Numeri primi

Alessandro Logar

Dipartimento di Matematica e Geoscienze
Università di Trieste

Problemi guida:

- Quanti sono i numeri primi?
- Come sono distribuiti?
- Come si trovano numeri primi “grandi”?

Problemi guida:

- Quanti sono i numeri primi?
- Come sono distribuiti?
- Come si trovano numeri primi “grandi”?

Problemi guida:

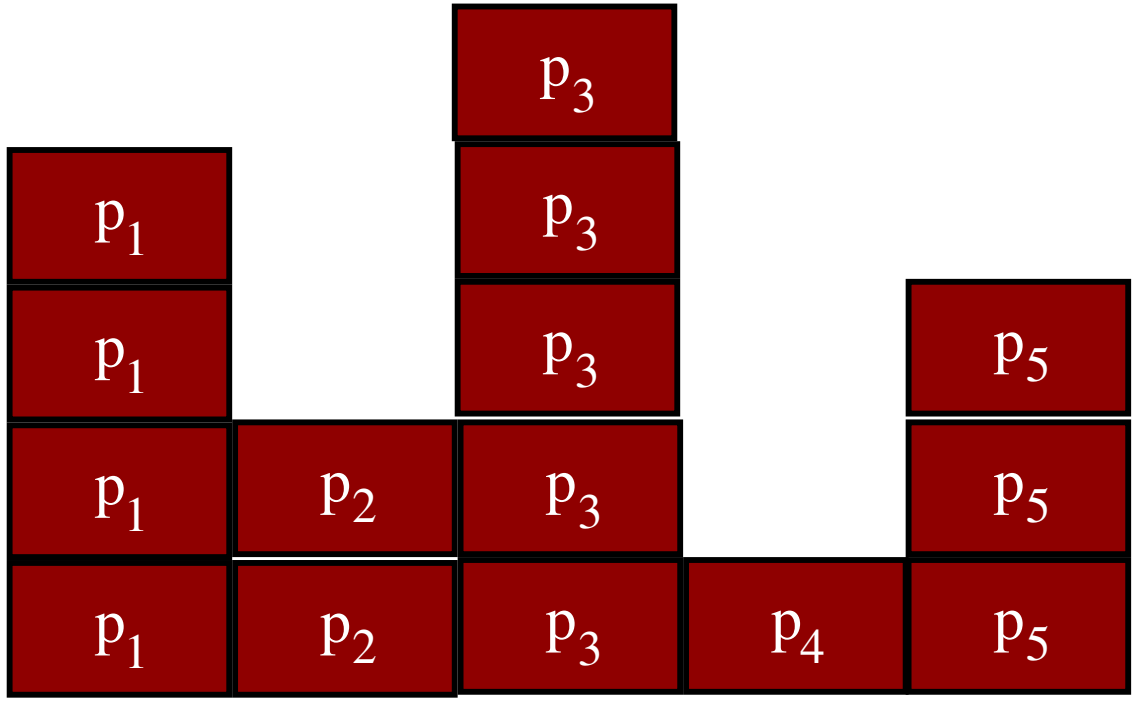
- Quanti sono i numeri primi?
- Come sono distribuiti?
- Come si trovano numeri primi “grandi”?

Ogni numero naturale è della forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

con $p_1, \ldots, p_k$ numeri primi.

$n =$



Euclide (circa 300 a.c.)

Euclide (libro IX, proposizione 20): i numeri primi sono infiniti.

Dimostrazione: Supponiamo siano finiti. Indichiamoli con $p_1, p_2, \ldots, p_k$. Consideriamo

$$N = p_1 \cdot p_2 \cdots p_k + 1$$

N deve essere un prodotto di numeri primi, quindi deve essere divisibile per qualche p_i. Allora p_i divide 1, assurdo.

Euclide (libro IX, proposizione 20): i numeri primi sono infiniti.

Dimostrazione: Supponiamo siano finiti. Indichiamoli con $p_1, p_2, \ldots, p_k$. Consideriamo

$$N = p_1 \cdot p_2 \cdots p_k + 1$$

N deve essere un prodotto di numeri primi, quindi deve essere divisibile per qualche p_i. Allora p_i divide 1, assurdo.

Euclide (libro IX, proposizione 20): i numeri primi sono infiniti.

Dimostrazione: Supponiamo siano finiti. Indichiamoli con $p_1, p_2, \ldots, p_k$. Consideriamo

$$N = p_1 \cdot p_2 \cdots p_k + 1$$

N deve essere un prodotto di numeri primi, quindi deve essere divisibile per qualche p_i. Allora p_i divide 1, assurdo.

Leonhard Euler (nato 1707, morto 1783)

“In Italia, sotto i Borgia, per trent’anni hanno avuto guerre, terrore, assassinii, massacri: e hanno prodotto Michelangelo, Leonardo da Vinci e il Rinascimento. In Svizzera, hanno avuto amore fraterno, cinquecento anni di pace e democrazia, e cos’hanno prodotto? Gli orologi a cucù.”

(Harry Lime - Orson Welles, Il terzo uomo, 1949)

“In Italia, sotto i Borgia, per trent’anni hanno avuto guerre, terrore, assassinii, massacri: e hanno prodotto Michelangelo, Leonardo da Vinci e il Rinascimento. In Svizzera, hanno avuto amore fraterno, cinquecento anni di pace e democrazia, e cos’hanno prodotto? Gli orologi a cucù.”

(Harry Lime - Orson Welles, Il terzo uomo, 1949)

Eulero dimostra che i numeri primi sono infiniti in un modo molto diverso...

Vale la seguente formula:

$$\sum_{n=1}^{+\infty} \frac{1}{n} = \prod_{p} \frac{1}{1 - 1/p}$$

e la formula si generalizza in:

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - 1/p^s}$$

(funzione ζ di Eulero).

Eulero dimostra che i numeri primi sono infiniti in un modo molto diverso...

Vale la seguente formula:

$$\sum_{n=1}^{+\infty} \frac{1}{n} = \prod_{p} \frac{1}{1 - 1/p}$$

e la formula si generalizza in:

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - 1/p^s}$$

(funzione ζ di Eulero).

Eulero dimostra che i numeri primi sono infiniti in un modo molto diverso...

Vale la seguente formula:

$$\sum_{n=1}^{+\infty} \frac{1}{n} = \prod_{p} \frac{1}{1 - 1/p}$$

e la formula si generalizza in:

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - 1/p^s}$$

(funzione ζ di Eulero).

Eulero dimostra che i numeri primi sono infiniti in un modo molto diverso...

