Proprietà di ϕ(n)

26 October 2022 11:17

La φ di Eulero

$$\varphi : \mathbb{N}\setminus\{0\} \to \mathbb{N}\setminus\{0\}$$

$\cdot\ \varphi(1) = 1$

per $n>1$ $\varphi(n)$ = numero dei coprimi di n minori di n

OSS. Per Lagrange, $a^{\varphi(m)} \equiv 1\ (m)$ per $(a,m)=1$

OSS. 2 φ è una funzione aritmetica moltiplicativa (i.e. moltiplicativa rispetto a due coprimi): $\varphi(bc) = \varphi(b)\varphi(c) \Leftarrow$
$\Leftarrow (b,c) = 1$.

Dimostrazione

Dato $m>0$, se $s \equiv t\ (m)$, allora $(s,m)=1$
$\longleftrightarrow (t,m) = 1$

$s = mk'' + r$ $\quad$ $p|t \iff (p|m)$
$t = mk' + r$ $\quad$ $\leftrightarrow p|r \leftrightarrow$
$\iff p|s$ quindi
$(s,m) = (t,m)$

Calcoliamo $\varphi(bc)$.
Sia u un intero positivo $|u<bc$ e primo con bc.
Vale allora che

$$\begin{aligned} \varphi(b) & \left[\ u \equiv \lambda\ (b) \quad \text{con } 1 \le \lambda < b \right. \\ \varphi(c) & \left[\ u \equiv \mu\ (c) \quad \text{con } 1 \le \mu < c \right. \end{aligned}$$

$$\begin{cases} (u,b) = 1 \\ (\lambda,b) = (u,b) \end{cases} \Longrightarrow (\lambda, b) = 1$$

(idem) $\rightarrow (\nu, c) = 1$ (quindi u si scrive come coprimo di b e c).

Per il Teorema cinese del resto,

$$\begin{cases} u \equiv \lambda \ (b) \\ u \equiv \nu \ (c) \end{cases}$$

ammette un'unica soluzione modulo bc (poiché copr.mi).

Inoltre $(u,b) = 1 \wedge (u,c) = 1 \Rightarrow$

$\Rightarrow (u, bc) = 1$ (infatti $p \neq 1 | bc \Rightarrow p | b \vee p | c$, impossibile perché $(u,b) = (u,c) = 1$).

Si è dimostrata così la bigezione:

$$\varphi(bc) = \varphi(b)\varphi(c).$$

∎

Teorema

$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots$ con p_i primi $\Longrightarrow$

$$\Longrightarrow \varphi(m) = m \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots =$$

$$= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right)\dots$$

Dimostrazione

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

$p \quad 2p \quad 3p \quad \cdots \quad p^k$

ossia $\varphi(p^k) =$

$= p^k -$ "num. multipli di p" $=$

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

$(k, p) = 1 \rightarrow$

$\rightarrow (k, p^k) = 1$

$d | p^k \wedge d | k$