TERZA TAPPA

Adesso ti voglio parlare di un argomento matematico che viene studiato ancora oggi e che ha origini antichissime: i numeri primi. Pensa che le prime tracce della loro conoscenza risalgono addirittura al Paleolitico, tra i 20 e i 22 mila anni fa. Ma che cos'è un numero primo? E perché è stato, ed è tuttora, un argomento centrale nel mondo matematico?

Parto dalla sua definizione: numero intero maggiore di 1 che ammette solo divisori banali, cioè 1 e sé stesso; se un numero non è primo è detto composto. I divisori di un numero sono quei numeri che lo dividono in modo perfetto, ossia senza lasciare resto. Ad esempio sono numeri primi 2, 3 e 5, mentre sono composti 4 e 6: infatti i primi hanno come divisori solo 1 e loro stessi, i secondi sono divisibili rispettivamente per 1, 2 e 4 o per 1, 2, 3 e 6.

La prima testimonianza, già anticipata prima, è l'Osso d'Ishango, un osso di babbuino ricoperto di scalfiture su 3 colonne. Una di queste contiene per l'appunto i numeri primi tra 10 e 20, il che fa pensare a una rudimentale conoscenza degli stessi. I reperti seguenti sono molto più vicini nel tempo, risalenti a circa 4000 anni fa, e provengono dalla Mesopotamia e dall'Egitto. Nel primo caso la risoluzione di alcuni problemi fa sottintendere la consapevolezza della fattorizzazione in primi, ossia nella capacità di riscrivere ogni numero composto come prodotto dei primi che lo compongono. Nel secondo caso invece alcuni calcoli in frazioni egizie nel Papiro di Rhind fanno ipotizzare che gli egizi facessero distinzione tra i primi e i composti.

Per il momento, tutte queste fonti, fanno supporre la consapevolezza dell'esistenza dei numeri primi, ma la prima vera traccia incontestabile di uno studio dei numeri primi si trova negli *Elementi* di Euclide, datato tra i 2500 e i 2400 anni fa. In questo libro Euclide, matematico greco, racchiude tutte le conoscenze matematiche acquisite fino a quel punto. I due grandi risultati relativi ai numeri primi raccolti in questo libro sono il teorema dell'infinità dei primi, ossia la Proposizione 20 del libro IX e la Proposizione 30 del libro VII, nota anche come lemma di Euclide. Dopo l'interesse del mondo greco, lo studio dei numeri primi venne accantonato per diverso tempo. Fu solo con il diciassettesimo secolo che la ricerca matematica in questo campo portò nuovi importanti risultati. Di questo, parte del merito va a Pierre de Fermat, "il principe dei dilettanti", così chiamato per il suo importante contributo al mondo matematico, nonostante se ne occupasse solo nel tempo libero. In questo periodo si iniziò a congetturare possibili modi per individuare i numeri primi: nacquero così quelli che oggi sono chiamati *numeri di Fermat*, ossia numeri della forma $2^{2^n} + 1$, e i *primi di Mersenne*, della forma $2^p - 1$ con p numero primo. Per quanto riguarda i numeri di Fermat, Eulero dimostrò che non tutti i numeri di questa forma sono primi. I primi di Mersenne invece sono un sottogruppo dei numeri primi contenente solo i primi che si possono ottenere da quella formula: ad esempio, nonostante 11 sia un numero primo, il numero M_{11} che si ottiene tramite la formula di Mersenne, non è primo. Infatti $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$, quindi non è un primo di Mersenne. Molti altri risultati interessanti nel campo dei numeri primi vennero ottenuti dallo svizzero Eulero nel 1700. In uno scambio di lettere tra lui e Goldbach, matematico tedesco, emerse la famosa congettura di Goldbach, enunciata da quest'ultimo. La congettura, riformulata poi da Eulero, afferma che:

"Ogni numero pari maggiore di 2 può essere scritto come somma di due numeri primi."

e rimane ancora oggi non dimostrata.