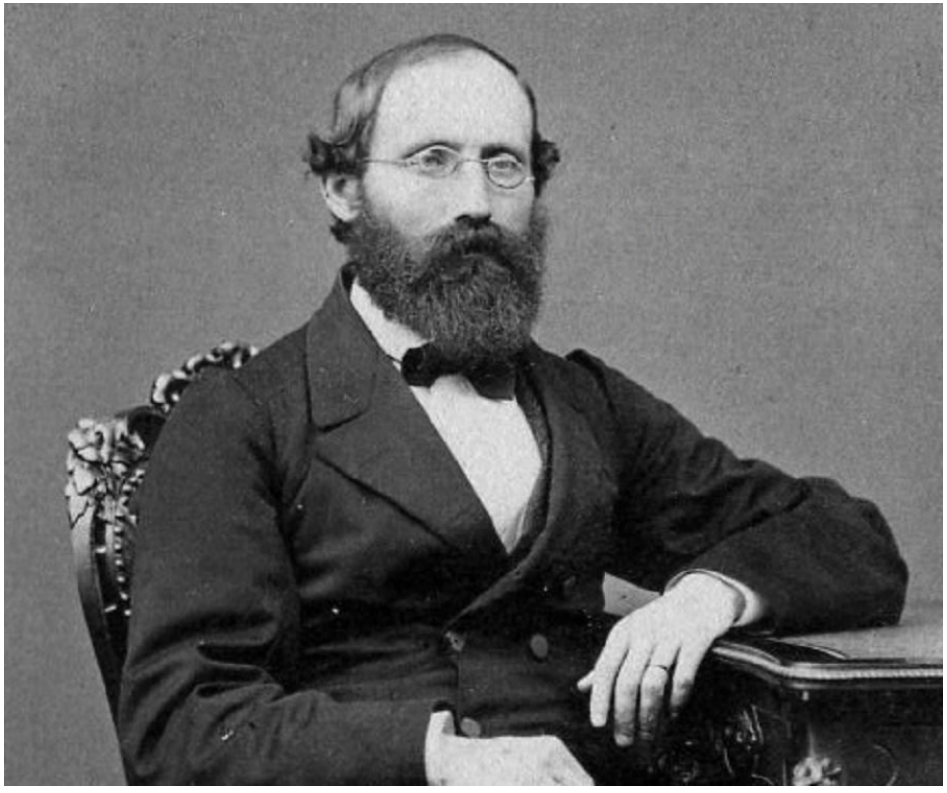
Vale la seguente formula:

$$\sum_{n=1}^{+\infty} \frac{1}{n} = \prod_{p} \frac{1}{1 - 1/p}$$

e la formula si generalizza in:

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - 1/p^s}$$

(funzione ζ di Eulero).



Bernhard Riemann (nato 1826, morto 1866).

Cenno di dimostrazione

$$a^n - b^n = (a-b) \cdot \left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \right)$$

$$a^n - 1 = (a-1) \cdot (a^{n-1} + a^{n-2} + \cdots + a + 1)$$

o, anche:

$$a^n + a^{n-1} + \cdots + a + 1 = \frac{a^{n+1} - 1}{a - 1}$$

Se $-1 < a < 1$ allora $a^{+\infty} = 0$, quindi:

$$1 + a + a^2 + a^3 + a^4 + a^5 + \cdots = \frac{1}{1-a}$$

Cenno di dimostrazione

$$a^n - b^n = (a-b) \cdot \left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \right)$$

$$a^n - 1 = (a-1) \cdot (a^{n-1} + a^{n-2} + \cdots + a + 1)$$

o, anche:

$$a^n + a^{n-1} + \cdots + a + 1 = \frac{a^{n+1} - 1}{a - 1}$$

Se $-1 < a < 1$ allora $a^{+\infty} = 0$, quindi:

$$1 + a + a^2 + a^3 + a^4 + a^5 + \cdots = \frac{1}{1-a}$$

Cenno di dimostrazione

$$a^n - b^n = (a-b) \cdot \left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \right)$$

$$a^n - 1 = (a-1) \cdot (a^{n-1} + a^{n-2} + \cdots + a + 1)$$

o, anche:

$$a^n + a^{n-1} + \cdots + a + 1 = \frac{a^{n+1} - 1}{a - 1}$$

Se $-1 < a < 1$ allora $a^{+\infty} = 0$, quindi:

$$1 + a + a^2 + a^3 + a^4 + a^5 + \cdots = \frac{1}{1-a}$$

In particolare, se p è un numero primo:

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \cdots = \frac{1}{1 - 1/p}$$

Siano p_1 e p_2 due numeri primi. Vale:

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) = \frac{1}{1 - 1/p_1} \cdot \frac{1}{1 - 1/p_2}$$

Però vale anche:

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) =$$

$$1 + \left(\frac{1}{p_1} + \frac{1}{p_2}\right) + \left(\frac{1}{p_1^2} + \frac{1}{p_1 p_2} + \frac{1}{p_2^2}\right) + \left(\frac{1}{p_1^3} + \frac{1}{p_1^2 p_2} + \frac{1}{p_1 p_2^2} + \frac{1}{p_2^3}\right) + \cdots$$

In particolare, se p è un numero primo:

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \cdots = \frac{1}{1 - 1/p}$$

Siano p_1 e p_2 due numeri primi. Vale:

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) = \frac{1}{1 - 1/p_1} \cdot \frac{1}{1 - 1/p_2}$$

Però vale anche:

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) =$$

$$1 + \left(\frac{1}{p_1} + \frac{1}{p_2}\right) + \left(\frac{1}{p_1^2} + \frac{1}{p_1 p_2} + \frac{1}{p_2^2}\right) + \left(\frac{1}{p_1^3} + \frac{1}{p_1^2 p_2} + \frac{1}{p_1 p_2^2} + \frac{1}{p_2^3}\right) + \cdots$$

In particolare, se p è un numero primo:

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \cdots = \frac{1}{1 - 1/p}$$

Siano p_1 e p_2 due numeri primi. Vale:

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) = \frac{1}{1 - 1/p_1} \cdot \frac{1}{1 - 1/p_2}$$

Però vale anche:

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) =$$

$$1 + \left(\frac{1}{p_1} + \frac{1}{p_2}\right) + \left(\frac{1}{p_1^2} + \frac{1}{p_1 p_2} + \frac{1}{p_2^2}\right) + \left(\frac{1}{p_1^3} + \frac{1}{p_1^2 p_2} + \frac{1}{p_1 p_2^2} + \frac{1}{p_2^3}\right) + \cdots$$

I numeri primi sono infiniti. . .

Definiamo la funzione

$$\pi(x) = \text{num. el. } \{p \mid p \text{ è primo e } p \leq x\}$$

I numeri primi iniziano con:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

quindi

$$\pi(2) = 1, \quad \pi(10) = 4, \quad \pi(48) = \pi(49) = \pi(50) = 15 \ldots$$

I numeri primi sono infiniti...

