La funzione di Eulero

La funzione φ di Eulero (o funzione di Euler-Gauss) è l'applicazione di $\mathbb{N}^{\#}$ in sé definita ponendo, per ogni $n \in \mathbb{N}^{\#}$,

$$\varphi(n) = \big|\{a \in \mathbb{N}^{\#} \mid a \leq n \wedge a \text{ e } n \text{ sono coprimi}\}\big|.$$

Ad esempio, poiché tra gli interi positivi 1, 2, 3, 4, 5 e 6 ad essere coprimi con 6 sono (solo) 1 e 5 si ha $\varphi(6) = 2$.

La funzione di Eulero esprime le cardinalità del gruppo degli invertibili dei quozienti di $\mathbb{Z}$. Infatti, per ogni $n \in \mathbb{N}^{\#}$, sappiamo che gli elementi dell'anello $\mathbb{Z}_n$ corrispondono precisamente ai numeri interi positivi a tali che $a \leq n$, nel senso che

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{N}^{\#} \wedge a \leq n\}$$

e se a e b sono interi positivi minori o uguali a n si ha $[a]_n = [b]_n$ se e solo se $a = b$. Sappiamo inoltre che, con queste stesse notazioni, $[a]_n$ è invertibile in $\mathbb{Z}_n$ se e solo se a e n sono coprimi. Dunque

$$\mathcal{U}(\mathbb{Z}_n) = \{[a]_n \mid a \in \mathbb{N}^{\#} \wedge a \leq n \wedge a \text{ e } n \text{ sono coprimi}\}$$

e quindi

$$\big|\mathcal{U}(\mathbb{Z}_n)\big| = \varphi(n).$$

Calcolo dei valori della funzione di Eulero. Sia p un numero (naturale) primo, e sia $n \in \mathbb{N}^{\#}$. Se $a \in \mathbb{Z}$ è chiaro che se a e p^n non sono coprimi, dunque se a e p hanno un fattore primo positivo in comune, questo fattore non potrà che essere p, l'unico divisore positivo primo di p^n. Da ciò segue facilmente che gli interi non coprimi con p^n sono tutti e soli i multipli p. Abbiamo allora:

$$\varphi(p^n) = \big|\{a \in \mathbb{N}^{\#} \mid a \leq n \wedge p \nmid a\}\big|.$$

Per ottenere $\varphi(p^n)$ basta dunque sottrarre a p^n (il numero degli interi positivi minori o uguali a p^n) il numero dei multipli positivi di p minori o uguali a p^n. Questi multipli sono $p, 2p, 3p, \dots, p^{n-1}p = p^n$, e sono evidentemente p^{n-1} in tutto. Pertanto:

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1). \tag{$*$}$$

Un caso particolare, per $n = 1$, è $\varphi(p) = p - 1$, cosa che si può verificare anche direttamente (tutti gli interi positivi minori di p sono coprimi con p).

Il calcolo di $\varphi(n)$ per un arbitrario intero positivo n si esegue utilizzando $(*)$ e la prossima informazione, di cui si omette la dimostrazione:

se s e t sono interi positivi <u>coprimi</u> si ha $\varphi(st) = \varphi(s)\varphi(t)$. $(**)$

Da una applicazione ripetuta di questo risultato si ottiene un enunciato (apparentemente) più generale: *se $t_1, t_2, \dots, t_r$ sono interi positivi a due a due coprimi, si ha $\varphi(t_1 t_2 \cdots t_r) = \varphi(t_1)\varphi(t_2)\cdots\varphi(t_r)$.*

Sia ora assegnato $n \in \mathbb{N}^{\#}$, e supponiamo di voler calcolare $\varphi(n)$. Scomponiamo n in prodotto di potenze di primi, dunque $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$ per opportuni primi $p_1, p_2, \dots, p_r$ a due a due distinti e interi positivi $\lambda_1, \lambda_2, \dots, \lambda_r$. Allora $\varphi(n) = \varphi(p_1^{\lambda_1})\varphi(p_2^{\lambda_2})\cdots\varphi(p_r^{\lambda_r})$, che sappiamo calcolare grazie a $(*)$.

Esempio. Calcoliamo $\varphi(360)$. Si ha $360 = 2^3 3^2 5$. Ora, $\varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$, inoltre $\varphi(3^2) = 3^2 - 3 = 6$ e $\varphi(5) = 5 - 1 = 4$. Pertanto

$$\varphi(360) = \varphi(2^3)\varphi(3^2)\varphi(5) = 4 \cdot 6 \cdot 4 = 96.$$

Notare che $\varphi(360) = \varphi(36 \cdot 10) \neq \varphi(36)\varphi(10) = \varphi(4)\varphi(9)\varphi(2)\varphi(5) = 2 \cdot 6 \cdot 1 \cdot 4 = 48$; più semplicemente $2 = \varphi(4) = \varphi(2 \cdot 2) \neq \varphi(2)\varphi(2) = 1 \cdot 1 = 1$. Ciò mostra come in $(**)$ sia importante l'ipotesi che i fattori s e t siano tra loro coprimi.