I numeri primi: teoremi, congetture e applicazioni
Scuola Estiva di San Pellegrino Terme

Alessandro Zaccagnini
Dipartimento di Matematica e Informatica
Università di Parma

San Pellegrino Terme, 7 settembre 2016

Il Teorema di Euclide: esistono infiniti numeri primi

Teorema (Euclide)

L'insieme dei numeri primi è illimitato superiormente

Il Teorema di Euclide: esistono infiniti numeri primi

Teorema (Euclide)

L'insieme dei numeri primi è illimitato superiormente

Esempio

Troviamo un numero primo > 1000

Il Teorema di Euclide: esistono infiniti numeri primi

Teorema (Euclide)

L'insieme dei numeri primi è illimitato superiormente

Esempio

Troviamo un numero primo > 1000. Facile! Un qualsiasi fattore primo di $1000! + 1$

Il Teorema di Euclide, II

Dimostrazione

Sia n un qualsiasi intero positivo e sia p un qualsiasi fattore primo di $M = n! + 1$

Il Teorema di Euclide, II

Dimostrazione

Sia n un qualsiasi intero positivo e sia p un qualsiasi fattore primo di $M = n! + 1$: evidentemente $p > n$ dato che $M \equiv 1 \bmod d$ per ogni intero $d \in [2, n]$

Il Teorema di Euclide, II

Dimostrazione

Sia n un qualsiasi intero positivo e sia p un qualsiasi fattore primo di $M = n! + 1$: evidentemente $p > n$ dato che $M \equiv 1 \bmod d$ per ogni intero $d \in [2, n]$. Dunque l'insieme dei numeri primi è illimitato superiormente

Il Teorema di Euclide, II

Dimostrazione

Sia n un qualsiasi intero positivo e sia p un qualsiasi fattore primo di $M = n! + 1$: evidentemente $p > n$ dato che $M \equiv 1 \bmod d$ per ogni intero $d \in [2, n]$. Dunque l'insieme dei numeri primi è illimitato superiormente

Esempio

n	1	2	3	4	5	6	7	8	9	10
p_n	2	3	7	5	11	7	71	61	19	11

p_n è il piú piccolo fattore primo di $n! + 1$

Quanti sono i numeri primi?

1. 2, 4, 6, 8, 10, 12, . . . , 90, 92, 94, 96, 98, 100 [50]

Quanti sono i numeri primi?

1. 2, 4, 6, 8, 10, 12, . . . , 90, 92, 94, 96, 98, 100 [50]
2. 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 [25]

Quanti sono i numeri primi?

1. 2, 4, 6, 8, 10, 12, . . . , 90, 92, 94, 96, 98, 100 [50]
2. 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 [25]
3. 1, 4, 9, 16, 25, 36, 49, 64, 81, 100 [10]

Quanti sono i numeri primi?

1. 2, 4, 6, 8, 10, 12, . . . , 90, 92, 94, 96, 98, 100 [50]
2. 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 [25]
3. 1, 4, 9, 16, 25, 36, 49, 64, 81, 100 [10]
4. 1, 2, 3, 5, 8, 13, 21, 34, 55, 89 [10]

Quanti sono i numeri primi?

1. 2, 4, 6, 8, 10, 12, . . . , 90, 92, 94, 96, 98, 100 [50]
2. 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 [25]
3. 1, 4, 9, 16, 25, 36, 49, 64, 81, 100 [10]
4. 1, 2, 3, 5, 8, 13, 21, 34, 55, 89 [10]
5. 1, 2, 4, 8, 16, 32, 64 [7]

Quanti sono i numeri primi?

1. 2, 4, 6, 8, 10, 12, . . . , 90, 92, 94, 96, 98, 100 [50]
2. 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 [25]
3. 1, 4, 9, 16, 25, 36, 49, 64, 81, 100 [10]
4. 1, 2, 3, 5, 8, 13, 21, 34, 55, 89 [10]
5. 1, 2, 4, 8, 16, 32, 64 [7]
6. 1, 2, 6, 24 [4]

Quanti sono i numeri primi?

Indichiamo con $\pi(n)$ il numero dei numeri primi fino ad n

Quanti sono i numeri primi?

Indichiamo con $\pi(n)$ il numero dei numeri primi fino ad n

1. Crivello di Eratostene (per determinare i numeri primi)

Quanti sono i numeri primi?

Indichiamo con $\pi(n)$ il numero dei numeri primi fino ad n

1. Crivello di Eratostene (per determinare i numeri primi)
2. Calcolo numerico esatto di $\pi(n)$ per $n = 10, 10^2, 10^3$ fino ad $n = 10^{25}$

n	$\pi(n)$
10	4
10^2	25
10^3	168
10^4	1229
10^5	9592
10^6	78498
10^7	664579
10^8	5761455

Quanti sono i numeri primi?