Definiamo la funzione

$$\pi(x) = \text{num. el. } \{p \mid p \text{ è primo e } p \leq x\}$$

I numeri primi iniziano con:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

quindi

$$\pi(2) = 1, \quad \pi(10) = 4, \quad \pi(48) = \pi(49) = \pi(50) = 15 \ldots$$

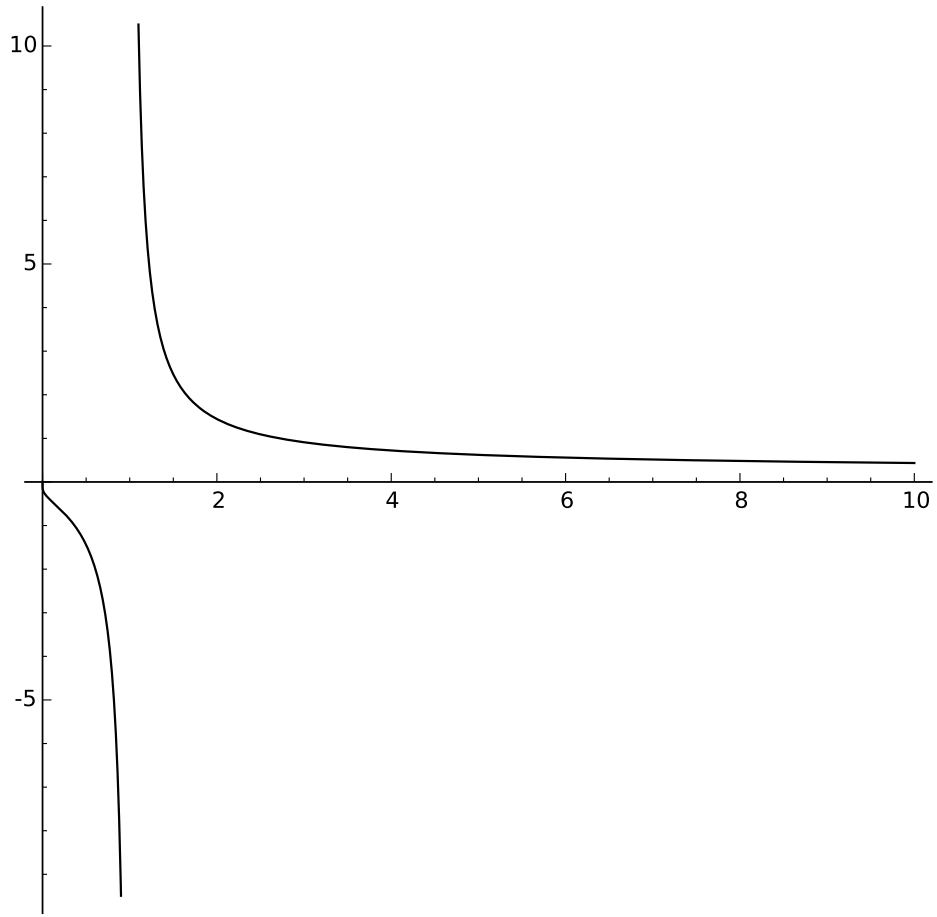
esempio sage (1)

Carl Friedrich Gauss (nato 1777, morto 1855)

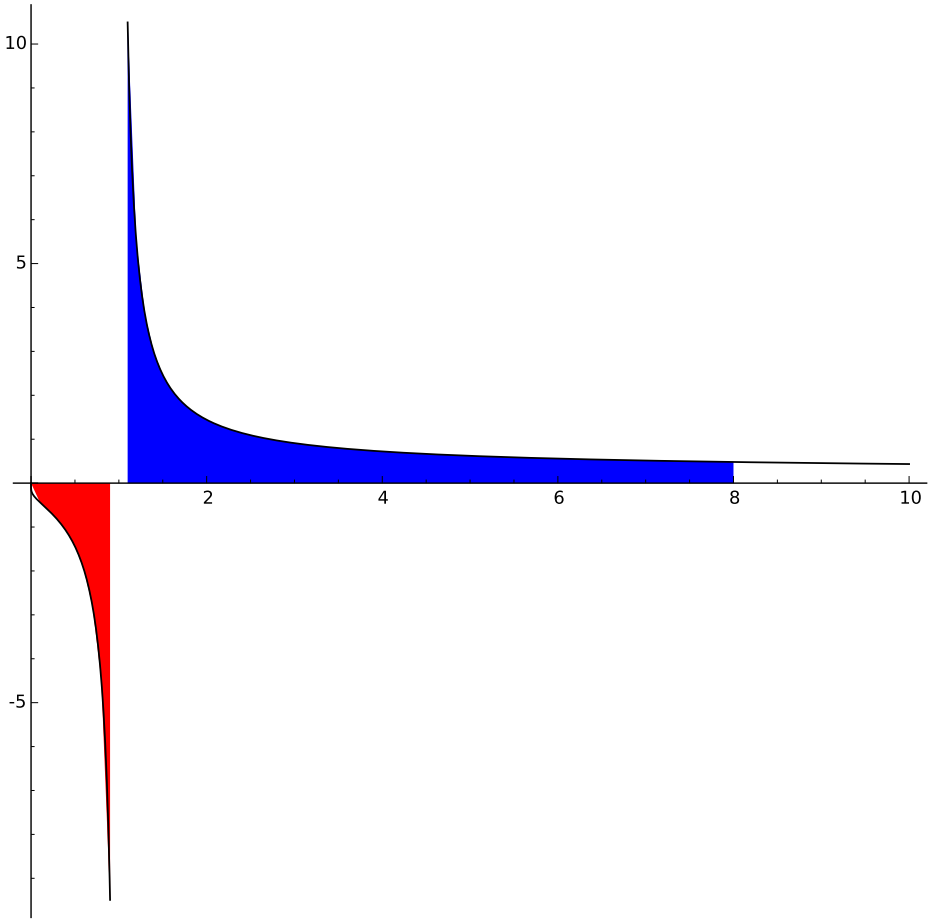
Teorema fondamentale dei numeri primi:

$$\frac{x}{\pi(x)} \simeq \log(x)$$

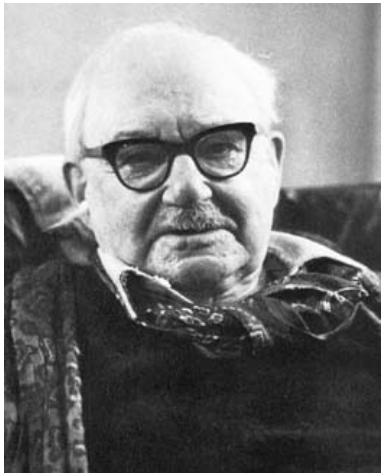
La funzione $f(x) = 1/\log(x)$:



La funzione $f(x) = \mathrm{li}(x)$ (logaritmo integrale):



esempio sage (2)



John Edensor Littlewood (nato 1885, morto 1977)

