**Numeri primi e test di primalità**

di Antonino Giambò

**1.** C'è un argomento che, per la sua complessità, non viene neanche proposto agli studenti della scuola secondaria di 2° grado, quello che tratta dei cosiddetti *test di primalità*. Ed è giusto che sia così.

Ciò non di meno, è mio convincimento che quegli studenti che avessero intenzione di proseguire gli studi universitari in ambito scientifico, potrebbero avere interesse a saperne qualcosa. Magari non tutto, cosa impossibile d'altronde, ma almeno le nozioni più elementari.

È a costoro che sono rivolte le riflessioni contenute nel presente contributo.

**2.** Incomincio con alcune nozioni che, ad onor del vero, dovrebbero costituire patrimonio culturale di tutti gli studenti e certamente lo sono.

Un numero naturale si dice **primo** se è maggiore di 1 ed è divisibile solamente per 1 e per se stesso.

È "solamente" la parola chiave, giacché tutti i numeri maggiori di 1 sono divisibili per 1 e per se stessi, ma ai numeri primi si richiede di essere divisibili "solamente" per 1 e per se stessi.

Se un numero naturale maggiore di 1 non è primo si dice **composto**.

In base alle suddette definizioni, i numeri 0 e 1 non sono né primi né composti.

Un diagramma di Eulero-Venn (figura 1) riassume quella che si può considerare una ripartizione dell'insieme ℕ dei numeri naturali.

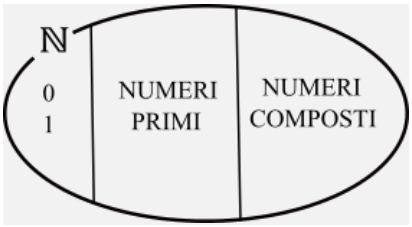


figura 1

Le definizioni di "numero primo" e di "numero composto" risalgono alla scuola pitagorica (VI sec. a.C.) e si ritrovano in Euclide (III sec. a.C.). Precisamente, nel libro VII degli *Elementi* [3] figura tra le *definizioni* sia la definizione di numero primo:

*Numero primo è quello che è misurato soltanto dall'unità* (definizione XI),

sia quella di numero composto:

*Numero composto è quello che è misurato da un qualche numero* (definizione XIII).

Euclide però non fa una trattazione mistica dell'argomento, come i Pitagorici, ma uno studio approfondito.

In particolare dimostra uno dei teoremi più belli della matematica antica (*Elementi*, libro IX, prop. 20):

*Esistono numeri primi in numero maggiore di quanti numeri primi si voglia proporre.*

Oggigiorno la proposizione è enunciata in questo modo:

*L'insieme dei numeri primi è infinito*.

Perché, ci chiediamo, Euclide ricorre a quella perifrasi?

Bisogna sapere che ad Euclide, come a tutti gli studiosi di quell'epoca, la matematica ufficiale inibiva l'uso del termine "infinito" ed è per questa ragione che Euclide si serve di una circonlocuzione per l'enunciato. In ogni caso, la sua dimostrazione è un capolavoro di logica.

La riproduco, anche se sono convinto che sia conosciuta dalla maggior parte degli studenti delle scuole superiori, se non addirittura da tutti.

Ovviamente, per la dimostrazione ci serviamo del nostro linguaggio, anche simbolico [1].

DIMOSTRAZIONE (dell'infinità dei numeri primi).

Ragioniamo per assurdo e supponiamo che l'insieme dei numeri primi sia finito, ossia che la successione dei numeri primi abbia un limite superiore, vale a dire che esiste un numero primo p che supera tutti gli altri numeri primi, per cui tutti i numeri primi sarebbero questi:

$$2,\ 3,\ 5,\ 7,\ \ldots\ ,\ p\,.$$

Consideriamo allora il loro prodotto P, aumentato di 1, cioè:

$$P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p + 1\,.$$

Chiaramente P>p. Delle due l'una: o P è un numero primo o è un numero composto. *Tertium non datur*.

