i*Quaderni* della CMSI

Piero Antognini

I numeri primi e i numeri perfetti

CMSI
Commissione di Matematica della Svizzera Italiana

Ho impostato queste lezioni seguendo due principi:

- nessuna conoscenza particolare di matematica
- interazione continua della matematica con la storia dell'uomo

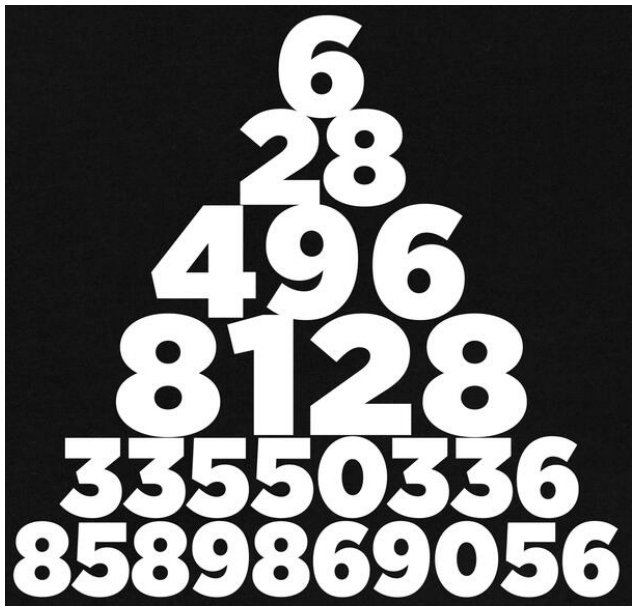
Motivazione

Perché parlare di numeri primi?

I numeri primi sono ciò che rimane una volta eliminati tutti gli schemi: penso che i numeri primi siano come la vita. Sono molto logici ma non si riesce mai a scoprirne le regole, anche se si passa tutto il tempo a pensarci su. (Haddon [2003])

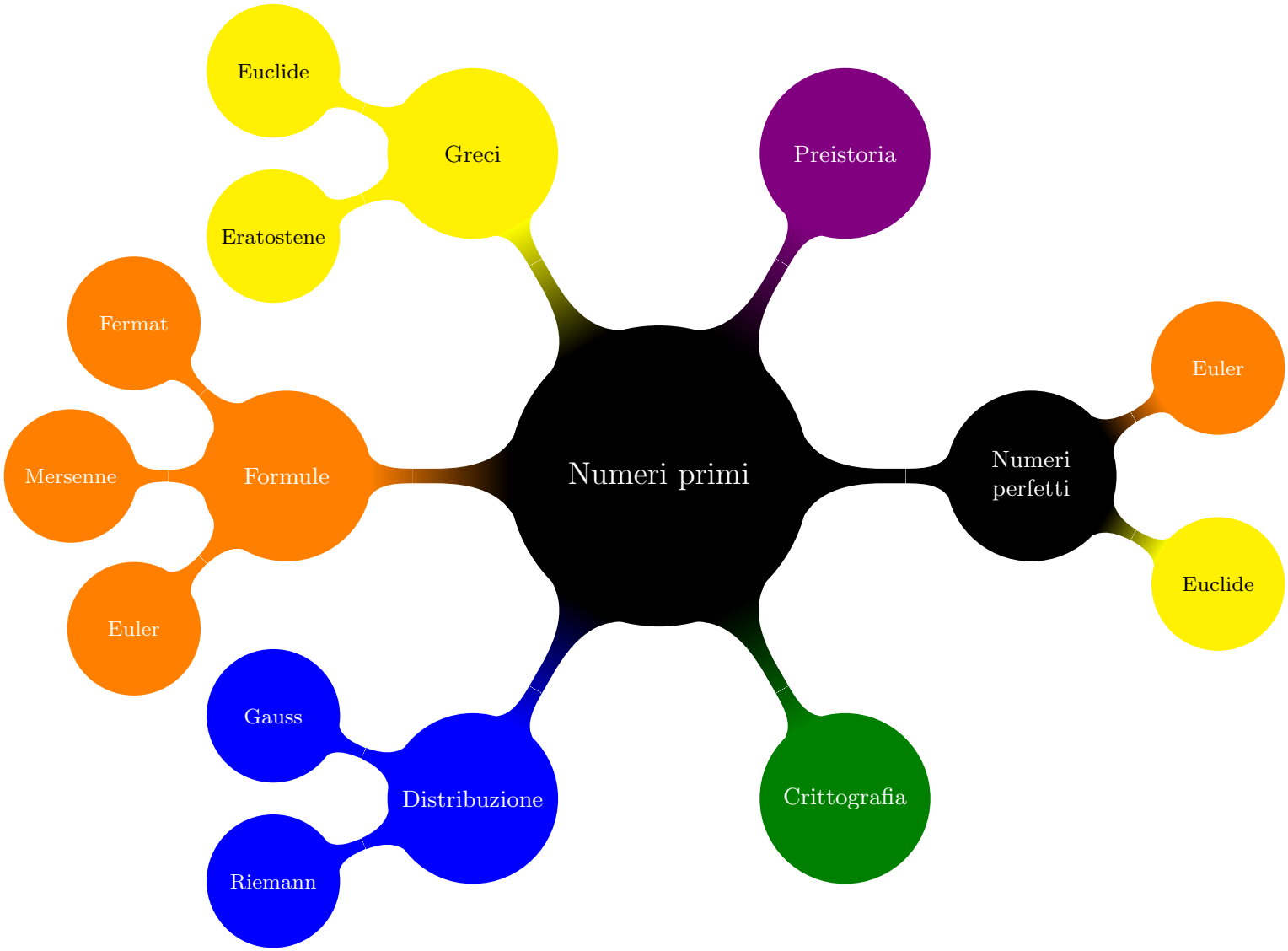
Motivazione

E di numeri perfetti?



