m \quad 1 \le m \le n,\ p_1 p_2 \mid m\} = A_{p_1} \cap A_{p_2}$$

$$A_{p_1 p_2 p_3} = \{m \quad 1 \le m \le n,\ p_1 p_2 p_3 \mid m\} = A_{p_1} \cap A_{p_2} \cap A_{p_3}$$

$$|A_{p_1}| = n/p_1$$

$$|A_{p_2}| = n/p_2$$

$$|A_{p_3}| = n/p_3$$

$$|A_{p_1 p_2}| = \frac{n}{p_1 p_2}$$

$$|A_{p_1 p_2 p_3}| = \frac{n}{p_1 p_2 p_3}$$

$$\varphi(n) = n - |A_{p_1} \cup A_{p_2} \cup A_{p_3}|$$

$$\overset{\text{PIE}}{=} n - \Big(|A_{p_1}| + |A_{p_2}| + |A_{p_3}| - |A_{p_1 p_2}| - |A_{p_2 p_3}| - |A_{p_3 p_1}| \Big)$$

$$+ |A_{p_1p_2p_3}|)$$

$$= n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3}\right) + \left(\frac{n}{p_1p_2} + \frac{n}{p_2p_3} + \frac{n}{p_3p_1}\right)$$

$$- \frac{n}{p_1p_2p_3}$$

$$= n\left(1 - 1/p_1\right)\left(1 - 1/p_2\right)\left(1 - 1/p_3\right)$$

In generale

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

$$A_{p_i} = \{ m \quad 1 \le m \le n,\ p_i \mid m \} \qquad i = 1, \dots, k$$

$$A_{p_ip_j} = \{ m \quad 1 \le m \le n,\ p_ip_j \mid m \} \qquad i \neq j$$

Se J è un sottoinsieme di $\{1, \dots, k\}$,

chiamiamo $A_J = \{ m \mid 1 \le m \le n,\ p_j \mid m \ \forall j \in J \}$

$$\varphi(n) = n - \left| \bigcup_{j=1}^{k} A_{p_j} \right| = n - \left| \bigcup_{j=1}^{k} A_{\{j\}} \right|$$

PRINCIPIO DI INCLUSIONE ESCLUSIONE PIE

$$= n - \left(\sum_{J \subseteq \{1, \dots, k\}} (-1)^{|J|+1} |A_J| \right)$$

$J \neq \emptyset$

$$= \sum_{J \subseteq \{1,\dots,k\}} (-1)^{|J|} |A_J|$$

ponendo $A_\emptyset = \{m \quad 1 \le m \le n\}$

$$= \sum_{J \subseteq \{1,\dots,k\}} (-1)^{|J|} \frac{n}{\prod_{j \in J} p_j}$$

$$= n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Teorema Se $n = p_1^{e_1} \cdots p_k^{e_k}$, allora

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= p_1^{e_1 - 1}(p_1 - 1)\, p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1)$$

Esempio $\varphi(100) = \varphi(2^2 5^2) =$

$$= 4 \cdot 25 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$$

$$= 2 \cdot 20 = 40$$

Corollario La funzione φ è MOLTIPLICATIVA, cioè per ogni coppia di interi m, n CHE SIANO PRIMI FRA LORO si ha

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

Esempio $\varphi(100) = \varphi(4)\,\varphi(25) = 2 \cdot 20$

$$2 = \varphi(4) \neq \varphi(2)\,\varphi(2) = 1$$

Dimostrazione $n = p_1^{e_1} \cdots p_k^{e_k}$

$$m = q_1^{f_1} \cdots q_r^{f_r}$$

dove ogni p_i è diverso da ogni q_j

In particolare, la fattorizzazione unica di $m \cdot n$ è $p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_r^{f_r}$

$$\varphi(n) = n \cdot (1 - 1/p_1) \cdots (1 - 1/p_k)$$

$$\varphi(m) = m \cdot (1 - 1/q_1) \cdots (1 - 1/q_r)$$

$$\varphi(mn) = mn \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_r}\right)$$

da cui in effetti $\varphi(mn) = \varphi(m)\,\varphi(n)$ □

Osservazioni

(A) "$\varphi(n)$ è (quasi) sempre pari"

$\varphi(n)$ dispari $\iff$ $n = 1$ o $n = 2$

Sia $n \geq 3$, $n = p_1^{e_1} \cdots p_k^{e_k}$. Allora

$$\varphi(n) = p_1^{e_1-1}(p_1-1) \cdots p_k^{e_k-1}(p_k-1)$$

(se n pari, $p_1 = 2$)

- Se n ha un divisore primo dispari, diciamo p_i, allora $(p_i - 1) \mid \varphi(n)$, e $p_i - 1$ è pari, quindi $\varphi(n)$ pari