Se P fosse un numero primo sarebbe un numero primo maggiore di p. Ma questo è assurdo avendo supposto che p è il massimo numero primo.

Supponiamo allora che P sia un numero composto. Osserviamo che, dividendolo per ciascuno dei numeri primi 2, 3, 5, ... , p, si ottiene sempre resto 1. Ragion per cui, P non è divisibile per alcuno di quei numeri primi, ma siccome è un numero composto deve esistere un numero primo che lo divide e questo numero, gioco forza, deve essere maggiore di p. Il che è assurdo avendo supposto che p è il massimo numero primo.

In conclusione, sotto l'ipotesi che esista un numero primo p che superi tutti gli altri numeri primi, il numero P non può essere né primo né composto. E questo ovviamente non può essere. Ragion per cui, la successione dei numeri primi non è limitata superiormente, è appunto illimitata; e dunque l'insieme dei numeri primi è infinito.

**3.** Euclide, pur fornendo la definizione di numero primo e dimostrando che esistono infiniti numeri primi, **non dà alcuna spiegazione circa il procedimento che bisogna seguire per ottenerli**. Ciò probabilmente perché la speculazione teorica, che lo affascina, non richiede quella ricerca e quindi, potremmo supporre, la cosa non lo interessa e non se ne occupa.

Comunque sia, un conto è sapere che ci sono infiniti numeri primi, altro è riuscire a determinarli. Non tutti, chiaramente, ché non si può, ma un qualche elenco parziale.

Ebbene, il primo matematico che ha fornito un criterio per costruire una successione di numeri primi è stato Eratostene di Cirene (275 circa – 194 a.C.), matematico e astronomo greco, che fu anche direttore della biblioteca di Alessandria.

Il metodo da lui elaborato va sotto il nome di ***crivello di Eratostene*** e la spiegazione che andiamo a fornire chiarisce bene tale denominazione.

Si scrivono uno di seguito all'altro il numero 2 ed il numero 3, che certamente sono numeri primi; quindi, a seguire, si scrivono tutti i numeri dispari, ovviamente su più colonne (tabella 1). Noi ci siamo fermati al numero 99, ma si capisce che potenzialmente potremmo spingerci fin dove vogliamo (si fa per dire).

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 5 | 7 | (9) | 11 | 13 | (15) | 17 | 19 |
| (21) | 23 | [25] | (27) | 29 | 31 | (33) | [35] | 37 | (39) |
| 41 | 43 | (45) | 47 | ~~49~~ | (51) | 53 | [55] | (57) | 59 |
| 61 | (63) | [65] | 67 | (69) | 71 | 73 | (75) | ~~77~~ | 79 |
| (81) | 83 | [85] | (87) | 89 | ~~91~~ | (93) | [95] | 97 | (99) |

tabella. 1

[1] Del teorema sull'infinità dei numeri primi esistono oggigiorno almeno altre 5 dimostrazioni. Chi avesse desiderio di conoscere tutte queste dimostrazioni può trovarle nel libro *Proofs from THE BOOK* di Martin Aigner e Günter M. Ziegler, (edizione italiana curata da Alfio Quarteroni), Milano, Springer, 2006, pagg. 3-6.

È inutile scrivere i numeri pari maggiori di 2 poiché sicuramente, essendo divisibili per 2, non sono numeri primi. A questo punto, a partire da 3 ma escludendolo, si eliminano dall'elenco tutti i multipli di 3 (nella tabella sono inscritti in un cerchietto). Finita quest'operazione, si ritorna al primo numero successivo al 3, che non sia stato eliminato. Costatato che si tratta del 5, lo si salta e si eliminano dall'elenco tutti i multipli di 5 che sono rimasti (nella tabella sono inscritti in un quadratino). Di nuovo si ritorna al primo numero successivo al 5 e si costata che è il 7. Si ripete l'operazione con i multipli di 7 (nella tabella sono contrassegnati da un quadrilatero intrecciato) e poi con quelli di 11, di 13 e così via finché essa è possibile.

