La funzione phi di Eulero

di Antonino Giambò

1. In un precedente articolo ho avuto modo di mostrare il ruolo importante svolto dalla funzione $\varphi(n)$. In questo nuovo contributo intendo approfondire il discorso su questa funzione.

Devo dire che l'argomento non rientra nel piano di studi di uno studente liceale, ma può ugualmente essere utile a chi nutre qualche interesse per lo studio della Matematica.

La funzione $\varphi(n)$ è denominata *funzione φ di Eulero* (o anche *funzione toziente* o ancora *funzione indicatrice di Eulero*). A volte anche *funzione di Eulero-Gauss*.

Essa associa ad ogni numero naturale n non nullo il numero dei numeri naturali minori di n e primi con esso.

Un'apposita tabella (tabella 1) evidenzia questa corrispondenza per i numeri n tali che $1<n\leq 20$.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(n)$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

tabella 1

Si può costatare che non è stato preso in considerazione il valore di $\varphi(1)$. Questo perché è necessaria una postilla. Il fatto è che, a rigor di logica dovrebbe essere $\varphi(1)=0$, ma si assume per convenzione $\varphi(1)=1$.

Di solito l'insieme dei numeri minori di un dato numero n e primi con esso è indicato con il simbolo U_n.

Cosicché, per esempio: $U_3=\{1, 2\}$, $U_8=\{1, 3, 5, 7\}$.

È dunque, in generale:

$$\varphi(n) = \text{card}\ (U_n)\ ,$$

vale a dire che $\varphi(n)$ è il cardinale dell'insieme U_n, per l'appunto il numero degli elementi che costituiscono l'insieme U_n.

La domanda interessante è però la seguente:

Una volta fissato n, come si calcola $\varphi(n)$?

Nella tabella precedente abbiamo elencato alcuni casi. Si tratta di casi piuttosto semplici, in verità, dato che sono stati considerati i primi valori di n, per cui è facile contarli.

S'intuisce poi agevolmente che se n è un numero primo, i numeri naturali minori di n e primi con esso sono tutti i numeri da 1 ad $n-1$, estremi inclusi, e sono pertanto in numero di $n-1$. Ecco perciò una prima regola:

REGOLA PER IL CALCOLO DI $\varphi(n)$ QUANDO n È UN NUMERO PRIMO.

Quando n è un numero primo, allora:

$$\varphi(n) = n - 1\ .$$

Più complicato si presenta il calcolo di $\varphi(n)$ quando n è un numero composto piuttosto "grande".

Per esempio, quanto vale $\varphi(2.400)$?

Impresa improba se intendiamo determinare per elencazione l'insieme $U_{2.400}$.

Per adesso non ci pensiamo e andiamo avanti, tenendo comunque presente che, in sostanza, non ci interessa conoscere gli elementi di U_n ma quanti sono questi elementi.

Mostriamo allora che esistono regole idonee per il calcolo di $\varphi(n)$, noto che sia n.

Sono state trovate da Eulero [1] e da Gauss [2].

---

1 Leonardo Eulero (nome italianizzato di Leonhard Euler), matematico svizzero, 1707-1783.

2 Carl Friedrich Gauss, matematico tedesco, 1777-1855.

2. Eulero per primo dimostrò una regola per il calcolo di $\varphi(n)$.

REGOLA DI EULERO PER IL CALCOLO DI $\varphi(n)$.

Se n = a b, con a, b numeri primi fra loro, allora:

$$\boldsymbol{\varphi(n) = \varphi(a) \cdot \varphi(b)} .$$

La sua dimostrazione richiede una premessa, un lemma.

LEMMA.

Dato il numero $n = p^s$, dove p è un numero primo ed s un numero naturale non nullo, risulta:

$$\boldsymbol{\varphi(n) = \varphi(p^s) = p^s \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p}\right)} .$$

DIMOSTRAZIONE DEL LEMMA.

Elenchiamo tutti i numeri naturali (diversi da 0) minori di n, che però non siano primi con n. Essi sono solo ed esclusivamente i seguenti numeri:

$$p \cdot 1, \;\; p \cdot 2, \;\; p \cdot 3, \;\; \ldots , \;\; p \cdot (p^{s-1} - 1)$$

e sono evidentemente in numero di $p^{s-1} - 1$.