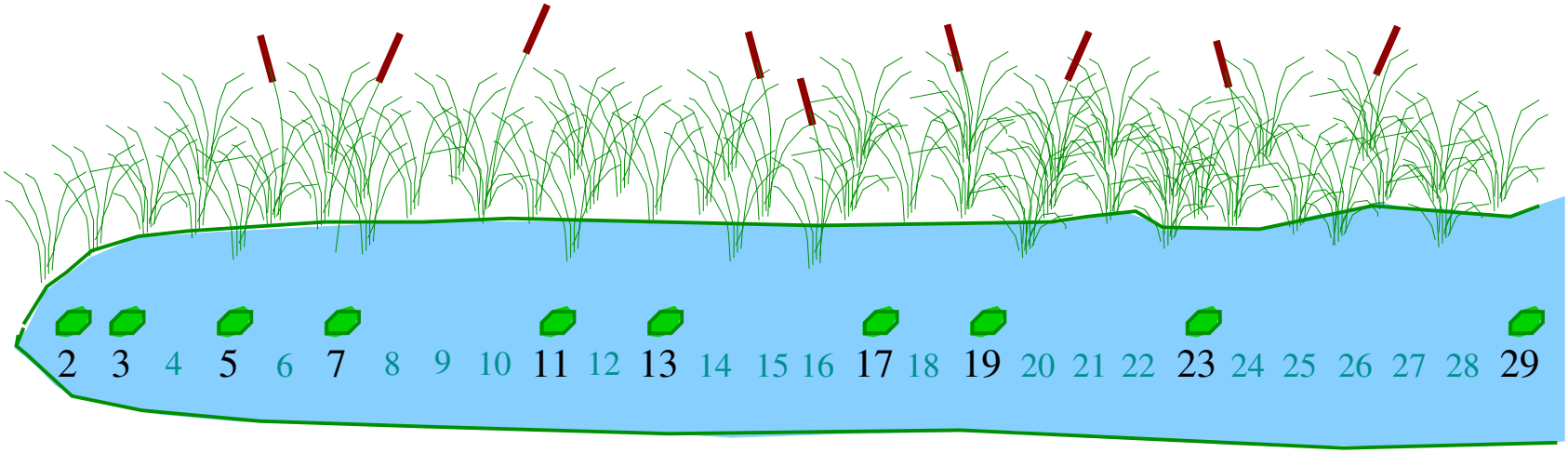
- Non è vero che $\mathrm{li}(x) > \pi(x)$ per ogni x.
- Ci sono infiniti valori di x per cui $\mathrm{li}(x) < \pi(x)$. Il più piccolo x per cui $\mathrm{li}(x)$ sta sotto $\pi(x)$ non si sa quanto valga.
- Si sa però che è inferiore a $e^{727.951346801}$ ($\simeq 1.4 \times 10^{316}$) (stima di Saouter e Demichel (2010) e Zegowitz (2010)) ed è superiore a 10^{19} (stima di Büthe del 2015).

- Non è vero che $\mathrm{li}(x) > \pi(x)$ per ogni x.
- Ci sono infiniti valori di x per cui $\mathrm{li}(x) < \pi(x)$. Il più piccolo x per cui $\mathrm{li}(x)$ sta sotto $\pi(x)$ non si sa quanto valga.
- Si sa però che è inferiore a $e^{727.951346801}$ ($\simeq 1.4 \times 10^{316}$) (stima di Saouter e Demichel (2010) e Zegowitz (2010)) ed è superiore a 10^{19} (stima di Büthe del 2015).

- Non è vero che $\mathrm{li}(x) > \pi(x)$ per ogni x.
- Ci sono infiniti valori di x per cui $\mathrm{li}(x) < \pi(x)$. Il più piccolo x per cui $\mathrm{li}(x)$ sta sotto $\pi(x)$ non si sa quanto valga.
- Si sa però che è inferiore a $e^{727.951346801}$ ($\simeq 1.4 \times 10^{316}$) (stima di Saouter e Demichel (2010) e Zegowitz (2010)) ed è superiore a 10^{19} (stima di Büthe del 2015).

Problema della rana:

In un lago (infinito) ci sono delle ninfee disposte sui numeri primi, come in figura. Il massimo salto che può fare una rana è di lunghezza k. La rana può raggiungere l'infinito saltando solo sulle ninfee?



La distanza tra due primi consecutivi può quindi essere grande quanto si vuole.

Stesso problema negli interi di Gauss: irrisolto.

La distanza tra due primi consecutivi può quindi essere grande quanto si vuole.
Stesso problema negli interi di Gauss: irrisolto.

. . . La distanza tra due primi consecutivi può quindi essere grande quanto si vuole.

Ci sono però primi che distano tra loro il meno possibile:

$$3, 5, \quad 5, 7, \quad 11, 13, \quad 17, 19, \ldots$$

Questi si chiamano primi gemelli.

. . . La distanza tra due primi consecutivi può quindi essere grande quanto si vuole.
Ci sono però primi che distano tra loro il meno possibile:

$$3, 5, \quad 5, 7, \quad 11, 13, \quad 17, 19, \ldots$$

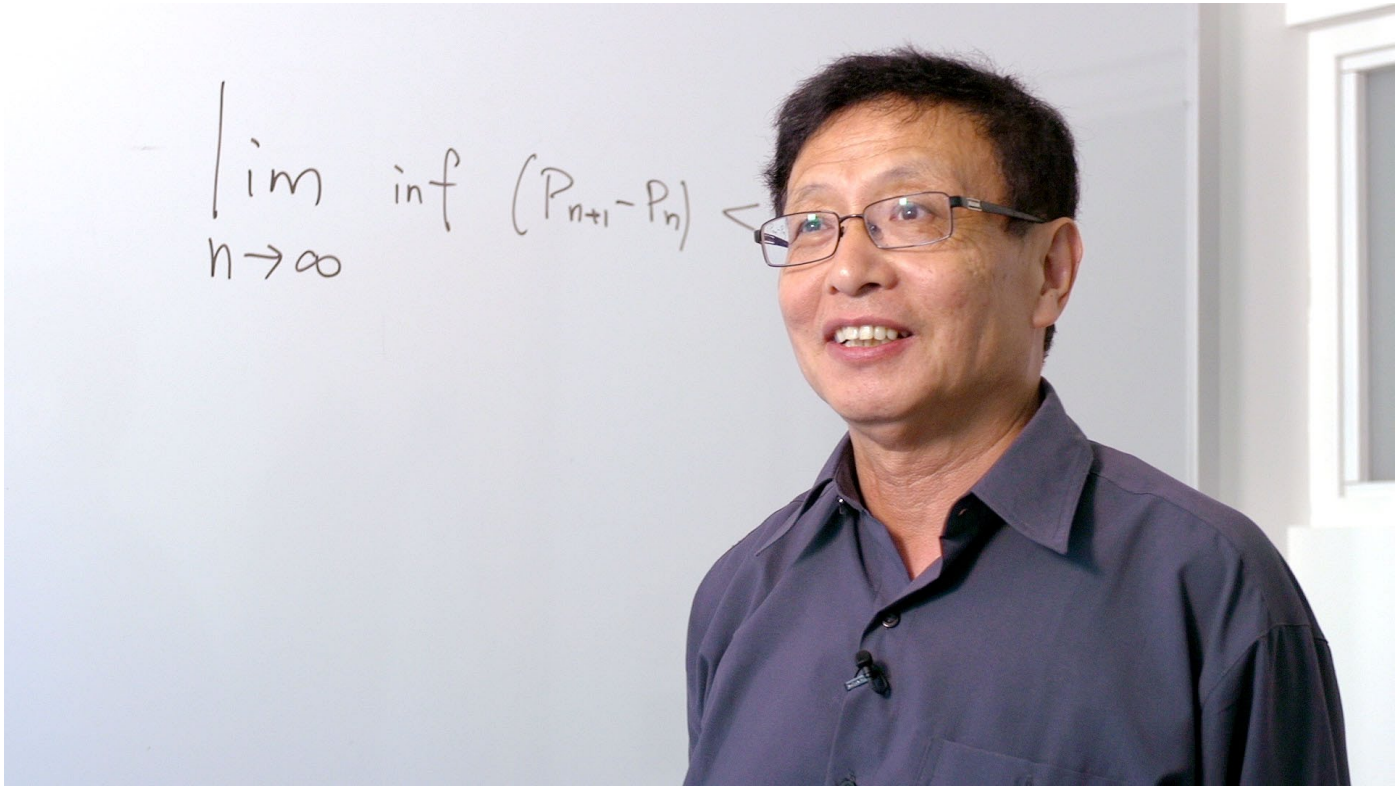
Questi si chiamano primi gemelli.

esempi sage (3)

I numeri primi gemelli sono infiniti? Problema irrisolto da secoli (forse proposto da Euclide).

Però. . . In questi anni il problema scricchiola. . .

I numeri primi gemelli sono infiniti? Problema irrisolto da secoli (forse proposto da Euclide).
Però. . . In questi anni il problema scricchiola. . .



Yitang Xhang (nato 1955, –)

Yitang Zhang ha dimostrato nel 2013 che ci sono infiniti primi che distano al massimo 70 milioni.

Nell'ambito del progetto Polymath, si è dimostrato (nel 2014) che ci sono infiniti primi a distanza 246.

Polymath è stato fondato da Timothy Gowers.

Yitang Zhang ha dimostrato nel 2013 che ci sono infiniti primi che distano al massimo 70 milioni.
Nell'ambito del progetto Polymath, si è dimostrato (nel 2014) che ci sono infiniti primi a distanza 246.
Polymath è stato fondato da Timothy Gowers.

Yitang Zhang ha dimostrato nel 2013 che ci sono infiniti primi che distano al massimo 70 milioni.
Nell'ambito del progetto Polymath, si è dimostrato (nel 2014) che ci sono infiniti primi a distanza 246.
Polymath è stato fondato da Timothy Gowers.

William Timothy Gowers (nato 1963, –)

I primi trigemini:

$$3, 5, 7$$

sono tre primi consecutivi (gemelli trigemini). Esistono altri primi gemelli trigemini?

I primi trigemini:

$$3, 5, 7$$

sono tre primi consecutivi (gemelli trigemini). Esistono altri primi gemelli trigemini?

Il problema dei primi gemelli rientra in un elenco di 4 famosi problemi riproposti nel 1912 (ad un congresso di matematica a Cambridge) dal matematico tedesco Edmund Landau.

Edmund Landau (nato 1877, morto 1938)

I 4 problemi riproposti da Landau:

1. La congettura di Goldbach (1742): ogni numero pari > 2 è somma di due primi;
2. La congettura dei primi gemelli (Euclide?);
3. La congettura di Legendre (~ 1800): esiste sempre almeno un numero primo tra n^2 e $(n+1)^2$, qualunque sia $n \in \mathbb{N}$.
4. Quinta congettura di Hardy-Littlewood.

I 4 problemi riproposti da Landau:

1. La congettura di Goldbach (1742): ogni numero pari > 2 è somma di due primi;
2. La congettura dei primi gemelli (Euclide?);
3. La congettura di Legendre (~ 1800): esiste sempre almeno un numero primo tra n^2 e $(n+1)^2$, qualunque sia $n \in \mathbb{N}$.
4. Quinta congettura di Hardy-Littlewood.

I 4 problemi riproposti da Landau:

1. La congettura di Goldbach (1742): ogni numero pari > 2 è somma di due primi;
2. La congettura dei primi gemelli (Euclide?);
3. La congettura di Legendre ($\sim$ 1800): esiste sempre almeno un numero primo tra n^2 e $(n+1)^2$, qualunque sia $n \in \mathbb{N}$.
4. Quinta congettura di Hardy-Littlewood.

I 4 problemi riproposti da Landau:

1. La congettura di Goldbach (1742): ogni numero pari > 2 è somma di due primi;
2. La congettura dei primi gemelli (Euclide?);
3. La congettura di Legendre ($\sim$ 1800): esiste sempre almeno un numero primo tra n^2 e $(n+1)^2$, qualunque sia $n \in \mathbb{N}$.
4. Quinta congettura di Hardy-Littlewood.

La quinta congettura di HL.

Tutti i numeri primi (a parte il 2) sono della forma $2n + 1$.

Quanti numeri primi sono della forma: $3n + 1$? o $3n + 2$?

Quanti numeri primi sono della forma: $4n + 1$? o $4n + 2$? o $4n + 3$?

In generale, quanti numeri primi sono della forma $an + b$?

La quinta congettura di HL.
Tutti i numeri primi (a parte il 2) sono della forma $2n + 1$.
Quanti numeri primi sono della forma: $3n + 1$? o $3n + 2$?
Quanti numeri primi sono della forma: $4n + 1$? o $4n + 2$? o $4n + 3$?
In generale, quanti numeri primi sono della forma $an + b$?

La quinta congettura di HL.
Tutti i numeri primi (a parte il 2) sono della forma $2n + 1$.
Quanti numeri primi sono della forma: $3n + 1$? o $3n + 2$?
Quanti numeri primi sono della forma: $4n + 1$? o $4n + 2$? o $4n + 3$?
In generale, quanti numeri primi sono della forma $an + b$?

La quinta congettura di HL.
Tutti i numeri primi (a parte il 2) sono della forma $2n + 1$.
Quanti numeri primi sono della forma: $3n + 1$? o $3n + 2$?
Quanti numeri primi sono della forma: $4n + 1$? o $4n + 2$? o $4n + 3$?
In generale, quanti numeri primi sono della forma $an + b$?