Si può notare che il primo numero che si cancella, partendo da 3 è 9; partendo da 5 è 25; partendo da 7 è 49. Vale in effetti la seguente proprietà generale:

**Il primo numero da cancellare, nel crivello di Eratostene, ogni volta che l'operazione si ripete a partire da un dato numero n, è il quadrato di n**.

I numeri che rimangono dopo questa operazione di "setaccio", di "crivello" appunto, sono numeri primi.

Nel caso particolare della tabella 2, essi sono i numeri seguenti e sono esattamente i 25 numeri primi compresi nel primo centinaio di numeri naturali:

**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.**

La ricerca di numeri primi suscita da sempre l'interesse e la curiosità di esperti e dilettanti. Oggigiorno, con l'ausilio di idonei strumenti di calcolo automatico, se ne possono trovare anche di molto grandi.

Occorre precisare, tuttavia, che già nel XVIII secolo, quando gli strumenti di calcolo automatico non erano nemmeno un sogno, esistevano elenchi di numeri primi fino a qualche milione. Il grande Gauss, per esempio, disponeva di un elenco di numeri primi fino a 3 milioni. Ma ancor prima, nel XVII secolo, il matematico inglese John Pell (1611-1685) era in grado di ottenere un elenco di numeri primi fino a 100.000.

Alla data del 7 dicembre 2018 è stato scoperto il più grande numero primo conosciuto. Si tratta di un numero esagerato: $2^{82.589.933} - 1$, che, sviluppato e scritto nel sistema di numerazione decimale, è composto da 24.862.048 cifre. Non so dire se nel frattempo siano stati scoperti numeri primi più grandi, né se sono noti tutti i numeri primi minori di quello.

**4.** Giudico interessante una curiosità sui numeri primi che riprendo da [4, pag. 221].

Riguarda un quadrato magico molto singolare. Precisamente, un quadrato magico di ordine 6, **i cui elementi sono tutti numeri primi** (figura 2) e la cui costante è 666, il *numero della Bestia* (S. Giovanni Apostolo, Apocalisse, cap. 13, vers.18).

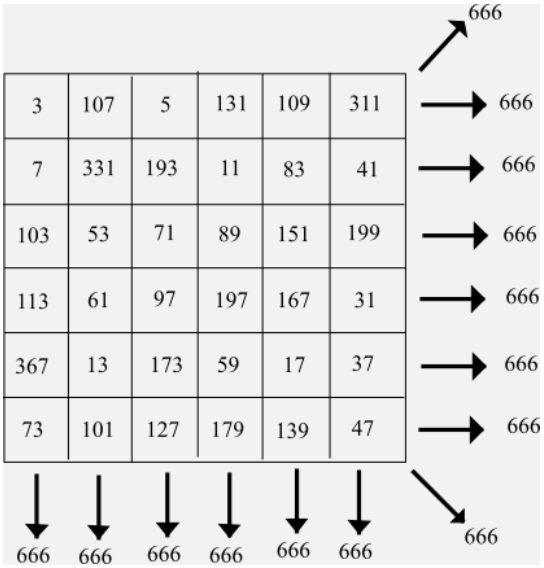


figura 2

Pickover lo definisce ***quadrato magico apocalittico*** e dichiara che è stato costruito da un non meglio identificato A. W. Johnson non si sa quando.

**5.** Si presenta, a questo punto, un problema interessante:

**Assegnato un qualsiasi numero naturale, come si fa a stabilire se è un numero primo?**

Si capisce che, se il numero assegnato non supera il maggiore dei numeri primi che compongono un dato elenco, la risposta è facile: se il numero si trova in quell'elenco è primo, altrimenti non lo è.

La difficoltà sorge se non disponiamo di un elenco di numeri primi o se il numero assegnato è più grande del maggiore dei numeri primi che costituiscono l'elenco di cui disponiamo.

Descrivo quello che, in base alle nostre conoscenze, potrebbe essere il primo procedimento idoneo a stabilire se un assegnato numero è primo o no.