D'altro canto i numeri naturali diversi da 0 e minori di n – vale a dire i numeri $1, 2, 3, \ldots , n-1$ – sono in numero di $n-1$ e perciò, essendo $n=p^s$, sono in numero di $p^s - 1$.

Si desume che il numero $\varphi(n)$ dei numeri naturali minori di n e primi con esso è:

$$\varphi(n) = (p^s - 1) - (p^{s-1} - 1) = p^s - p^{s-1} = p^s \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p}\right) .$$ [c. v. d.]

Per esempio, se $n=3^5=243$, per cui $p=3$ e $s=5$, i numeri (diversi da 0) minori di n, che non siano primi con n – tenendo presente che in questo caso si ha: $p \cdot (p^{s-1} - 1)=3 \cdot \left(3^{5-1}-1\right) = 3 \cdot 80$ – sono i seguenti:

$$3 \cdot 1, \;\; 3 \cdot 2, \;\; 3 \cdot 3, \;\; \ldots , \;\; 3 \cdot 80 ,$$

e sono chiaramente in numero di 80.

Mentre i numeri naturali diversi da 0 e minori di $n=243$ sono ovviamente 242.

Pertanto:

$$\varphi(243) = 242 - 80 = 162 \quad \text{e di fatto:} \quad 243 \cdot \left(1 - \frac{1}{3}\right) = 162.$$

In particolare, se n è esattamente uguale al numero primo p, si ha:

$$\varphi(n) = n \left(1 - \frac{1}{n}\right) = n - 1 .$$

Cosa che, del resto, sapevano già.

- Ripercorrendo la precedente dimostrazione, si può notare un fatto rilevante, una relazione, che costituisce in sostanza un'altra regola per il calcolo di $\varphi(n)$.

ALTRA REGOLA PER IL CALCOLO DI $\varphi(n)$.

Se p è un numero primo ed s è un naturale qualsiasi non nullo, risulta:

$$\boldsymbol{\varphi(p^s) = p^s - p^{s-1}} .$$

Esempi:

$$\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54\,; \quad \varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$$

Passiamo adesso alla dimostrazione della regola di Eulero.

DIMOSTRAZIONE DELLA REGOLA DI EULERO.

Supponiamo che sia $n = a\,b$, con $a=p^s$ e $b=q^t$, essendo p, q numeri primi diversi fra loro ed s, t numeri naturali non nulli, per cui a, b sono numeri coprìmi.

Osserviamo che i numeri diversi da 0 e minori di n, che però non siano primi con n, sono solo ed esclusivamente i numeri seguenti:

$$p\cdot 1,\ \ p\cdot 2,\ \ p\cdot 3,\ \ \ldots,\ \ p\cdot\left(\frac{n}{p}-1\right);\quad q\cdot 1,\ \ q\cdot 2,\ \ q\cdot 3,\ \ \ldots,\ \ q\cdot\left(\frac{n}{q}-1\right).$$

Questi due gruppi di numeri non sono però disgiunti. Ad entrambi appartengono infatti i numeri del seguente terzo raggruppamento:

$$p\,q\cdot 1,\ \ p\,q\cdot 2,\ \ p\,q\cdot 3,\ \ \ldots,\ \ p\,q\cdot\left(\frac{n}{p\,q}-1\right).$$

[Al fine di chiarire quanto detto a proposito di questi tre raggruppamenti, facciamo un esempio.

Supponiamo allora che sia $a=p^2=3^2$ e $b=q^2=5^2$, per cui:

$$n = 225,\quad \frac{n}{p}-1=\frac{225}{3}-1=74,\quad \frac{n}{q}-1=\frac{225}{5}-1=44,\quad \frac{n}{p\,q}-1=\frac{225}{15}-1=14.$$

Dunque:

- il primo raggruppamento è formato dai seguenti numeri: $3\cdot1,\ \ 3\cdot2,\ \ 3\cdot3,\ \ldots,\ \ 3\cdot74$;
- il secondo raggruppamento è formato dai seguenti numeri: $5\cdot1,\ \ 5\cdot2,\ \ 5\cdot3,\ \ldots,\ \ 5\cdot44$;
- il terzo raggruppamento è formato dai seguenti numeri: $3\cdot5\cdot1,\ \ 3\cdot5\cdot2,\ \ 3\cdot5\cdot3,\ \ldots,\ \ 3\cdot5\cdot14$.