Esempio: primi della forma $4n + 3$. Si possono anche scrivere come $4n - 1$.

Supponiamo siano finiti e sia p il più grande. Consideriamo

$$N = 4 \cdot 3 \cdot 5 \cdot 7 \cdots p - 1$$

$N > p$ è della forma $4n - 1$, quindi è composto. Tutti i suoi fattori primi sono $> p$ e quindi della forma $4n + 1$.
Prodotto di numeri della forma $4n + 1$ è ancora della forma $4n + 1$. Assurdo.

Esempio: primi della forma $4n + 3$. Si possono anche scrivere come $4n - 1$.
Supponiamo siano finiti e sia p il più grande. Consideriamo

$$N = 4 \cdot 3 \cdot 5 \cdot 7 \cdots p - 1$$

$N > p$ è della forma $4n - 1$, quindi è composto. Tutti i suoi fattori primi sono $> p$ e quindi della forma $4n + 1$.
Prodotto di numeri della forma $4n + 1$ è ancora della forma $4n + 1$. Assurdo.

Esempio: primi della forma $4n + 3$. Si possono anche scrivere come $4n - 1$.
Supponiamo siano finiti e sia p il più grande. Consideriamo

$$N = 4 \cdot 3 \cdot 5 \cdot 7 \cdots p - 1$$

$N > p$ è della forma $4n - 1$, quindi è composto. Tutti i suoi fattori primi sono $> p$ e quindi della forma $4n + 1$.
Prodotto di numeri della forma $4n + 1$ è ancora della forma $4n + 1$. Assurdo.

Esempio: primi della forma $4n + 3$. Si possono anche scrivere come $4n - 1$.
Supponiamo siano finiti e sia p il più grande. Consideriamo

$$N = 4 \cdot 3 \cdot 5 \cdot 7 \cdots p - 1$$

$N > p$ è della forma $4n - 1$, quindi è composto. Tutti i suoi fattori primi sono $> p$ e quindi della forma $4n + 1$.
Prodotto di numeri della forma $4n + 1$ è ancora della forma $4n + 1$. Assurdo.

Johann Peter Gustav Lejeune Dirichlet (nato 1805, morto 1859).

Dirichlet ha dimostrato (nel 1837) che, se a, b sono interi, primi tra loro e $a > 0$, allora ci sono infiniti primi della forma $an + b$.

Altro modo di enunciare il risultato:

il polinomio di primo grado $f(x) = ax + b$ (a, b coprimi, $a > 0$) fornisce numeri primi per infiniti $x \in \mathbb{N}$.

Dirichlet ha dimostrato (nel 1837) che, se a, b sono interi, primi tra loro e $a > 0$, allora ci sono infiniti primi della forma $an + b$.

Altro modo di enunciare il risultato:

il polinomio di primo grado $f(x) = ax + b$ (a, b coprimi, $a > 0$) fornisce numeri primi per infiniti $x \in \mathbb{N}$.

Si può generalizzare il problema per polinomi di grado più alto?

Consideriamo il polinomio

$$f(x) = x^2 + x + 41$$

Si può generalizzare il problema per polinomi di grado più alto?

Consideriamo il polinomio

$$f(x) = x^2 + x + 41$$

esempio sage (4)

Nessun polinomio, quando valutato sui numeri interi, può dare solo numeri primi.

Consideriamo il polinomio:

$$f(x) = x^2 + 1$$

è vero che $f(n)$ è un numero primo per infiniti $n \in \mathbb{N}$?

Questo è il *quarto problema di Landau*, ossia la quinta congettura di Hardy-Littlewood. Problema ancora irrisolto.

Nessun polinomio, quando valutato sui numeri interi, può dare solo numeri primi.

Consideriamo il polinomio:

$$f(x) = x^2 + 1$$

è vero che $f(n)$ è un numero primo per infiniti $n \in \mathbb{N}$?

Questo è il *quarto problema di Landau*, ossia la quinta congettura di Hardy-Littlewood. Problema ancora irrisolto.

Nessun polinomio, quando valutato sui numeri interi, può dare solo numeri primi.

Consideriamo il polinomio:

$$f(x) = x^2 + 1$$

è vero che $f(n)$ è un numero primo per infiniti $n \in \mathbb{N}$?

Questo è il *quarto problema di Landau*, ossia la quinta congettura di Hardy-Littlewood. Problema ancora irrisolto.

Godfrey Harold Hardy (nato 1877, morto 1947)

Consideriamo ora il polinomio:

$$f(x) = x^2 - 1$$

Quanti primi può dare quando valutato sui naturali?

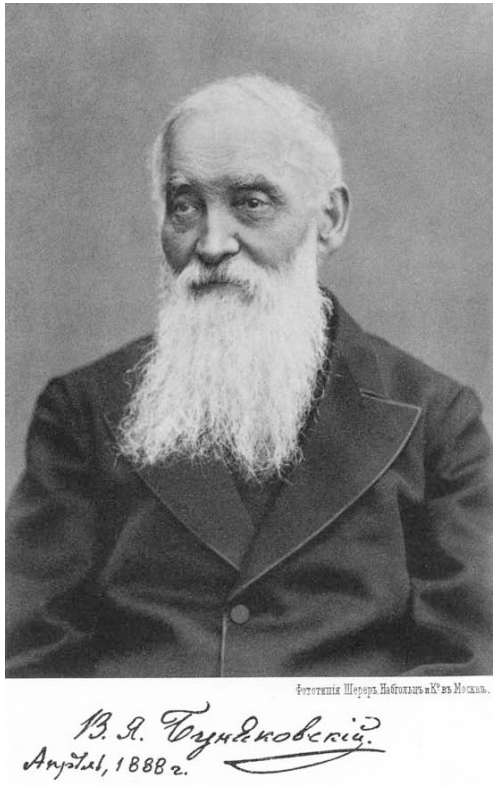
Consideriamo ora il polinomio:

$$f(x) = x^2 - 1$$

Quanti primi può dare quando valutato sui naturali?

Congettura di Bunyakovskij (1857):

Dato un polinomio $f(x)$ a coefficienti interi "buono" (coefficiente direttivo positivo, irriducibile su $\mathbb{Z}[x]$, primitivo), $f(n)$ è primo per infiniti valori di $n \in \mathbb{N}$.



Viktor Yakovlevich Bunyakovskij (nato 1804, morto 1889).

Attualmente non si conosce un solo polinomio di grado ≥ 2 a coefficienti interi che dia infiniti numeri primi.

Come ottenere numeri primi “grandi”?

Ci sono varie formule. Il numero primo più grande che si conosce attualmente ha 22.338.618 cifre. È stato calcolato il 7 gennaio 2016.