L'attribuzione di proprietà mistiche o magiche ai numeri è frequente presso molte culture. Sia nella Grecia classica sia in periodi anteriori, l'idea di perfezione venne in qualche modo associata a quei numeri interi che risultano uguali alla somma dei loro divisori. (Weil [1984])

Struttura


Numeri primi
Greci
Euclide
Eratostene
Preistoria
Formule
Fermat
Mersenne
Euler
Numeri perfetti
Euler
Euclide
Distribuzione
Gauss
Riemann
Crittografia

Natura e preistoria

Cicale Magicicada:
cicli vitali di 13 e 17 anni.

Osso di Ishango (18-20'000 a.C.):
tacche con i numeri 11, 13, 17, 19.

Nascita dello spirito matematico

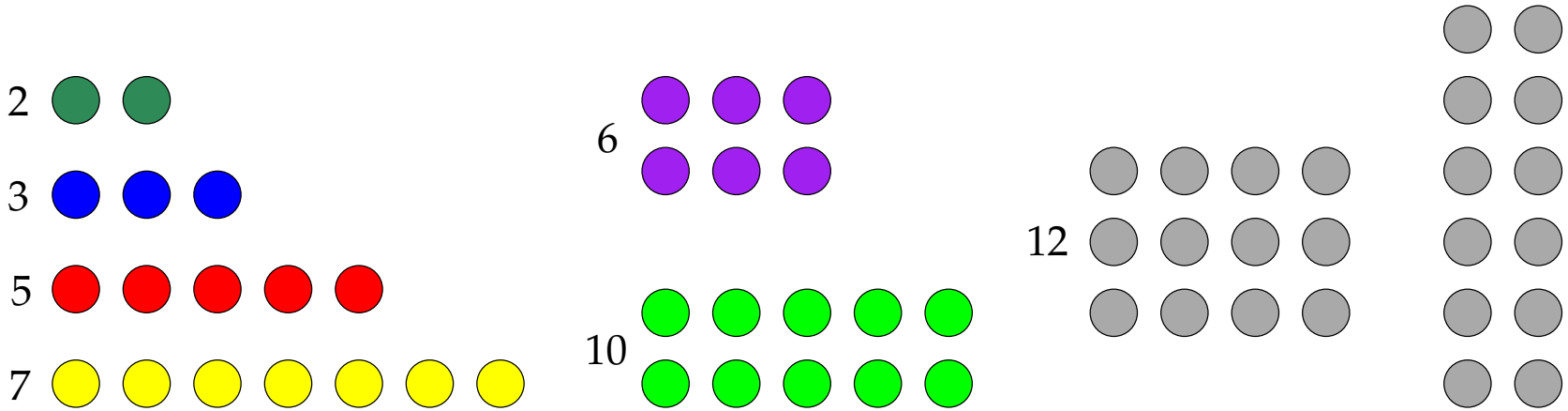
- Tra il 600 e il 300 a.C. in Grecia si sviluppa il ragionamento deduttivo.
- I pitagorici procedono ad una prima classificazione dei numeri, distinguendo fra numeri pari e dispari.

Euclide (IV–III secolo a.C.)

Raffaello Sanzio (1483–1520), *Euclide e i suoi allievi*,
particolare dalla *Scuola di Atene*, 1509–1511, Stanze vaticane.

- Negli *Elementi* dedica tre dei tredici libri all'aritmetica, in particolare ai numeri primi.

Interpretazione geometrica di numeri primi e composti



- I numeri **solo** rettilinei si dicono *numeri primi*.
- I numeri rettangolari si dicono invece *numeri composti*.

Teorema fondamentale dell'aritmetica

Ogni numero naturale (diverso da 1*) o è primo o si può esprimere in un solo modo (se si prescinde dall'ordine dei fattori) come prodotto di numeri primi.*

- Esistenza: Euclide, *IX Elementi*
- Unicità: Carl Friedrich Gauss, *Disquisitiones Arithmeticae* (1798)

Infinità dei numeri primi

Proposizione 20 del IX libro degli *Elementi*:

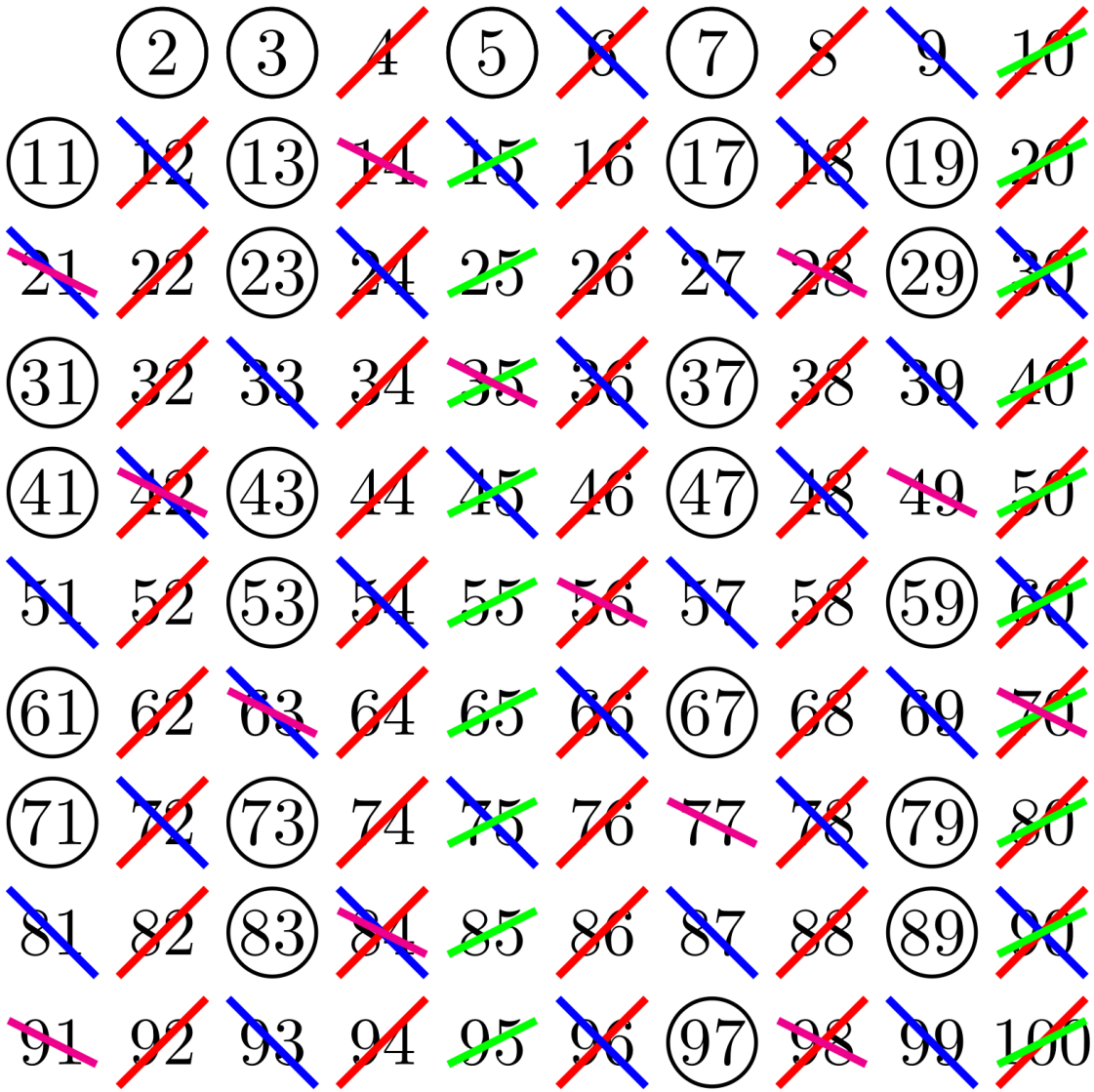
> *I numeri primi sono in quantità maggiore di qualsiasi numero prefissato di numeri primi.*

La dimostrazione viene quasi sempre presentata in classe come primo esempio di *reductio ad absurdum*.

Eratostene (276–194 a.C.)

Bernardo Strozzi (1581–1644), *Eratostene mentre insegna ad Alessandria*, 1635, Montreal, Museum of Fine Arts.

Crivello di Eratostene



Pierre de Fermat (1601–1665) e Leonhard Euler (1707–1783)

Numeri di Fermat

$$\mathcal{F}_n = 2^{2^n} + 1$$

Fermat fornisce questi numeri fino a $n = 6$:

$$\mathcal{F}_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$$

$$\mathcal{F}_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$$

$$\mathcal{F}_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$$

$$\mathcal{F}_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$

$$\mathcal{F}_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65'537$$

$$\mathcal{F}_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4'294'967'297$$

$$\mathcal{F}_6 = 2^{2^6} + 1 = 2^{64} + 1 = 18'446'744'073'709'551'617$$

e congettura che siano tutti numeri primi.

Confutazione di Eulero

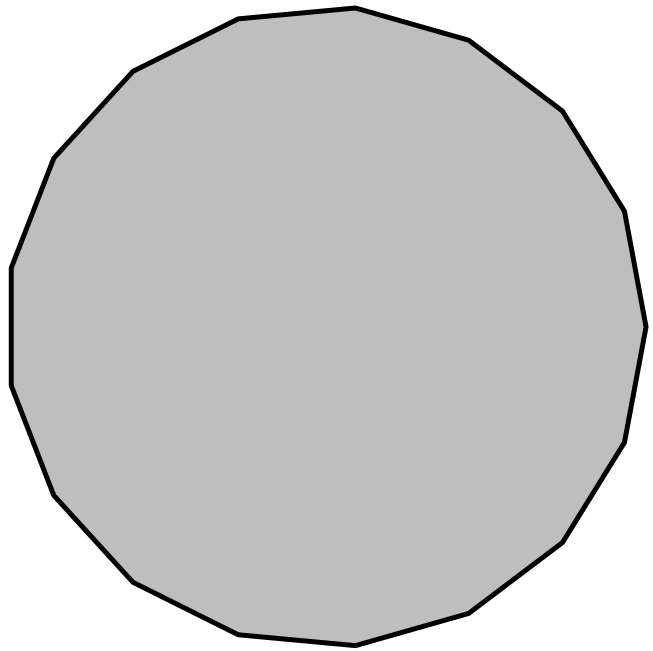
Eulero (1732) mostra che la congettura di Fermat è falsa:

$$\mathcal{F}_5 = 2^{32} + 1 = 641 \cdot 6'700'417.$$

Attualmente non è stato trovato nessun altro numero di Fermat primo.

Curiosità: costruzione dei poligoni regolari

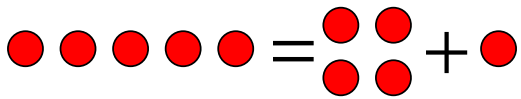
- Gauss nel 1796 costruisce con riga e compasso il poligono regolare di 17 lati.