Dall'inizio dell'Ottocento, furono molti i matematici che studiarono la distribuzione dei numeri primi. Il francese Legendre e il tedesco Gauss congetturarono indipendentemente l'andamento della funzione che conta i numeri primi minori o uguali a un certo x. Attualmente la congettura è nota come il teorema dei numeri primi ed è stata dimostrata in modo indipendente da Hadamard e de la Vallée Poussin, dopo che

Bernhard Riemann collegò questo problema con un altro, quello di trovare gli zeri della funzione zeta di Riemann.
I numeri primi non hanno avuto un'applicazione pratica fino agli anni settanta. Con lo sviluppo della crittografia, nasce il concetto di chiave pubblica/privata; per cifrare e decifrare i messaggi viene creato l'algoritmo RSA che utilizza numeri che abbiano solo due fattori primi (ossia due numeri primi che moltiplicati tra loro mi diano il numero di partenza), che rappresentano le due chiavi. La ricerca di numeri primi sempre più grandi è necessaria per il buon funzionamento dell'algoritmo, e al giorno d'oggi avviene attraverso i computer.
Molti sono i problemi ancora irrisolti nel campo dei numeri primi. Il più importante riguarda lo studio della funzione zeta di Riemann, che permetterebbe di trovare una certa regolarità nella distribuzione dei numeri primi. Altre congetture non ancora dimostrate appartengono a Goldbach, a Legendre e anche ad Euclide, che ricordiamo essere vissuto nel 300 a.C.. Altri problemi irrisolti riguardano l'esistenza o meno di infiniti primi di una certa forma, come i *primi di Mersenne o di Fermat*.
Una piccola curiosità: le specie appartenenti al genere delle Magicicada, delle cicale molto diffuse nel Nord America, hanno cicli vitali di 13 e 17 anni, due numeri primi. Si ipotizza che il motivo di questa particolarità sia legato all'evoluzione della specie: il numero primo di anni ha garantito a queste specie di Magicicada una maggiore sopravvivenza. Infatti si sostiene che se il ciclo vitale di questi insetti fosse un numero non primo, tutti i predatori con ciclo vitale divisore di quel numero, avrebbero avuto la possibilità di specializzarsi nella predazione della Magicicada.
Come abbiamo visto la ricerca dei numeri primi ha da sempre interessato i matematici. Uno dei primi metodi, risalente al 200 a.C., è sicuramente quello di Eratostene di Cirene, matematico greco. Scopriamo insieme questo metodo per la ricerca dei numeri primi, il ***crivello di Eratostene.***
Si tratta di un algoritmo iterativo, ossia un insieme di istruzioni da seguire più volte per ottenere il risultato richiesto. Esso permette di trovare tutti i numeri primi al di sotto di una certa soglia *n*.

Vediamo il suo funzionamento con *n*=30.
Scriviamo in una tabella i primi 30 numeri naturali:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

Escludiamo 1, in quanto non è nè numero primo, nè numero composto. Si tratta infatti di un caso particolare. Partiamo quindi dalla casella successiva. Sottolineiamo il 2, e scartiamo tutti i suoi multipli.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~

Al termine di questa operazione, sottolineiamo il primo numero della tabella successivo al 2 che non è stato ancora scartato: il 3. Come nel caso precedente eliminiamo tutti i multipli.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~

Ripetiamo l'operazione per il primo numero successivo al 3 che non è ancora stato scartato, il 5, e scartiamo i suoi multipli.
Operiamo in questo modo fino ad esaurire i numeri della tabella.

~~1~~	**2**	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~

Tutti i numeri sottolineati sono numeri primi, perché non hanno divisori che non siano 1 e loro stessi. Infatti, per costruzione, abbiamo eliminato tutti i multipli presenti nella tabella.
Abbiamo così ottenuto tutti i numeri primi minori o uguali a 30:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Ora tocca a te! Utilizzando il crivello di Eratostene, trova il numero **primo più grande minore di 60**.

FONTI TERZA TAPPA

- Numero primo - Wikipedia
- numero primo in "Enciclopedia della Matematica" (treccani.it)
- Osso d'Ishango - Wikipedia
- Pierre de Fermat - Wikipedia
- Crivello di Eratostene (youmath.it)