Indichiamo con $\pi(n)$ il numero dei numeri primi fino ad n

1. Crivello di Eratostene (per determinare i numeri primi)
2. Calcolo numerico esatto di $\pi(n)$ per $n = 10, 10^2, 10^3$ fino ad $n = 10^{25}$

n	$\pi(n)$
10	4
10^2	25
10^3	168
10^4	1229
10^5	9592
10^6	78498
10^7	664579
10^8	5761455

3. Congettura di Gauss–Legendre

Una maggiorazione per il numero di numeri primi

Utilizziamo il coefficiente binomiale centrale: per esempio, per $n = 16$ abbiamo

▸ Coefficienti binomiali

$$\binom{32}{16} = \frac{17 \cdot 18 \cdot 19 \cdots 31 \cdot 32}{16!} = 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot m \leq 2^{32}$$

Qui m è un certo intero positivo

Una maggiorazione per il numero di numeri primi

Utilizziamo il coefficiente binomiale centrale: per esempio, per $n = 16$ abbiamo

▸ Coefficienti binomiali

$$\binom{32}{16} = \frac{17 \cdot 18 \cdot 19 \cdots 31 \cdot 32}{16!} = 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot m \leq 2^{32}$$

Qui m è un certo intero positivo. Dunque

$$17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \leq 2^{32}$$

Una maggiorazione per il numero di numeri primi

Utilizziamo il coefficiente binomiale centrale: per esempio, per $n = 16$ abbiamo

▸ Coefficienti binomiali

$$\binom{32}{16} = \frac{17 \cdot 18 \cdot 19 \cdots 31 \cdot 32}{16!} = 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot m \leq 2^{32}$$

Qui m è un certo intero positivo. Dunque

$$17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \leq 2^{32}$$

Ma

$$17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \geq 16 \cdot 16 \cdot 16 \cdot 16 \cdot 16$$

Una maggiorazione per il numero di numeri primi

Utilizziamo il coefficiente binomiale centrale: per esempio, per $n = 16$ abbiamo

▸ Coefficienti binomiali

$$\binom{32}{16} = \frac{17 \cdot 18 \cdot 19 \cdots 31 \cdot 32}{16!} = 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot m \leq 2^{32}$$

Qui m è un certo intero positivo. Dunque

$$17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \leq 2^{32}$$

Ma

$$17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \geq 16 \cdot 16 \cdot 16 \cdot 16 \cdot 16$$

Posto $x = \pi(32) - \pi(16)$, abbiamo

$$16^x \leq 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \leq \binom{32}{16} \leq 2^{32}$$