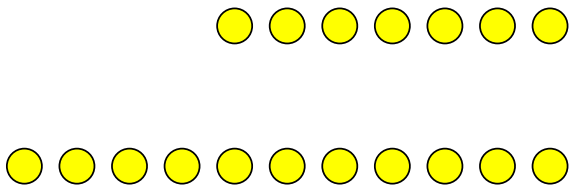


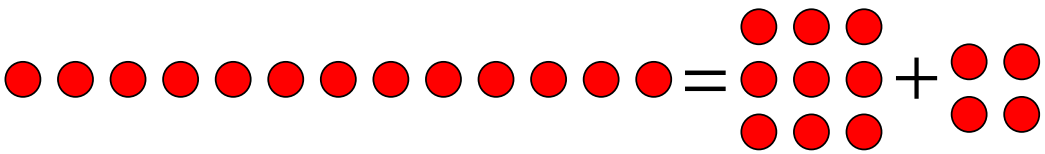
- E dimostra che i fattori primi dispari del numero dei lati di un poligono costruibile sono i numeri primi di Fermat (presi una sola volta!).

Teorema di Natale

(Fermat, 25 dicembre 1640, dim. Euler 1749)







Ogni numero primo della forma $4k+1$ può esser espresso in un solo modo come somma di due quadrati.
Nessun numero primo della forma $4k+3$ può essere espresso come somma di due quadrati.

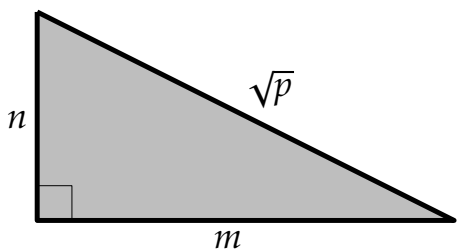
Legame con Pitagora

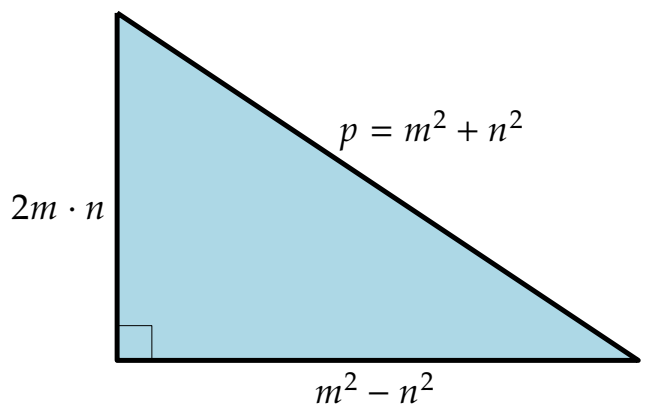
Esercizio

Se un numero dispari (primo) è la somma di due quadrati allora deve avere la forma $4k + 1$.

Esercizio

Se per un numero (primo) p vale $p = m^2 + n^2$, allora $2mn$, $m^2 - n^2$ e p costituiscono una terna pitagorica.





Numeri di Mersenne

Padre Marin Mersenne (1588–1648) studiò i numeri della forma

$$\mathcal{M}_p = 2^p - 1$$

in cui p è un numero primo.

Esercizio

Se n non è primo anche $2^n - 1$ non è primo.

Numeri primi di Mersenne

- Mersenne afferma (1644) che $\mathcal{M}_p$ è primo per

$$p = 2,\ \ 3,\ \ 5,\ \ 7,\ \ 13,\ \ 17,\ \ 19,\ \ 31,\ \ 67,\ \ 127,\ \ 257$$

  e non lo è per nessun altro esponente primo fino a 257.

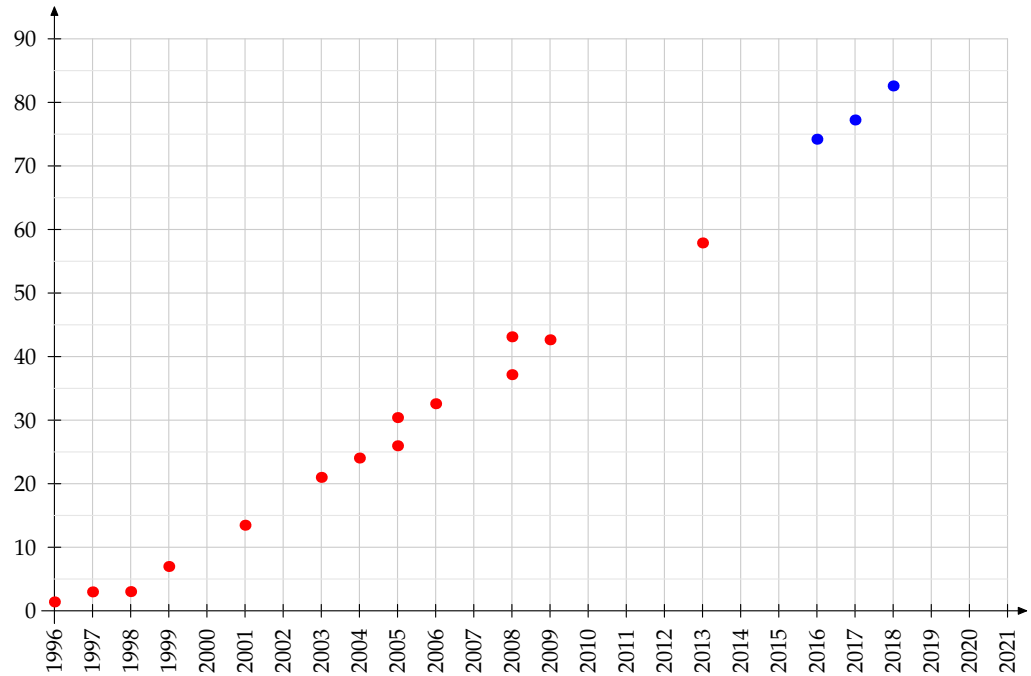
- Commette cinque errori (trovati nell'arco di tre secoli!):
  - $\mathcal{M}_{67}$ e $\mathcal{M}_{257}$ non sono primi
  - nella lista mancano $\mathcal{M}_{61}, \mathcal{M}_{89}$ e $\mathcal{M}_{107}$

- Celebre la dimostrazione di Nelson Cole (1903) della scomposizione di $2^{67} - 1$:

$$\begin{aligned} 2^{67} - 1 &= 147'573'952'589'676'412'927 \\ &= 193'707'721 \cdot 761'838'257'287 \end{aligned}$$

Numeri primi di Mersenne oggi

- Grazie al progetto GIMPS (*Great Internet Mersenne Prime Search*) sono stati trovati 51 primi di Mersenne, i primi 48 nell'ordine crescente corretto.