Spieghiamo perché ogni elemento del terzo raggruppamento è comune agli altri due. Per capirlo basta costatare che il numero $3\cdot5\cdot14$, che è il numero più grande del terzo raggruppamento, può essere scritto in due modi convenienti $3\cdot70$ e $5\cdot42$; di questi due numeri, il primo è minore di $3\cdot74$, che è il numero più grande del primo raggruppamento, il secondo è minore di $5\cdot44$, che è il numero più grande del secondo raggruppamento.]

Quest'ultimo fatto, il fatto cioè che i numeri del terzo raggruppamento si trovano tutti anche nei primi due raggruppamenti, può essere spiegato in generale.

A questo proposito, mettiamo a confronto il numero più grande del terzo raggruppamento, cioè:

$$p\,q\cdot\left(\frac{n}{p\,q}-1\right) = n - p\,q\,,$$

con i numeri più grandi dei primi due raggruppamenti, vale a dire:

$$p\cdot\left(\frac{n}{p}-1\right) = n - p \quad \text{e} \quad q\cdot\left(\frac{n}{q}-1\right) = n - q\,.$$

Non ci vuol molto a capire che si ha: $n - p\,q < n - p$ e $n - p\,q < n - q$.

E questo basta per concludere che effettivamente tutti i numeri del terzo raggruppamento si trovano anche nei primi due.

Ora, i numeri dei primi due raggruppamenti sono in numero rispettivamente di $\left(\frac{n}{p}-1\right)$ e $\left(\frac{n}{q}-1\right)$, mentre quelli comuni ai due raggruppamenti sono in numero di $\left(\frac{n}{pq}-1\right)$. Ne discende che i numeri naturai diversi da 0 e minori di n, che però non siano primi con n, sono in numero di:

$$\left(\frac{n}{p}-1\right)+\left(\frac{n}{q}-1\right)-\left(\frac{n}{pq}-1\right)=\frac{n}{p}+\frac{n}{q}-\frac{n}{pq}-1.$$

Considerato che il numero dei numeri naturali diversi da 0 e minori di n è n−1, si ha:

$$\varphi(n) = (n-1)-\left(\frac{n}{p}+\frac{n}{q}-\frac{n}{pq}-1\right) = n\left[\left(1-\frac{1}{p}\right)-\frac{1}{q}\left(1-\frac{1}{p}\right)\right] = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right).$$

Ossia, ricordando che $n = a\,b$:

$$\varphi(n) = a\,b\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = \left[a\left(1-\frac{1}{p}\right)\right]\left[b\left(1-\frac{1}{q}\right)\right] = \varphi(a)\cdot\varphi(b). \qquad [c.v.d.]$$

Facciamo un esempio.

Sia al riguardo n=72, vale a dire $n = 2^3 \cdot 3^2$. Ebbene, in base alla regola di Eulero, risulta:

$$\varphi(72) = \varphi(2^3)\cdot\varphi(3^2) = 2^3\left(1-\frac{1}{2}\right)\cdot 3^2\left(1-\frac{1}{3}\right) = 8\cdot\frac{1}{2}\cdot 9\cdot\frac{2}{3} = 24\,.$$

Di fatto:

$$U_{72} = \{1,5,7,11,13,17,19,23,25,29,31,35,37,41,43,47,49,53,55,59,61,65,67,71\}$$

Un'altra regola si ottiene come semplice corollario della regola di Eulero. Ed è la seguente:

COROLLARIO DELLA REGOLA DI EULERO.

Se a, b sono numeri primi, diversi fra loro, risulta:

$$\boldsymbol{\varphi(a\,b) = (a-1)(b-1)}\,.$$

DIMOSTRAZIONE.

Considerato che se a, b sono numeri primi allora sono certamente numeri primi fra loro, per la regola di Eulero si ha: $\varphi(a\,b)=\varphi(a)\varphi(b)$ e di conseguenza: $\varphi(a\,b)=(a-1)(b-1)$. [c.v.d.]

NOTA BENE.

È fondamentale precisare che a, b sono numeri diversi fra loro. Se infatti così non fosse e fosse invece a=b, allora risulterebbe: $\varphi(a^2) = (a-1)^2$, mentre è noto che si ha $\varphi(a^2) = a^2\left(1-\frac{1}{a}\right) = a^2-a$. Ed evidentemente è:

$$(a-1)^2 \neq a^2 - a\,.$$

A meno che non sia a=1, ma in questo caso a non sarebbe un numero rimo.