Una maggiorazione per il numero di numeri primi, II

Riassumendo, abbiamo

$$16^x \leq 2^{32}$$

Una maggiorazione per il numero di numeri primi, II

Riassumendo, abbiamo

$$16^x \leq 2^{32}$$

Quindi

$$x \log(16) = \big(\pi(32) - \pi(16)\big) \log(16) \leq 32 \log(2)$$

Una maggiorazione per il numero di numeri primi, II

Riassumendo, abbiamo

$$16^x \leq 2^{32}$$

Quindi

$$x \log(16) = \big(\pi(32) - \pi(16)\big) \log(16) \leq 32 \log(2)$$

cioè

$$x = 5 \leq \frac{32 \log(2)}{\log(16)} = 8$$

Una maggiorazione per il numero di numeri primi, II

Riassumendo, abbiamo

$$16^x \leq 2^{32}$$

Quindi

$$x \log(16) = \big(\pi(32) - \pi(16)\big) \log(16) \leq 32 \log(2)$$

cioè

$$x = 5 \leq \frac{32 \log(2)}{\log(16)} = 8$$

In generale, per $n \geq 2$ abbiamo

$$\pi(2n) - \pi(n) \leq \frac{2n \log(2)}{\log(n)}$$

▸ Funzioni esponenziale e logaritmo

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\pi(2^{10}) - \pi(2^9) \qquad \leq 113$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned} \pi(2^{10}) - \pi(2^9) &\leq 113 \\ \pi(2^9) - \pi(2^8) &\leq 64 \end{aligned}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned} \pi(2^{10}) - \pi(2^9) &\leq 113 \\ \pi(2^9) - \pi(2^8) &\leq 64 \\ \pi(2^8) - \pi(2^7) &\leq 36 \end{aligned}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned} \pi(2^{10}) - \pi(2^9) &\leq 113 \\ \pi(2^9) - \pi(2^8) &\leq 64 \\ \pi(2^8) - \pi(2^7) &\leq 36 \\ \pi(2^7) - \pi(2^6) &\leq 21 \end{aligned}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned}
\pi(2^{10}) - \pi(2^9) &\leq 113 \\
\pi(2^9) - \pi(2^8) &\leq 64 \\
\pi(2^8) - \pi(2^7) &\leq 36 \\
\pi(2^7) - \pi(2^6) &\leq 21 \\
\pi(2^6) - \pi(2^5) &\leq 12
\end{aligned}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned}
\pi(2^{10}) - \pi(2^9) &\leq 113 \\
\pi(2^9) - \pi(2^8) &\leq 64 \\
\pi(2^8) - \pi(2^7) &\leq 36 \\
\pi(2^7) - \pi(2^6) &\leq 21 \\
\pi(2^6) - \pi(2^5) &\leq 12 \\
\pi(2^5) - \pi(2^4) &\leq 8
\end{aligned}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned}
\pi(2^{10}) - \pi(2^9) &\leq 113 \\
\pi(2^9) - \pi(2^8) &\leq 64 \\
\pi(2^8) - \pi(2^7) &\leq 36 \\
\pi(2^7) - \pi(2^6) &\leq 21 \\
\pi(2^6) - \pi(2^5) &\leq 12 \\
\pi(2^5) - \pi(2^4) &\leq 8 \\
\pi(2^4) &= 6
\end{aligned}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned}
\pi(2^{10}) - \pi(2^9) &\leq 113 \\
\pi(2^9) - \pi(2^8) &\leq 64 \\
\pi(2^8) - \pi(2^7) &\leq 36 \\
\pi(2^7) - \pi(2^6) &\leq 21 \\
\pi(2^6) - \pi(2^5) &\leq 12 \\
\pi(2^5) - \pi(2^4) &\leq 8 \\
\pi(2^4) &= 6 \\
\text{Totale} \quad \pi(2^{10}) &\leq 260
\end{aligned}$$

Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}\log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}$$

Per esempio

$$\begin{aligned}
\pi(2^{10}) - \pi(2^9) &= 75 \leq 113 \\
\pi(2^9) - \pi(2^8) &= 43 \leq 64 \\
\pi(2^8) - \pi(2^7) &= 23 \leq 36 \\
\pi(2^7) - \pi(2^6) &= 13 \leq 21 \\
\pi(2^6) - \pi(2^5) &= 7 \leq 12 \\
\pi(2^5) - \pi(2^4) &= 5 \leq 8 \\
\pi(2^4) &= 6 = 6 \\
\text{Totale} \qquad \pi(2^{10}) &= 172 \leq 260
\end{aligned}$$

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Qual è la massima potenza di 5 che divide 1000! ?

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Qual è la massima potenza di 5 che divide 1000! ?

Nell'intervallo $[1, 1000]$ ci sono 200 multipli di 5

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Qual è la massima potenza di 5 che divide 1000! ?

Nell'intervallo $[1, 1000]$ ci sono 200 multipli di 5; ma poi ci sono 40 multipli di $25 = 5^2$

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Qual è la massima potenza di 5 che divide 1000! ?

Nell'intervallo $[1, 1000]$ ci sono 200 multipli di 5; ma poi ci sono 40 multipli di $25 = 5^2$; e poi ancora 8 multipli di $125 = 5^3$

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Qual è la massima potenza di 5 che divide 1000! ?

Nell'intervallo $[1, 1000]$ ci sono 200 multipli di 5; ma poi ci sono 40 multipli di $25 = 5^2$; e poi ancora 8 multipli di $125 = 5^3$; e infine un multiplo di $625 = 5^4$

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Qual è la massima potenza di 5 che divide 1000! ?

Nell'intervallo $[1, 1000]$ ci sono 200 multipli di 5; ma poi ci sono 40 multipli di $25 = 5^2$; e poi ancora 8 multipli di $125 = 5^3$; e infine un multiplo di $625 = 5^4$

Complessivamente, $200 + 40 + 8 + 1 = 249$

Con quante cifre 0 termina 1000! ?

In altre parole, qual è la massima potenza di 10 che divide 1000! ?

Qual è la massima potenza di 5 che divide 1000! ?