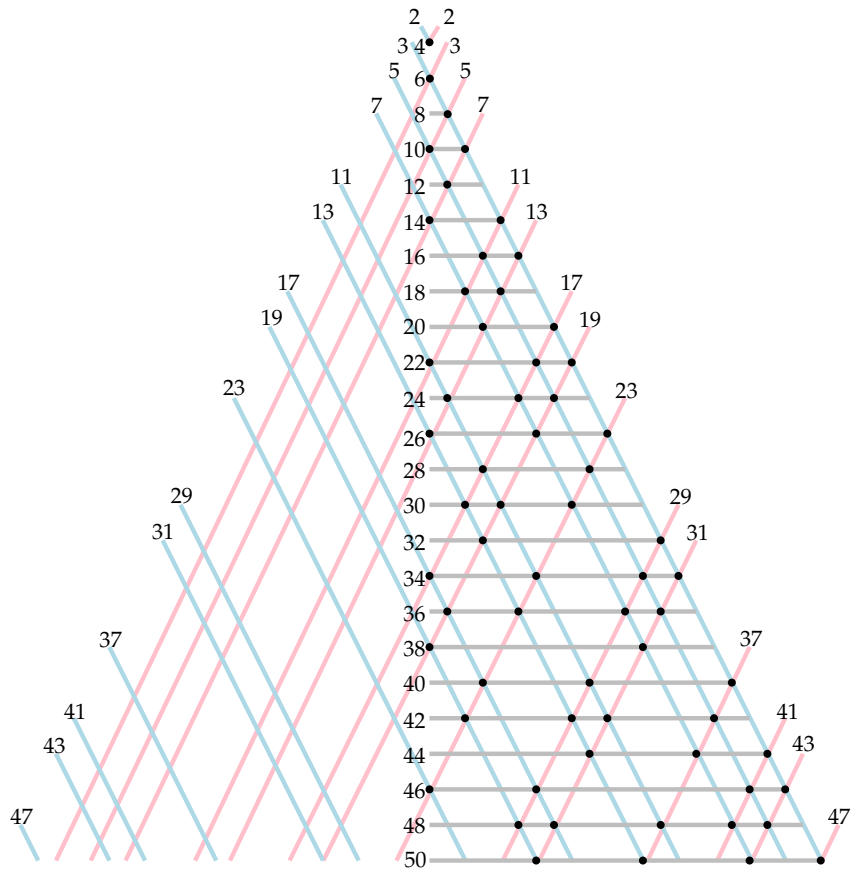
- L'ultimo numero, scoperto il 7 dicembre 2018,

$$\mathcal{M}_{82'589'933} = 2^{82'589'933} - 1$$

costituisce attualmente il più grande numero primo noto.

Congettura di Goldbach (1742)

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



Numeri primi gemelli

- Due numeri primi la cui differenza è 2 vengono dunque detti *numeri primi gemelli*.
- Rimane irrisolta la questione se le coppie di numeri primi gemelli siano infinite.

Esercizio

Se $p > 3$ e $p+2$ sono numeri primi gemelli, allora $p+1$ deve essere divisibile per 6.

Numeri primi di Eulero

$$p(n) = n^2 + n + 41 \qquad (n \in \mathbb{N})$$

- I primi 40 numeri sono primi: $41, 43, 47, \ldots, 1601$.
- Ma per $n = 40$ e $n = 41$ si ottengono numeri composti:

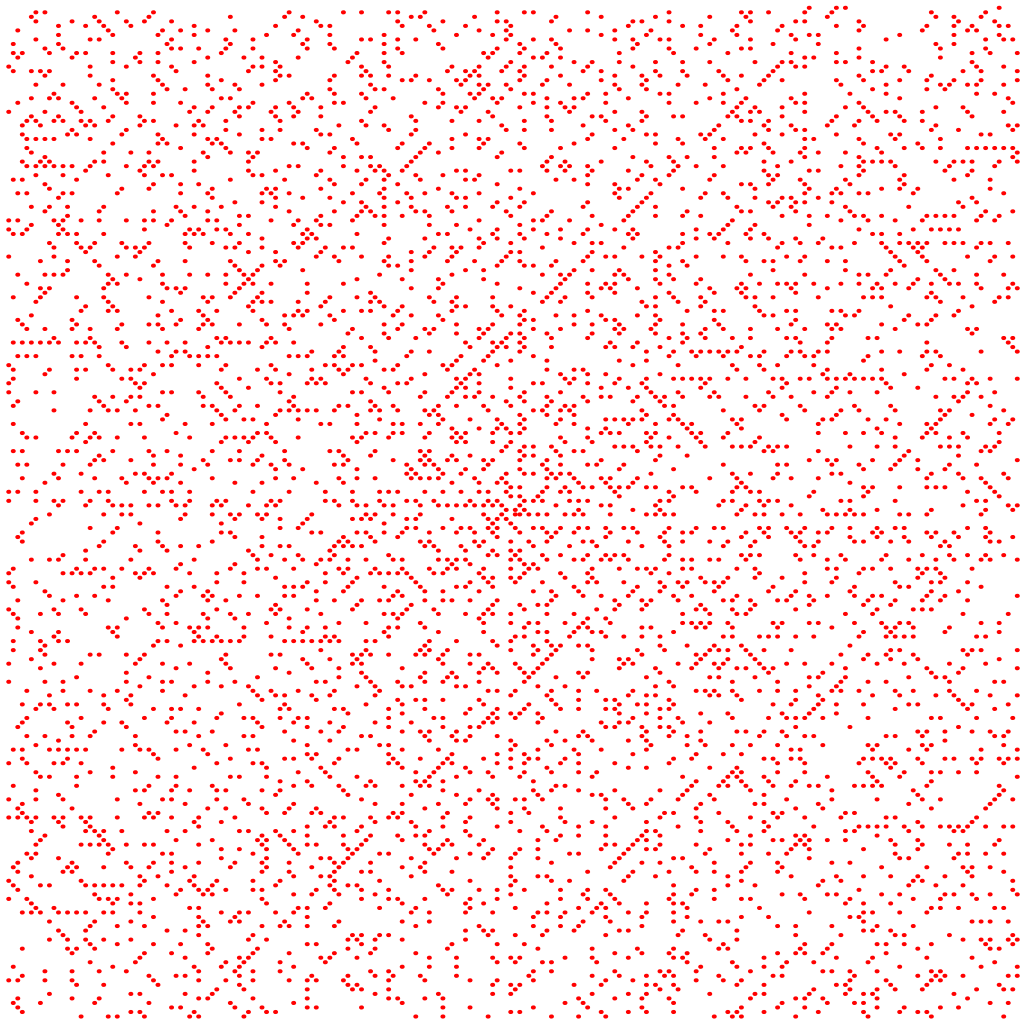
$$p(40) = 40^2 + 40 + 41 = 40 \cdot (40 + 1) + 41 = 41 \cdot 41$$
$$p(41) = 41^2 + 41 + 41 = 41 \cdot 41 + 41 \cdot 2 = 41 \cdot 43$$