Ovviamente è inutile prendere in considerazione i numeri pari, che certamente sono divisibili per 2 e pertanto non sono numeri primi, fatta eccezione naturalmente per il numero 2, che è l'unico numero ad essere contemporaneamente pari e primo.

Sia dunque N un numero naturale dispari. Intanto è certo che non è divisibile per alcun numero pari. Se allora esiste un numero naturale dispari, compreso fra 3 ed N−1, che divide N, allora N è un numero composto, altrimenti è primo.

In realtà, non occorre indagare su tutti i numeri dispari n compresi fra 3 ed N−1; basta fermarsi a $n=\sqrt{N}$. Questo perché i prodotti nq del numero n, con $n>\sqrt{N}$, per il quoziente q della divisione di N per n riproducono i fattori che si presentano nei prodotti nq ottenuti prendendo n minore di $\sqrt{N}$.

Per esempio, se $N=81$, per cui $\sqrt{N}=9$, per $n=3$ si ha $q=N:3=27$, dunque $N=3\times27$. Prodotto i cui fattori sono gli stessi fattori del prodotto $27\times3$, ottenuto prendendo $n=27$. Cosicché è inutile indagare su questo secondo valore. Insomma è sufficiente indagare fino al valore 9 di n.

Ecco allora una prima modalità per riconoscere se un dato numero è primo (*test di primalità*):

TEST DI PRIMALITÀ 1.

È dato il numero naturale dispari N. Se NON esiste alcun numero naturale dispari, compreso fra 3 e $\sqrt{N}$, che divide N, allora il numero N è un numero primo, altrimenti e un numero composto.

Vediamo un esempio.

Sia il numero $N=149$. Costatato che $\sqrt{149}\approx12{,}2$ è sufficiente indagare sui numeri dispari compresi fra 3 e 11, estremi inclusi.

Il numero non è divisibile per 3, poiché la somma delle sue cifre, cioè 14, non è divisibile per 3, e quindi non è divisibile neppure per 9. Non è divisibile per 5 poiché la cifra delle sue unità non è 0 né 5. Non è divisibile per 7: infatti 149 diviso per 7 dà quoziente 21 e resto 2. Non è divisibile per 11, poiché la differenza fra la somma delle sue cifre di posto dispari, a partire da destra, e quelle delle cifre di posto pari, cioè $(9+1)-4=6$, non è divisibile per 11. In definitiva, il numero 149 non è divisibile per alcuno dei numeri dispari compresi fra 3 e 11. Quindi è un numero primo.

Il test appena descritto va bene se abbiamo a che fare con numeri piuttosto "piccoli", ma se il numero sul quale dobbiamo indagare è "grande" il test non è più adatto.

Tanto per capirci, supponiamo di voler indagare sul numero $N=384.496.377.451$. Dopo aver calcolato, magari con il supporto di una calcolatrice, che $\sqrt{N}\approx620.077{,}7$ si tratterebbe di provare a dividere N per tutti i numeri dispari compresi fra 3 e 620.077: non è una passeggiata di salute, anche se si dispone di un computer.

Bisogna trovare altri test più efficaci.

Per la cronaca, il numero in questione è un numero composto. Si ha infatti:

$$384.496.377.451 = 367 \times 503 \times 2.082.851\,.$$

Alla ricerca di test di primalità efficaci si dedicarono i matematici a partire dal Seicento e abbiamo visto prima come siano riusciti a compilare elenchi comprendenti numeri primi molto grandi.

Noi descriveremo due test basati, uno sul "piccolo teorema di Fermat", l'altro sul "teorema di Wilson". In realtà, lo dico subito, i due test non risolvono il problema, ma danno un'idea riguardo a molte cose.

**6.** Del primo teorema ho avuto modo di occuparmi in un articolo pubblicato tempo fa su questa medesima rubrica, l'articolo *Dal romanzo* "*Gli artisti dei numeri – 2*". Mi limito pertanto ad enunciarlo.