Nell'intervallo $[1, 1000]$ ci sono 200 multipli di 5; ma poi ci sono 40 multipli di $25 = 5^2$; e poi ancora 8 multipli di $125 = 5^3$; e infine un multiplo di $625 = 5^4$

Complessivamente, $200 + 40 + 8 + 1 = 249$

$$\begin{aligned} 249 &= \left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] \\ &\sim \frac{1000}{5}\left(1 + \frac{1}{5} + \frac{1}{5^2} + \frac{1}{5^3}\right) \\ &\sim \frac{1000}{5} \cdot \frac{1}{1 - 1/5} = \frac{1000}{4} = 250 \end{aligned}$$

Scomponiamo in fattori $n!$

La scomposizione in fattori primi di $n!$ contiene informazioni sui numeri primi fino ad n

Scomponiamo in fattori $n!$

La scomposizione in fattori primi di $n!$ contiene informazioni sui numeri primi fino ad n. Per esempio

$$20! = 2^{10+5+2+1} \cdot 3^{6+2} \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$$

Scomponiamo in fattori $n!$

La scomposizione in fattori primi di $n!$ contiene informazioni sui numeri primi fino ad n. Per esempio

$$20! = 2^{10+5+2+1} \cdot 3^{6+2} \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$$

Il punto essenziale è che c'è un modo alternativo per calcolare (approssimativamente) quanto vale $n!$

▸ La formula di Stirling

Scomponiamo in fattori $n!$

La scomposizione in fattori primi di $n!$ contiene informazioni sui numeri primi fino ad n. Per esempio

$$20! = 2^{10+5+2+1} \cdot 3^{6+2} \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$$

Il punto essenziale è che c'è un modo alternativo per calcolare (approssimativamente) quanto vale $n!$

▸ La formula di Stirling

Con qualche calcolo ulteriore si dimostra che per n grande

$$\sum_{p \leq n} \frac{\log(p)}{p-1} \sim \log(n) \qquad \text{e} \qquad \pi(n) \geq \frac{n \log(2)}{\log(n)}$$

e quindi esistono infiniti numeri primi!

Teorema di Eulero, versione qualitativa

▸ Serie geometrica

$$A = 2 = \left(1 - \frac{1}{2}\right)^{-1} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots \geq 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8}$$

$$B = \frac{3}{2} = \left(1 - \frac{1}{3}\right)^{-1} = 1 + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \ldots \geq 1 + \frac{1}{3} + \frac{1}{9}$$

$$C = \frac{5}{4} = \left(1 - \frac{1}{5}\right)^{-1} = 1 + \frac{1}{5} + \frac{1}{25} + \ldots \geq 1 + \frac{1}{5}$$

$$D = \frac{7}{6} = \left(1 - \frac{1}{7}\right)^{-1} = 1 + \frac{1}{7} + \frac{1}{49} + \ldots \geq 1 + \frac{1}{7}$$

Teorema di Eulero, versione qualitativa, II

$$\begin{aligned} A \cdot B \cdot C \cdot D &\geq \left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}\right)\left(1+\frac{1}{3}+\frac{1}{9}\right)\left(1+\frac{1}{5}\right)\left(1+\frac{1}{7}\right) \\ &\geq 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10} \\ &\geq \log(10) \end{aligned}$$

▸ La serie armonica

Teorema di Eulero, versione qualitativa, II

$$\begin{aligned} A \cdot B \cdot C \cdot D &\geq \left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}\right)\left(1+\frac{1}{3}+\frac{1}{9}\right)\left(1+\frac{1}{5}\right)\left(1+\frac{1}{7}\right) \\ &\geq 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10} \\ &\geq \log(10) \end{aligned}$$

▸ La serie armonica

Teorema (Eulero)

Per $n \geq 2$ si ha

$$\prod_{p \leq n}\left(1-\frac{1}{p}\right)^{-1} \geq 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \geq \log(n)$$

dove il prodotto è fatto su tutti i numeri primi che non superano n

L'identità di Eulero e la funzione zeta di Riemann

Teorema (Identità di Eulero)

Se $x > 1$ *allora*

$$\begin{aligned}\zeta(x) &= 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \cdots \\ &= \left(1 - \frac{1}{2^x}\right)^{-1} \cdot \left(1 - \frac{1}{3^x}\right)^{-1} \cdot \left(1 - \frac{1}{5^x}\right)^{-1} \cdot \left(1 - \frac{1}{7^x}\right)^{-1} \cdots\end{aligned}$$

dove il prodotto è fatto su tutti i numeri primi

L'identità di Eulero e la funzione zeta di Riemann

Teorema (Identità di Eulero)