- Questa formula è un'ottima generatrice di numeri primi: procedendo fino a $n = 10^7$ si ottengono numeri primi con una percentuale del 47.5%.

Spirale di Ulam (1963)

101	100	99	98	97	96	95	94	93	92	91
102	65	64	63	62	61	60	59	58	57	90
103	66	37	36	35	34	33	32	31	56	89
104	67	38	17	16	15	14	13	30	55	88
105	68	39	18	5	4	3	12	29	54	87
106	69	40	19	6	1	2	11	28	53	86
107	70	41	20	7	8	9	10	27	52	85
108	71	42	21	22	23	24	25	26	51	84
109	72	43	44	45	46	47	48	49	50	83
110	73	74	75	76	77	78	79	80	81	82
111	112	113	114	115	116	117	118	119	120	121

Spirale di Ulam



I puntini rossi sono i 5′133 numeri primi in una spirale di numeri naturali da 1 a 50′000.

Carl Friedrich Gauss (1777–1855)

Appena quindicenne, Gauss, studiandone la distribuzione, formula il teorema dei numeri primi.

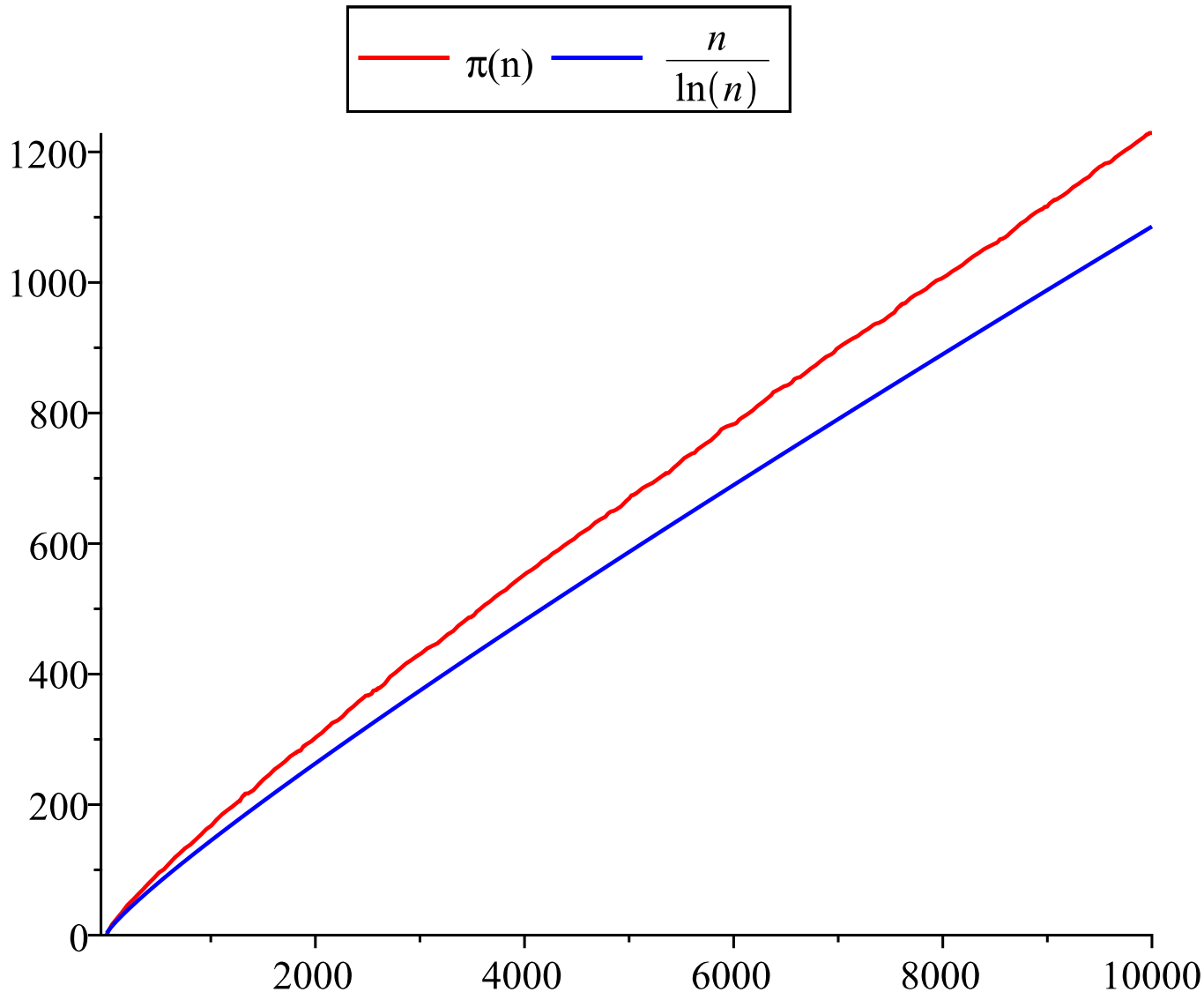
Teorema dei numeri primi

n	$\pi(n)$	$n/\pi(n)$
10	4	2.5
100	25	4.0
$1'000$	168	6.0
$10'000$	$1'229$	8.1
$100'000$	$9'592$	10.4
$1'000'000$	$78'498$	12.7
$10'000'000$	$664'579$	15.0
$100'000'000$	$5'761'455$	17.4
$1'000'000'000$	$50'847'534$	19.7
$10'000'000'000$	$455'055'511$	22.0

$$\frac{n}{\pi(n)} \sim \ln(n) \qquad \text{da cui} \qquad \pi(n) \sim \frac{n}{\ln n}$$

- Dimostrato solo nel 1896 in modo indipendente da Jacques Hadamard e Charles Jean de la Vallée-Poussin.

Teorema dei numeri primi



Deserto di numeri primi

Esercizio

Scelto un valore n, determinare una successione di n numeri consecutivi che siano tutti composti.

Soluzione. Il numero

$$2 \cdot 3 \cdot \ldots \cdot n \cdot (n+1) = (n+1)!$$

è multiplo di tutti i numeri da 2 a $n+1$, dunque

$$\begin{aligned}
&(n+1)!+2\\
&(n+1)!+3\\
&(n+1)!+4\\
&\vdots\\
&(n+1)!+n\\
&(n+1)!+(n+1)
\end{aligned}$$

sono gli n numeri composti cercati.

Bernhard Riemann (1826–1866)

Nel 1859 pubblica:

> *Über die Anzahl der Primzahlen unter einer gegebenen Grösse.*

L'ipotesi di Riemann

- Studia funzione ζ, prolungamento in campo complesso della funzione

$$\zeta(x) = 1 + \left(\frac{1}{2}\right)^x + \left(\frac{1}{3}\right)^x + \left(\frac{1}{4}\right)^x + \dots$$

