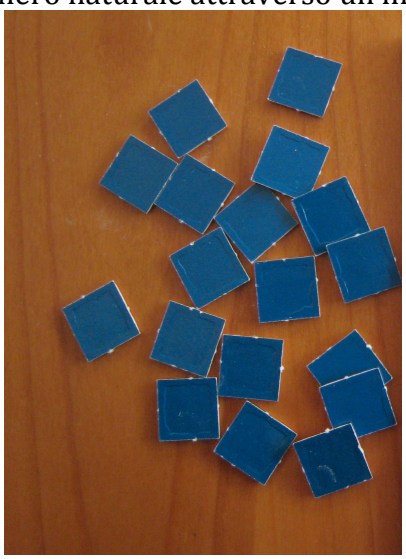
Numeri primi

I numeri primi sono stati introdotti e studiati dagli antichi Greci; Euclide li ha descritti negli "Elementi", dimostrando che sono infiniti.
La nozione di numero primo si estende in ambito più generale, ma noi la studieremo solo per i numeri naturali.

Definizione Un numero naturale è detto *numero primo* se è maggiore di 1 e ha come divisori solo 1 e sé stesso: un numero primo ha quindi esattamente 2 divisori.
Un numero maggiore di 1 che non è primo, ha più di due divisori ed è detto *composto*.

Rappresentiamo ogni numero naturale attraverso un insieme di quadratini:


Il numero 18

Un numero è primo quando posso formare con esso solo un rettangolo (identificando tra loro i rettangoli che hanno lati uguali); per questo motivo, Euclide chiamava *numeri lineari* i numeri primi. Possiamo studiare a mano i numeri più piccoli, concludendo che 2, 3 e 5 sono numeri primi.

5 

Un numero è composto quando posso formare più di un rettangolo. Per ogni divisore, si può formare un rettangolo che ha per lato il divisore: a mano possiamo controllare che 4, 6, 9 sono numeri composti. E' più efficace pensare che un numero è composto se può essere diviso (con resto zero) da un numero più piccolo di lui e diverso da 1.

3×2 

Ogni numero naturale diverso da 0 o 1 è primo o composto.

Numeri primi minori di 100: il setaccio (o crivello) di Eratostene

E' possibile trovare tutti i numeri primi? Questo è un problema che ha appassionato i matematici per moltissimi secoli. Una soluzione operativa a questo problema è stata trovata da Eratostene.
Il metodo di Eratostene non permette di elencare tutti i numeri primi, ma di elencare tutti i numeri primi che siano minori di un prefissato numero.

Eratostene (Cirene, 276a.C. - Alessandria d'Egitto, 194 a.C.) è stato uno studioso della Grecia antica, esperto in molti settori differenti: matematica, astronomia, geografia e poesia. Bibliotecario della Biblioteca di Alessandria in Egitto, ha misurato per primo e con notevole precisione le dimensioni della Terra e disegnato delle accuratissime carte geografiche del Mediterraneo. A lui si deve l'usanza di datare gli eventi a partire dalla prima Olimpiade.

Il metodo proposto da Eratostene per individuare l'elenco dei numeri primi più piccoli è utilizzato anche attualmente, e si basa sulla seguente osservazione: ***Se un numero è primo, tutti i suoi multipli (diversi da lui) non possono essere primi.***
Il metodo procede come segue: partiamo dalla tabella con i numeri da 1 a 100. Procedendo analogamente, è possibile determinare l'elenco dei numeri primi minori di un qualsiasi prefissato numero.

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
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

La tabella va letta partendo da in alto a sinistra, seguendo l'ordine crescente dei naturali.
L'elenco dei numeri primi si ottiene cancellando dall'elenco di tutti i numeri quelli che non sono primi.
Cancelliamo 1 che non è un numero primo. Contorniamo con un cerchietto il numero 2 (ad esempio con il giallo) e cancelliamo con un tratto obliquo tutti i suoi multipli.
Ora riprendiamo la tabella dall'inizio: il numero più piccolo che non è nè cerchiato nè cancellato è il 3; questo numero deve necessariamente essere primo (perché non c'è nessun numero più piccolo di lui che lo può dividere): lo si cerchia e si cancellano i suoi multipli
Proseguiamo cerchiando il numero più piccolo che non è stato nè cerchiato nè cancellato, e cancellando i suoi multipli.
Alla fine del lavoro, i numeri cerchiati sono i numeri primi entro il 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,
53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

I numeri primi sono infiniti
Questo risultato è stato dimostrato da Euclide [IX libro degli *Elementi*, proposizione 20]
Premettiamo una proposizione che riflette in modo più preciso sulla nozione di numero composto e sul ruolo dei numeri primi.