PICCOLO TEOREMA DI FERMAT.

**Se p è un numero primo ed a è primo con p allora $a^{p-1} \equiv_p 1$ .**

Oppure, dopo aver moltiplicato entrambi i membri della congruenza per a ed aver sottratto a da entrambi i membri così ottenuti:

**Se p è un numero primo ed a è primo con p allora $a^p - a \equiv_p 0$ .**

Insomma, detto a parole:

**Se p è un numero primo ed a è primo con p allora il numero $a^p - a$ è divisibile per p.**

Allora, dati due numeri naturali a, p, primi fra loro, se risulta che il numero $a^p - a$ è divisibile per p, il teorema assicura che p è un numero primo ?

NO, la risposta è NO, nel senso che il numero p può essere primo ma può non esserlo.

Questo perché il teorema, rispetto alla primalità di p, fornisce solo una *condizione necessaria*; vale a dire che, se p è primo ed a è primo con p, allora certamente $a^p - a$ è divisibile per p.

Ma non è una *condizione sufficiente*; vale a dire che, se a e primo con p e $a^p - a$ è divisibile per p, allora non è certo che p sia primo: può esserlo e può non esserlo.

Chiariamo questo secondo aspetto con un paio di esempi:

- Considerati i numeri a=3 e p=7, primi fra loro, risulta $3^7 - 3 = 2.349 - 3 = 2.346$. Questo numero è divisibile per 3 e 7 è un numero primo.
- Considerati i numeri a=3 e p=8, primi fra loro, risulta $3^8 - 3 = 7.047 - 3 = 7.044$. Questo numero è divisibile per 3, ma 8 non è un numero primo.

Detto questo, il piccolo teorema di Fermat, o meglio il suo contronominale, fornisce un criterio per stabilire se, sotto speciali condizioni, un dato numero è composto. Enunciamo allora il contronominale del piccolo teorema di Fermat:

**Dati due numeri naturali a, p, primi fra loro, se risulta che il numero $a^p - a$ NON è divisibile per p, allora il numero p è un numero composto.**

Non è un vero e proprio test di primalità, ma aiuta.

Facciamo un esempio.

Considerati i numeri a=2 e p=15, primi fra loro, risulta $2^{15} - 2 = 32.768 - 2 = 32.766$. Questo numero non è divisibile per 15, dal che si conclude che 15 è un numero composto (cosa che ovviamente sapevano).

Ribadisco, comunque, che, sapere che $a^p - a$ è divisibile per p, non permette di concludere che p è un numero primo.

**7.** Occupiamoci adesso del teorema di Wilson.

Diciamo, per dovere di cronaca, che quello che al giorno d'oggi è denominato teorema di Wilson è in realtà una scoperta di uno scienziato arabo conosciuto in Occidente con il nome di Alhazen (965 circa – 1039), che lo enunciò intorno all'anno 1.000 ma senza dimostrarlo. Così come lo enunciarono, ma senza dimostrarlo, il matematico inglese Edward Waring (1736-1798) e lo stesso John Wilson (1741-1793), che fu suo allievo, anche se sembra che quest'ultimo ne abbia dato una dimostrazione parziale.

Chi diede una dimostrazione completa del teorema fu il matematico italo-francese Giuseppe Luigi Lagrange (1736-1813).

Questo è l'enunciato del teorema.

TEOREMA DI WILSON.

**Condizione necessaria e sufficiente affinché un numero p sia primo è che sia soddisfatta la seguente congruenza:**

$$(p-1)! + 1 \equiv_p 0 .$$

È possibile, come già detto, una dimostrazione completa del teorema. Ma per i nostri scopi basta dimostrare che la condizione è sufficiente ed è quello che faremo.

Dunque, bisogna dimostrare la seguente proposizione che, si può ben capire, fornisce un vero e proprio test di primalità:

TEST DI PRIMALITÀ 2.
**Dato un numero p>1, se il numero (p–1)!+1 è divisibile per p, allora p è un numero primo.**

DIMOSTRAZIONE.