- Ipotizza che:

> Tutti gli zeri non banali della funzione ζ nel piano complesso si trovano sulla retta verticale $x = \frac{1}{2}$.

L'ipotesi di Riemann

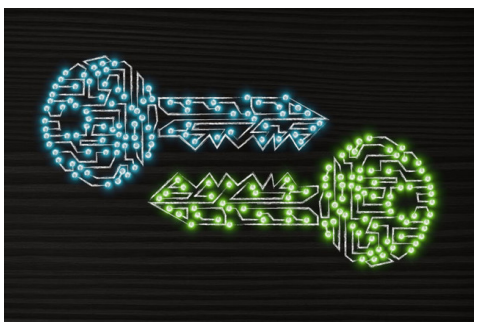
- L'ipotesi è collegata all'esistenza di una legge di regolarità nella distribuzione dei primi.

L'ipotesi di Riemann

- È l'ottavo dei 23 problemi proposti da Hilbert nel 1900 al congresso di Parigi e nel 2000 è stata inclusa nei sette problemi del millennio.
- Nonostante molte evidenze numeriche a favore, resta non dimostrata.

Crittografia

- Fino agli anni 70 *crittografia simmetrica*: mittente e destinatario utilizzano la stessa *chiave segreta* per cifrare e decifrare i messaggi.
- Verso la fine degli anni 70 vengono realizzati i primi sistemi di *crittografia asimmetrica*, in cui esistono due chiavi:
  - una *chiave pubblica* per cifrare (nota a tutti)
  - una *chiave privata* per decifrare (nota solo al destinatario)



RSA

Nel 1977 **R**ivest, **S**hamir, **A**dleman realizzano l'*algoritmo RSA*.

- La chiave privata è essenzialmente costituita da una coppia di numeri primi p e q (di almeno 100 cifre).
- La chiave pubblica è essenzialmente costituita dal prodotto $n = p \cdot q$.
- Per un computer, scomporre n in fattori primi può richiedere un tempo enorme.

Inutilità dei numeri primi

Nel 1940 Godfrey Hardy scriveva:

> *La 'vera' matematica [...] è quasi totalmente 'inutile' [...] Non è possibile giustificare la vita di nessun vero matematico sulla base dell''utilità' del suo lavoro. (Hardy [1940])*

E ancora:

> *C'è una conclusione facile e confortante per un vero matematico. La vera matematica non ha alcun effetto sulla guerra. Nessuno ha ancora scoperto un uso bellico della teoria dei numeri o della relatività, e sembra improbabile che se ne scopra uno ancora per molti anni. (Hardy [1940])*

Numeri perfetti

- Già i pitagorici (530 a.C.) associano l'idea di perfezione a un numero, come 6, che è somma delle sue parti.
- Nell'antichità si conoscono secondo Nicomaco di Gerasa (I secolo d.C.) quattro numeri perfetti:

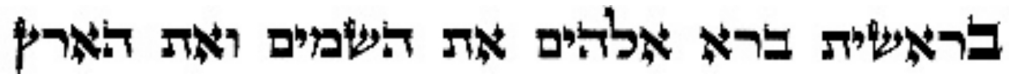
$$6 \qquad 28 \qquad 496 \qquad 8128$$

Significato simbolico di 6 e 28

- I primi commentatori dell'Antico Testamento utilizzano il significato matematico dei numeri perfetti come aiuto per l'interpretazione teologica.
- Ad esempio Sant'Agostino (354–430) nel *De Civitate Dei* scrive:

  A causa della perfezione del numero 6*, la Sacra Scrittura narra che la creazione è stata portata a termine in sei giorni. Dio avrebbe potuto creare tutte le cose insieme in un solo istante, e dispiegarle successivamente nel tempo, ma mediante il simbolismo del* 6 *ha voluto indicare la perfezione del creato. Il* 6 *infatti è il primo numero a completarsi con l'addizione delle proprie parti.*

- Il primo versetto della Genesi nel testo ebraico è costituito da 28 lettere.



(In principio Dio creò il cielo e la terra)

Numeri abbondanti e difettivi

- Un numero non perfetto è *abbondante* o *difettivo* se la somma dei divisori propri è rispettivamente maggiore o minore del numero stesso.

numero	somma dei divisori propri	tipo
1	0	difettivo
2	1	difettivo
3	1	difettivo
4	$1+2=3$	difettivo
5	1	difettivo
6	$1+2+3=6$	perfetto
7	1	difettivo
8	$1+2+4=7$	difettivo
9	$1+3=4$	difettivo
10	$1+2+5=8$	difettivo
11	1	difettivo
12	$1+2+3+4+6=16$	abbondante
13	1	difettivo
14	$1+2+7=10$	difettivo
15	$1+3+5=9$	difettivo
16	$1+2+4+8=15$	difettivo
17	1	difettivo
18	$1+2+3+6+9=21$	abbondante
19	1	difettivo
20	$1+2+4+5+10=22$	abbondante

- Circa tre quarti dei numeri sono difettivi, circa un quarto abbondanti, quasi nessuno è perfetto! (Deléglise, 1998)

Formula per i numeri perfetti pari

- Euclide nel libro IX degli *Elementi* fornisce una regola per il calcolo dei numeri perfetti, che conduce alla formula

$$(2^p - 1) \cdot 2^{p-1}$$

  in cui $2^p - 1$ deve essere primo, dunque un numero primo di Mersenne.
- Eulero dimostra nel XVIII secolo che questa è la sola formula per ottenere numeri perfetti pari.
- Ci sono dunque tanti numeri perfetti pari quanti numeri di Mersenne.
- Non si sa se esistano numeri perfetti dispari.

Da un numero di Mersenne a un numero perfetto

Esercizio

Se $2^p - 1$ è primo, allora $(2^p - 1) \cdot 2^{p-1}$ è perfetto, cioè è uguale alla somma dei suoi divisori propri.

Soluzione. I divisori propri sono

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

La loro somma è

$$\begin{aligned}
&\left(1 + 2 + 2^2 + \ldots + 2^{p-1}\right) + \left((2^p - 1) \cdot 1 + (2^p - 1) \cdot 2 + \ldots + (2^p - 1) \cdot 2^{p-2}\right) \\
&= (2^p - 1) + (2^p - 1) \cdot \left(1 + 2 + \ldots + 2^{p-2}\right) \\
&= (2^p - 1) \cdot 1 + (2^p - 1) \cdot \left(2^{p-1} - 1\right) \\
&= (2^p - 1) \cdot \left(1 + 2^{p-1} - 1\right) = (2^p - 1) \cdot 2^{p-1}
\end{aligned}$$

Numeri amici

- Secondo Pitagora:

  Amico è colui che è un altro me stesso, così come sono 220 *e* 284*.*

- 220 e 284 costituiscono la prima e più piccola coppia di *numeri amici*. Se si sommano tutti i divisori propri del primo numero si ottiene il secondo e viceversa.

- Attualmente si conoscono più di 1 miliardo e 227 milioni di coppie di numeri amici, spesso trovate con un progetto di calcolo distribuito (vedi `https://sech.me/ap/`).

Numeri socievoli

- I numeri $12'496$, $14'288$, $15'472$, $14'536$, $14'264$ costituiscono una *catena di numeri socievoli con cinque anelli*, cioè la somma dei divisori propri di ogni numero dà il seguente e sommando i divisori propri dell'ultimo si ottiene il primo.
- Numeri perfetti: catena con un solo anello.
- Numeri amici: catena con due anelli.
- Non è noto se esistano catene con tre anelli.
- Esiste una catena "perfetta" (con 28 anelli!) che inizia con $14'316$.

L'inafferrabile bellezza

Molte questioni relative a numeri primi e perfetti restano irrisolte. Questi numeri si ribellano ai ripetuti tentativi dei matematici di imbrigliarli in schemi.

Forse è proprio questo il loro fascino, la loro bellezza inafferrabile!

Da *Lodiamo i numeri primi* di Helen Spalding (1920–1991):

> *O inverosimili numeri primi,*
> *possano i cacciatori di formule*
> *a lungo affannarsi nell'astrazione,*
> *consumare la loro pazienza e*
> *ridursi a scheletri:*
> *restate anticonformisti, scomodi,*
> *fenomeni irriducibili*
> *a sistema, serie, schema*
> *o spiegazione.*

Grazie per l'attenzione

Roland Topor (1938–1997), *L'aritmetica*, disegno con penna e matite, 1978.

Citazioni

Mark Haddon. *Lo strano caso del cane ucciso a mezzanotte*. Einaudi, Torino, 2003.

Godfrey H. Hardy. *A Mathematician's Apology*. trad. it. Garzanti, Milano, 1940.

André Weil. *Number Theory*. trad. it. Einaudi, Torino, 1984.