- Altrimenti $n = p_1^{e_1} = 2^{e_1}$ con $e_1 \geq 2$ (perché $n \geq 3$)

  Allora $\varphi(n) = 2^{e_1-1} \cdot (2-1) = 2^{e_1-1}$, che è pari

(B) $\varphi(p) = p - 1$ banalmente (tutti i numeri interi nell'intervallo $[1, p-1]$ sono primi con p)

Esercizio Per ogni $n \in \mathbb{Z}_{>0}$ si ha

$$\sum_{d \mid n} \varphi(d) = n$$

Esempio Se $n = p^k$,

$$\sum_{d \mid p^k} \varphi(d) = \sum_{j=0}^{k} \varphi(p^j) =$$

$d = p^j$

$$= \left(\sum_{j=1}^{k} p^{j-1} \cdot (p-1) \right) + 1$$

$$= (p-1) \sum_{i=0}^{k-1} p^i + 1$$

$$= (p-1) \frac{p^k - 1}{p-1} + 1 = p^k$$

Dimostrazione generale

Consideriamo $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n-1}{n}, \frac{n}{n}$.

$$\#\text{frazioni} = n = \sum_{d \leq n} \#\{\text{fraz. con denom} = d\}$$

(ridotte ai min. termini)

$$= \sum_{d \mid n} \#\{\text{fraz. con denom.} = d\}$$

$$= \sum_{d \mid n} \varphi(d)$$

Esercizio Trovare tutti gli n tali che

$$\varphi(n) = 12$$

Svolgimento $n = p_1^{e_1} \cdots p_k^{e_k}$

$$12 = \varphi(n) = p_1^{e_1 - 1}(p_1 - 1) \cdots p_k^{e_k - 1}(p_k - 1)$$

Se $e_i \geq 2$ allora $p_i \mid \varphi(n) = 12 \Rightarrow$

$$\Rightarrow p_i \in \{2, 3\}$$

Se $p \mid n$, allora $(p-1) \mid \varphi(n) = 12$

$\Rightarrow p \leq 13$; in realtà, $p \in \{2, 3, 5, 7, 13\}$

Dividiamo in casi secondo il più grande primo che divide n:

- $p = 13$, $n = 13m$ con $(m, 13) = 1$

$$\Rightarrow \varphi(n) = \varphi(13) \cdot \varphi(m)$$

$$\begin{matrix} \| & & \| \\ 12 & = & 12 \cdot \varphi(m) \end{matrix}$$

$$\Rightarrow m \in \{1, 2\}$$

Prime due soluzioni: $n = 13, 26$

- $p = 7$, $n = 7m$ con $(m, 7) = 1$

$$12 = \varphi(n) = \varphi(7) \cdot \varphi(m)$$
$$= 6 \cdot \varphi(m) \Rightarrow \varphi(m) = 2$$

esercizio

$\Rightarrow m \in \{3, 4, 6\}$

Altre 3 soluzioni: 21, 28, 42

- $p = 5$ $n = 5m$ $(5, m) = 1$

$$12 = \varphi(n) = \varphi(5)\,\varphi(m)$$
$$= 4 \cdot \varphi(m)$$
$$\Rightarrow \varphi(m) = 3$$ **IMPOSSIBILE**

- $p = 3$ $n = 2^a 3^b$ con $b \geq 1$

$$12 = \varphi(n) = \varphi(2^a) \cdot \varphi(3^b)$$
$$= (2 \cdot 3^{b-1}) \cdot \varphi(2^a)$$

$* \; a = 0$ $12 = 2 \cdot 3^{b-1}$ $6 = 3^{b-1}$

IMPOSSIBILE

* $a \geq 1$ $\qquad 12 = 2 \cdot 3^{b-1} \cdot 2^{a-1}$

$$= 2^a \cdot 3^{b-1}$$

da cui $a = 2$, $b = 2$, $n = 36$

- $p = 2$, $n = 2^a \Rightarrow \varphi(2^a) = 2^{a-1}$ non è mai $= 12$

Risolvere $\varphi(m) = 2$

Supponiamo $p \mid m$, $p \geq 5$. Allora $(p-1) \mid \varphi(m)$, da cui $\varphi(m) \geq p-1 \geq 4$, assurdo.