Ragioniamo per assurdo, supponendo che p non sia primo. Deve essere dunque un numero composto, per cui ammette un divisore d tale che $1<d<p$. Ora, siccome $(p-1)!+1$ è, per ipotesi, divisibile per p, esso è ovviamente divisibile anche per d. Pertanto il numero d, che certamente è un fattore anche di $(p-1)!$, deve dividere pure 1. Il che è chiaramente assurdo.

Dunque, l'ipotesi fatta, che p sia non primo, è falsa. Essendo $p>1$, il numero p è pertanto un numero primo.

Ad onor del vero, il test non è molto pratico dal momento che i numeri che bisogna controllare crescono vertiginosamente attribuendo a p valori via via crescenti, come mostra d'altro canto la seguente tabella (tabella 2), costruita, *ça va sans dire*, con il supporto di uno strumento di calcolo automatico.

| p | (p–1)!+1 | Divisibile per p? | Esito circa la primalità di p |
|---|---|---|---|
| 2 | 2 | sì | primo |
| 3 | 3 | sì | primo |
| 4 | 7 | no | composto |
| 5 | 25 | sì | primo |
| 6 | 121 | no | composto |
| 7 | 721 | sì | primo |
| 8 | 5.041 | no | composto |
| 9 | 40.321 | no | composto |
| 10 | 362.881 | no | composto |
| 11 | 3.628.801 | sì | primo |
| 12 | 39.916.801 | no | composto |
| 13 | 479.001.601 | sì | primo |
| 14 | 6.227.020.801 | no | composto |
| 15 | 87.178.291.201 | no | composto |
| 16 | 1.307.674.368.001 | no | composto |
| 17 | 20.922.789.888.001 | sì | primo |
| 18 | 355.687.428.096.001 | no | composto |
| 19 | 6.402.373.705.728.001 | sì | primo |
| 20 | 121.645.100.408.832.001 | no | composto |

tabella 2

In essa sono presi in considerazione tutti i numeri da 2 a 20, compresi quelli che sappiamo essere composti come i numeri pari, i numeri che terminano per 5 e i numeri la somma delle cui cifre è un numero divisibile per 3. D'altro canto, i numeri primi che vi sono elencati non hanno bisogno di test speciali per essere riconosciuti tali. Ebbene, li abbiamo elencati tutti, numeri primi e numeri composti, semplicemente per mostrare come funzioni il test, ma anche per evidenziare come, al crescere di p, la crescita dei valori assunti dall'espressione $(p–1)!+1$ risulti veramente vertiginosa.

**8.** Test di primalità efficaci richiedono, oltre al supporto di potenti software matematici, il ricorso a concetti che esulano dai nostri piani. Comunque, non ce ne occupiamo.

Mi sembra tuttavia interessante riportare al riguardo un brano tratto da [2, pag. 133]:

«Attualmente gli algoritmi che si usano per determinare se un numero qualunque è primo sono di due tipi: polinomiale deterministico e polinomiale probabilistico.

«Il primo garantisce in modo assoluto che si tratta di un numero primo, però il tempo di elaborazione è alto. Il secondo è più rapido, però presenta una certa aleatorietà nel risultato».

Nonostante il risultato sia aleatorio, quello più usato è il secondo metodo, proprio perché richiede un minor tempo di elaborazione.

Bisogna dire comunque che entrambe le tipologie sono basate su generalizzazioni del piccolo teorema di Fermat.

BIBLIOGRAFIA.


[1] Luis Fernando Areán Álvarez, *Fermat*, collana Geni della Matematica, Milano, RBA Italia, 2017.

[2] Enrique Gracián, *I numeri primi*, Milano, Mondo Matematico, 2018.

[3] Euclide, *Gli Elementi* (a cura di A. Frajese e L. Maccioni), Torino, UTET, 1970.

[4] Clifford Pickover, *La magia dei numeri*, Milano, RBA Italia, 2008.

[5] Wikipedia, libera enciclopedia on-line.