3. Gauss enunciò e dimostrò una regola generale per il calcolo di $\varphi(n)$, valida quale che sia il numero naturale n>1, primo o composto, a condizione che, se il numero è composto, si sappiano trovare i suoi fattori primi.

REGOLA DI GAUSS PER IL CALCOLO DI $\varphi(n)$.

Dato un numero naturale n maggiore di 1 e ammesso che siano $p_1, p_2, \ldots, p_k$ i suoi fattori primi, il numero $\varphi(n)$ dei numeri minori di n e primi con esso è dato dalla seguente formula:

$$\boldsymbol{\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)}.$$

Cosicché, com'è già stato detto, si sa calcolare $\varphi(n)$ se si conoscono i fattori primi di n.

Esempi:

- Se n=3, per cui n ha un solo fattore primo, il 3 medesimo, si ha:

$$\varphi(3) = 3\left(1-\frac{1}{3}\right) = 2\,.$$

- Se n=10, per cui n ha come fattori primi 2 e 5, si ha:

$$\varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 4\,.$$

In entrambi i casi è confermato quanto indicato nella tabella 1.

- Ma riprendiamo il caso in cui n=2.400, che avevamo accantonato.

Si fattorizza il numero e si trova che $2.400 = 2^5\cdot 3\cdot 5^2$.

Quindi 2.400 ha come fattori primi i numeri $2, 3, 5$, per cui, in base alla regola di Eulero:

$$\varphi(2.400) = 2.400\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 640\,.$$

Vale a dire che sono 640 i numeri naturali minori di 2.400 e primi con esso.

Concludo proponendo una dimostrazione della regola di Gauss, come applicazione di quella di Eulero.

DIMOSTRAZIONE DELLA REGOLA DI GAUSS.

Ripartiamo dalla regola di Eulero. Per cui, se $n = a\,b$, con a, b numeri primi fra loro, allora si ha:

$$\varphi(n) = \varphi(a)\cdot\varphi(b).$$

Naturalmente se $n = a\,b\,c$, dove a, b, c, presi a due a due, sono numeri coprìmi, per la proprietà associativa della moltiplicazione, per cui $n = a\,b\,c = (a\,b)\,c$, si ha:

$$\varphi(n) = \varphi(a\,b)\cdot\varphi(c) \text{ e siccome } \varphi(a\,b) = \varphi(a)\cdot\varphi(b) \text{ allora } \varphi(n) = \varphi(a)\cdot\varphi(b)\cdot\varphi(c).$$

E così pure, se $n = a_1 a_2 \ldots a_k$, dove $a_1,\ a_2,\ \ldots,\ a_k$, presi a due a due, sono numeri coprìmi, ricorrendo più volte alla proprietà associativa della moltiplicazione e tenendo presenti i risultati precedenti, si ha:

$$\varphi(n) = \varphi(a_1)\cdot\varphi(a_2)\cdot\ldots\cdot\varphi(a_k)\,.$$

Poniamo ora

$$a_1 = {p_1}^{s_1},\ a_2 = {p_2}^{s_2},\ \ldots,\ a_k = {p_k}^{s_k},$$

con $p_1,\ p_2,\ \ldots,\ p_k$ numeri primi diversi fra loro e $s_1,\ s_2,\ \ldots,\ s_k$ numeri naturali non nulli.

Osserviamo che i numeri ${p_1}^{s_1},\ {p_2}^{s_2},\ \ldots,\ {p_k}^{s_k}$, presi a due a due, sono numeri coprìmi e costatiamo che, in virtù del lemma precedente, risulta:

$$a_j\left(1-\frac{1}{p_j}\right) = \varphi(a_j)\,,\ \text{ per } 1 \le j \le k\,.$$

Si ha pertanto:

$$\varphi(n) = \left[a_1\left(1-\frac{1}{p_1}\right)\right]\left[a_2\left(1-\frac{1}{2}\right)\right]\ldots\left[a_k\left(1-\frac{1}{p_k}\right)\right].$$

Da qui segue immediatamente la formula cercata.

BIBLIOGRAFIA.

[1] Richard Courant – Herbert Robbins, *Che cos'è la matematica*, Torino, Universale Boringhieri, edizione gennaio 2000.

[2] Joaquín Navarro Sandalinas, *Eulero*, collana Geni della Matematica, Milano, RBA Italia, 2017.

[3] Antonio Rufián Lizana, *Gauss*, collana Geni della Matematica, Milano, RBA Italia, 2017.