Dunque $m = 2^a 3^b$, e abbiamo due casi:

(i) $b > 0$. Allora $\varphi(m) = \varphi(2^a) \cdot \varphi(3^b) = \varphi(2^a) \cdot 2 \cdot 3^{b-1}$, $\overset{2}{=}$

da cui $b = 1$ e $\varphi(2^a) = 1 \Rightarrow a = 0, 1$. Questo fornisce le soluzioni $m = 3$ e $m = 6$

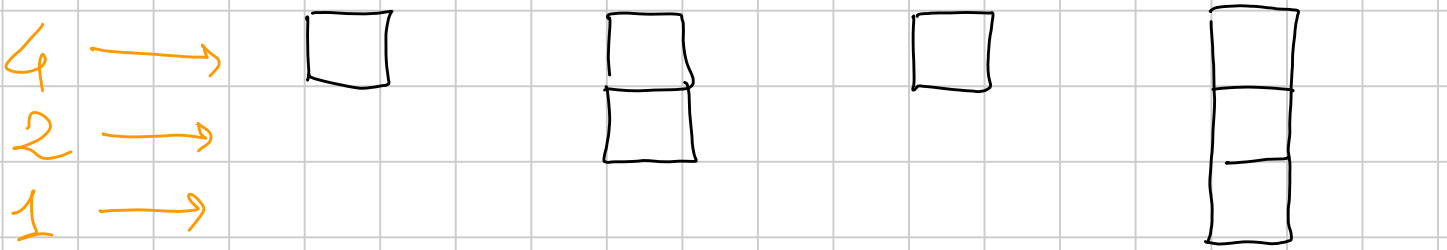
(ii) $b = 0$. Allora $2 = \varphi(2^a) = 2^{a-1} \Rightarrow a = 2$, il che dà la soluzione $m = 4$.

QUALCHE ESERCIZIO

① Sia p un numero primo, n un intero positivo. Qual è l'esponente di p nella fattorizzazione di $n!$?

$p = 2 \qquad n = 8$

$$1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8$$



$$1 + 2 + 1 + 3 = 7$$

Risposta:

$$v_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$$

Esempio $\quad v_3(30!) = \left\lfloor \frac{30}{3} \right\rfloor + \left\lfloor \frac{30}{9} \right\rfloor + \left\lfloor \frac{30}{27} \right\rfloor$

$$= 10 + 3 + 1 = 14$$

(2) Sia n un intero positivo. Sia

$$\mathcal{F}_n = \left\{ \frac{a}{b} \;\middle|\; \begin{array}{l} \text{frazioni} \in [0,1] \\ \text{con } b \le n \end{array} \right\}$$

insieme di Farey

$$\mathcal{F}_5 = \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \boxed{\frac{3}{5}}, \boxed{\frac{2}{3}}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\}$$

Siano $\frac{a}{b} < \frac{c}{d}$ due elementi adiacenti

Allora $bc - ad = 1$ $\quad \left(\begin{array}{l} (a,b) = 1 \\ (c,d) = 1 \end{array} \right)$

Dimostrazione Consideriamo l'equazione

$$bx - ay = 1$$

Vorrei mostrare che $(x,y) = (c,d)$ è una soluzione. Una soluzione c'è, e le altre si ottengono sommando a x multipli di a a y ——— b

In particolare c'è un'unica soluzione con

$$n - b < y \le n$$

Sia (x,y) la soluz. che rispetta questa disuguaglianza. Vorrei mostrare

$(x,y) = (c,d)$. Supponiamo che non lo sia.

$\frac{x}{y} \in \mathcal{F}_n$ $\qquad \frac{a}{b} < \frac{c}{d} < \frac{x}{y}$

$bx - ay = 1 \quad \Rightarrow \quad \frac{x}{y} = \frac{1}{by} + \frac{a}{b} > \frac{a}{b}$

$<$ viene da $a/b < x/y$ e $c/d > a/b$ sono adiacenti.

$$\frac{x}{y} - \frac{a}{b} = \frac{bx - ay}{yb} = \frac{1}{by}$$

$$\left(\frac{x}{y} - \frac{c}{d}\right) + \left(\frac{c}{d} - \frac{a}{b}\right) \geq \frac{1}{dy} + \frac{1}{bd}$$

$$\frac{1}{by} \geq \frac{1}{dy} + \frac{1}{bd}$$

$$d \geq b + y > b + (n-b) = n,$$

e questo è assurdo perché $c/d \in \mathcal{F}_n$, frazioni con denominatore $\leq n$. $\square$

Teorema (Hurwitz)

$\forall \alpha \in \mathbb{R} \setminus \mathbb{Q}$ esistono infinite frazioni p/q t.c. $\left|\alpha - p/q\right| \leq \frac{1}{\sqrt{5}q^2}$

$\frac{a}{b} < \alpha < \frac{c}{d}$ $\quad a/b, c/d \in F_n$ consecutive

Allora una delle 3 frazioni

$$\frac{a}{b}, \quad \frac{c}{d}, \quad \frac{a+c}{b+d}$$

verifica la disuguaglianza.