Come ottenere numeri primi “grandi”?
Ci sono varie formule. Il numero primo più grande che si conosce attualmente ha 22.338.618 cifre. È stato calcolato il 7 gennaio 2016.

I numeri primi di Mersenne.

Marin Mersenne (nato 1588, morto 1648).

Sia a un numero naturale. Quando

$$a^n - 1$$

ha la speranza di essere primo?

Deve essere della forma $M_p = 2^p - 1$ con p primo.

Ma non basta. Ad esempio $2^{11} - 1 = 23 \times 89$.
M_p si dice numero di Mersenne.

Sia a un numero naturale. Quando

$$a^n - 1$$

ha la speranza di essere primo?

Deve essere della forma $M_p = 2^p - 1$ con p primo.

Ma non basta. Ad esempio $2^{11} - 1 = 23 \times 89$.
M_p si dice numero di Mersenne.

Sia a un numero naturale. Quando

$$a^n - 1$$

ha la speranza di essere primo?

Deve essere della forma $M_p = 2^p - 1$ con p primo.

Ma non basta. Ad esempio $2^{11} - 1 = 23 \times 89$.
M_p si dice numero di Mersenne.

Sia a un numero naturale. Quando

$$a^n - 1$$

ha la speranza di essere primo?

Deve essere della forma $M_p = 2^p - 1$ con p primo.

Ma non basta. Ad esempio $2^{11} - 1 = 23 \times 89$.
M_p si dice numero di Mersenne.

Test di Lukas-Lehmer:

Definiamo la successione L_n in questo modo:

$$L_1 = 4, \quad L_{n+1} = L_n^2 - 2$$

La successione comincia così:

$$4,\ 14,\ 194,\ 37634,\ 1416317954,\ 2005956546822746114$$

Vale:
M_p è un numero primo se e solo se M_p divide L_{p-1}.

Test di Lukas-Lehmer:

Definiamo la successione L_n in questo modo:

$$L_1 = 4, \quad L_{n+1} = L_n^2 - 2$$

La successione comincia così:

$$4,\ 14,\ 194,\ 37634,\ 1416317954,\ 2005956546822746114$$

Vale:
M_p è un numero primo se e solo se M_p divide L_{p-1}.

Test di Lukas-Lehmer:

Definiamo la successione L_n in questo modo:

$$L_1 = 4, \quad L_{n+1} = L_n^2 - 2$$

La successione comincia così:

$$4,\ 14,\ 194,\ 37634,\ 1416317954,\ 2005956546822746114$$

Vale:
M_p è un numero primo se e solo se M_p divide L_{p-1}.

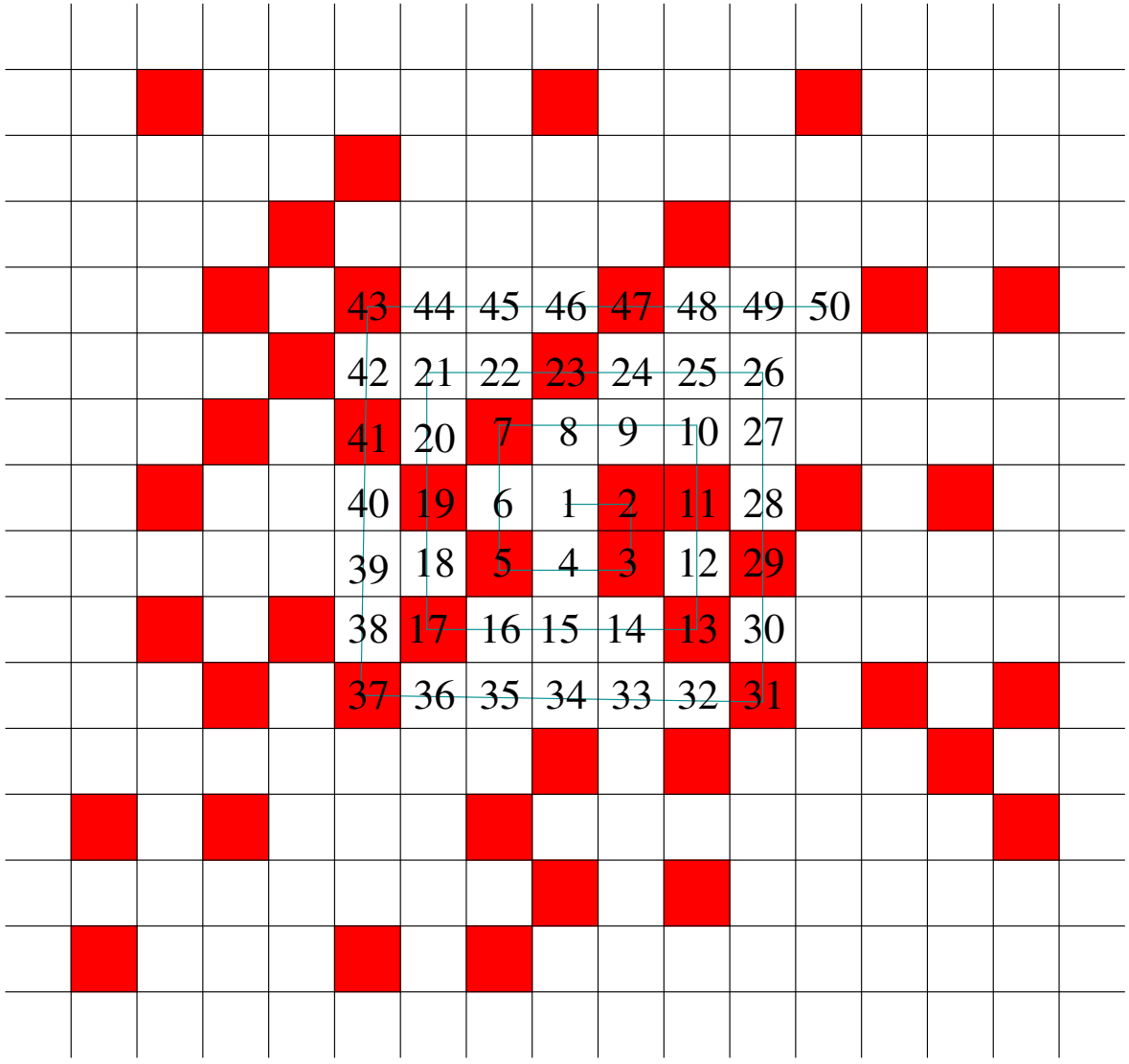
Esempio:

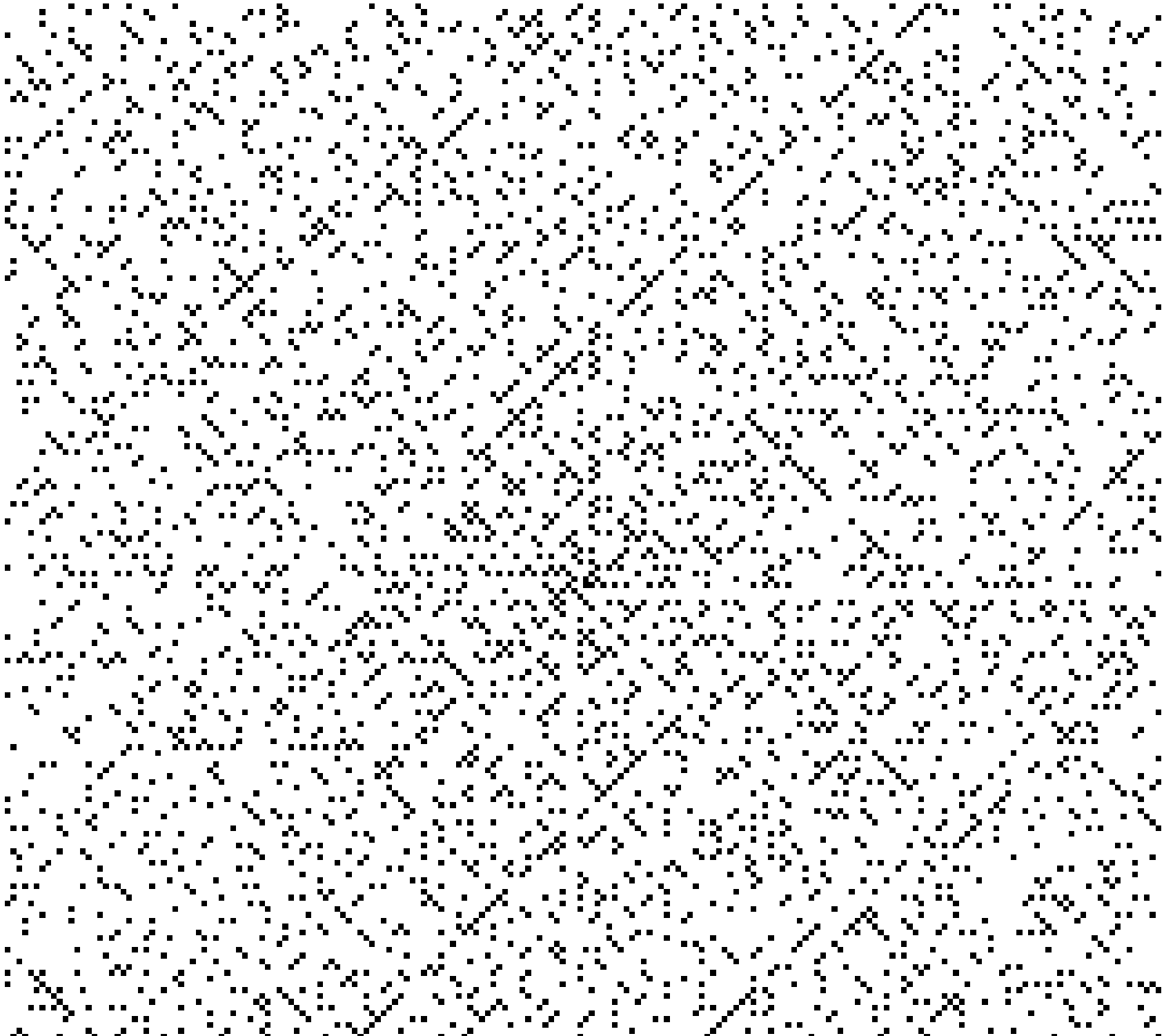
$$p = 3; \quad L_{p-1} = L_2 = 14, \quad M_p = 7.$$

esempio sage (5)
Corriere

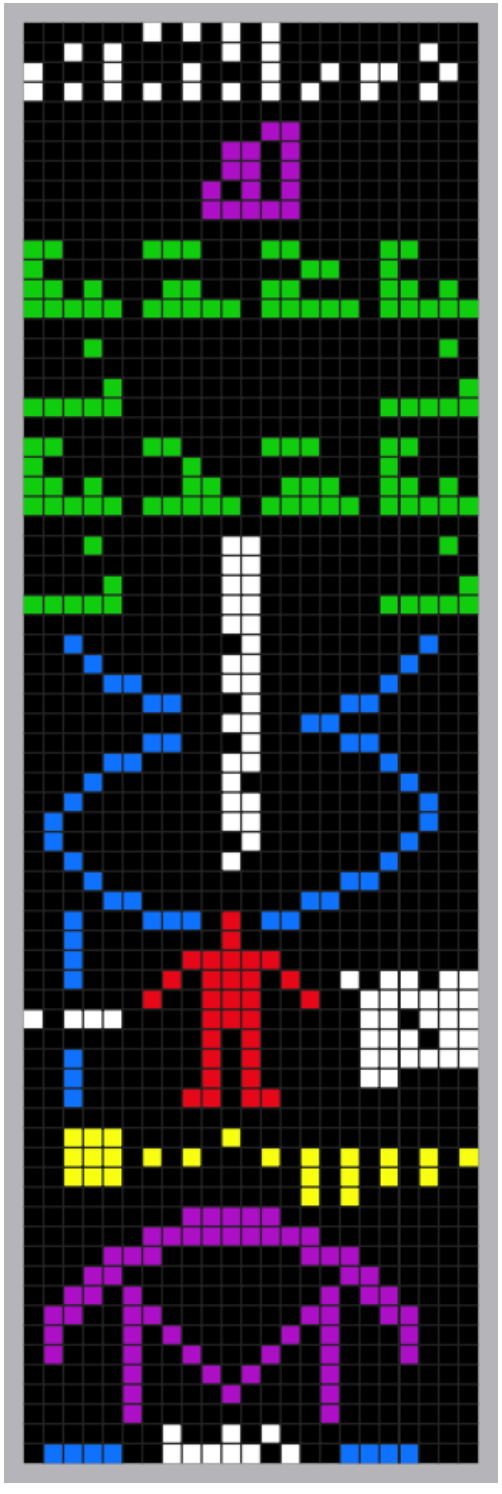
Stanisław Ulam (nato 1909, morto 1984).

Spirale di Ulam (1963).

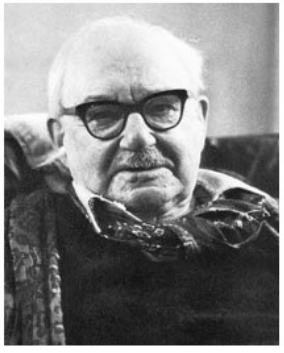




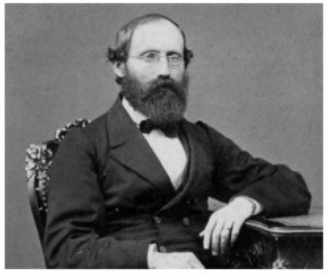
esempio sage (6)










Grazie
dell'attenzione!