Proposizione: *ogni numero naturale diverso da 1 è divisibile per un numero primo.*
dimostrazione: Il numero 0 è divisibile per ogni numero naturale, e quindi anche per un numero primo. Sia ora n un numero diverso da 0 e da 1. Se n è un primo, è divisibile per se stesso. Se, invece, n è composto, può essere scritto come prodotto

$$n = h\ k$$

ove h e k siano due numeri minori di n. Se h è un numero primo, abbiamo concluso la dimostrazione; se, invece, h non è un numero primo, allora h è un numero composto, e a sua volta è prodotto di due numeri più piccoli di lui:

$$h = h_1\, k_1 \qquad \text{e quindi} \qquad n = h\ k = (\ h_1\, k_1\ )\, k = \ h_1\, (k_1\ k\ )$$

e $h_1 < h < n$.
Se h_1 è un numero primo, abbiamo concluso la dimostrazione. Se h_1 è un numero composto, è possibile scomporlo ulteriormente come prodotto di fattori più piccoli di h_1 : il ragionamento può essere ripetuto, e, a ogni passo, i fattori diventano più piccoli: poiché ciascuno dei fattori coinvolti deve essere maggiore di 1. ♦
Corollario: *ogni numero naturale diverso da 1 è prodotto di numeri primi, cioè*
(*) $$n = q_1 \times q_2 \times q_3 \times \ldots\ldots \times q_t$$
per opportuni numeri primi q_1 , q_2 , q_3 , , … , q_t).

Una espressione della forma (*) è detta *fattorizzazione di n in fattori primi (o scomposizione in fattori primi)*. In *(*) non necessariamente i fattori primi sono diversi tra loro; è possibile che compaia solo un fattore primo, cioè che t=1.* Si osservi che *n è un numero primo se e solo se in (*) si ha t=1.*

Teorema (Euclide) I numeri primi sono infiniti.
dimostrazione La dimostrazione procede per assurdo. Supponiamo per assurdo che esista solo un numero finito di numeri primi e scriviamone l'elenco completo: $p_1, p_2, ..., p_n$ (in questo elenco, ogni numero primo viene scritto una volta sola).:

$$\text{Numeri primi} = \{\ p_1, p_2, ..., p_n\ \}$$

Definiamo ora un numero, che chiamiamo M, ottenuto sommando 1 al prodotto di tutti i numeri primi:

$$M = p_1 \times p_2 \times \cdots \times p_n + 1$$

Il numero è maggiore di 1 (perché c'è almeno un numero primo) e diverso da tutti i numeri primi p_i. (perchè maggiore di ciascun p_i).
Vi sono due possibilità per M: può essere primo o composto. Se M fosse primo avremmo una contraddizione: infatti abbiamo già osservato che M è diverso da ciascun p_i e quindi non può appartenere all'insieme dei numeri primi.
Allora M deve essere composto: ma allora dovrebbe avere un fattore primo d, che deve essere uno dei numeri primi p_i. Ma allora d divide sia M che il prodotto $p_1 p_2 \cdots p_n$ (essendo uno dei numeri primi), e quindi deve dividere la loro differenza $M - p_1 p_2 \cdots p_n = 1$, il che è impossibile. Quindi M non può essere né primo né composto: ma questo è assurdo.
Concludiamo che i numeri primi sono infiniti. ♦

Teorema fondamentale dell'aritmetica

Proposizione: *se un numero primo divide il prodotto di due numeri naturali, allora il numero primo divide almeno uno dei due fattori*.
In simboli: se n= ab con n, a, b numeri naturali e

$$p \text{ primo tale che } p \mid n = a\ b \ \Rightarrow p|a \text{ oppure } p|b.$$

dimostrazione Sia p un fattore primo di ab . Se p è un divisore di a, la dimostrazione è completa. Supponiamo che p non sia un divisore di a. Allora esiste un numero naturale k tale

che $ab = k\,p$. Dal momento che p è primo e non è un divisore di a, sappiamo che a e p sono coprimi, cioè $MCD(a,p)=1$. L'identità di Bézout assicura l'esistenza di esistono due interi s e t tali che

$$1 = s\,a + t\,p.$$

Moltiplichiamo per b entrambi i membri, ottenendo

$$b = b\,s\,a + b\,t\,p = (a\,b)\,s + b\,t\,p$$

Ricordando che $ab = k\,p$, segue:

$$b = (a\,b)\,s + b\,t\,p = k\,p\,s + b\,t\,p = p\,(k\,s + b\,t)$$

Di conseguenza, p è un divisore di b.
Quindi p divide necessariamente a oppure b (o entrambi).♦

Teorema fondamentale dell'aritmetica *Ogni numero naturale maggiore di 1 ammette una fattorizzazione come prodotto di fattori primi come in (*). Tale rappresentazione è unica, se non si prende in considerazione l'ordine in cui compaiono i fattori.*
dimostrazione
L'enunciato del teorema asserisce l'esistenza di una fattorizzazione in numeri primi per ogni numero naturale, e successivamente la sua unicità. Dimostriamo separatamente le due affermazioni.
L'esistenza è stata dimostrata in precedenza (una dimostrazione più precisa richiede il principio di induzione).
La dimostrazione dell'unicità è facoltativa.