Se $x > 1$ allora

$$\begin{aligned}\zeta(x) &= 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \cdots \\ &= \left(1 - \frac{1}{2^x}\right)^{-1} \cdot \left(1 - \frac{1}{3^x}\right)^{-1} \cdot \left(1 - \frac{1}{5^x}\right)^{-1} \cdot \left(1 - \frac{1}{7^x}\right)^{-1} \cdots\end{aligned}$$

dove il prodotto è fatto su tutti i numeri primi

- Riemann (1859)

L'identità di Eulero e la funzione zeta di Riemann

Teorema (Identità di Eulero)

Se $x > 1$ *allora*

$$\begin{aligned}\zeta(x) &= 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \cdots \\ &= \left(1 - \frac{1}{2^x}\right)^{-1} \cdot \left(1 - \frac{1}{3^x}\right)^{-1} \cdot \left(1 - \frac{1}{5^x}\right)^{-1} \cdot \left(1 - \frac{1}{7^x}\right)^{-1} \cdots\end{aligned}$$

dove il prodotto è fatto su tutti i numeri primi

- Riemann (1859)
- Eulero (XVIII secolo)

L'identità di Eulero e la funzione zeta di Riemann

Teorema (Identità di Eulero)

Se $x > 1$ allora

$$\begin{aligned}\zeta(x) &= 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \cdots \\ &= \left(1 - \frac{1}{2^x}\right)^{-1} \cdot \left(1 - \frac{1}{3^x}\right)^{-1} \cdot \left(1 - \frac{1}{5^x}\right)^{-1} \cdot \left(1 - \frac{1}{7^x}\right)^{-1} \cdots\end{aligned}$$

dove il prodotto è fatto su tutti i numeri primi

- Riemann (1859)
- Eulero (XVIII secolo)
- Problema di Mengoli (1644): quanto vale $\zeta(2)$?

Teorema di Eulero, versione quantitativa

$$\sum_{p \leq n} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p^*} \sim \log(\log(n)) \qquad \text{quando } n \to +\infty$$

dove p^* indica il massimo numero primo che non supera n

Teorema di Eulero, versione quantitativa

$$\sum_{p \leq n} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p^*} \sim \log(\log(n)) \qquad \text{quando } n \to +\infty$$

dove p^* indica il massimo numero primo che non supera n

Questo si dimostra utilizzando la serie geometrica, la serie armonica e il "limite notevole" per il logaritmo

La Congettura di Gauss–Legendre

Abbiamo dimostrato che, per n grande, si ha

$$\frac{n\log(2)}{\log(n)} \leq \pi(n) \leq \frac{2n\log(2)}{\log(n)}$$

La Congettura di Gauss–Legendre

Abbiamo dimostrato che, per n grande, si ha

$$\frac{n\log(2)}{\log(n)} \leq \pi(n) \leq \frac{2n\log(2)}{\log(n)}$$

Questo ci dà l'*ordine di grandezza* della funzione $\pi(n)$: Gauss e Legendre hanno immaginato che fosse vero un risultato piú preciso

La Congettura di Gauss–Legendre

Abbiamo dimostrato che, per n grande, si ha

$$\frac{n\log(2)}{\log(n)} \leq \pi(n) \leq \frac{2n\log(2)}{\log(n)}$$

Questo ci dà l'*ordine di grandezza* della funzione $\pi(n)$: Gauss e Legendre hanno immaginato che fosse vero un risultato piú preciso

Congettura (Gauss–Legendre)

$$\pi(n) \sim \frac{n}{\log(n)} \qquad \textit{quando } n \to +\infty$$

La funzione θ di Chebyshev

Poniamo

$$\begin{aligned}\theta(n) &= \sum_{p \leq n} \log(p) = \log(2) + \log(3) + \log(5) + \cdots + \log(p^*) \\ &= \log\left(2 \cdot 3 \cdot 5 \cdots p^*\right)\end{aligned}$$

dove p^* indica il massimo numero primo che non supera n

La funzione θ di Chebyshev

Poniamo

$$\begin{aligned}\theta(n) &= \sum_{p \leq n} \log(p) = \log(2) + \log(3) + \log(5) + \cdots + \log(p^*) \\ &= \log\left(2 \cdot 3 \cdot 5 \cdots p^*\right)\end{aligned}$$

dove p^* indica il massimo numero primo che non supera n

Per esempio, $\theta(100) \approx 83.7$ e $\theta(1000) \approx 956.2$

La funzione θ di Chebyshev

Poniamo

$$\begin{aligned}\theta(n) &= \sum_{p \leq n} \log(p) = \log(2) + \log(3) + \log(5) + \cdots + \log(p^*) \\ &= \log\left(2 \cdot 3 \cdot 5 \cdots p^*\right)\end{aligned}$$

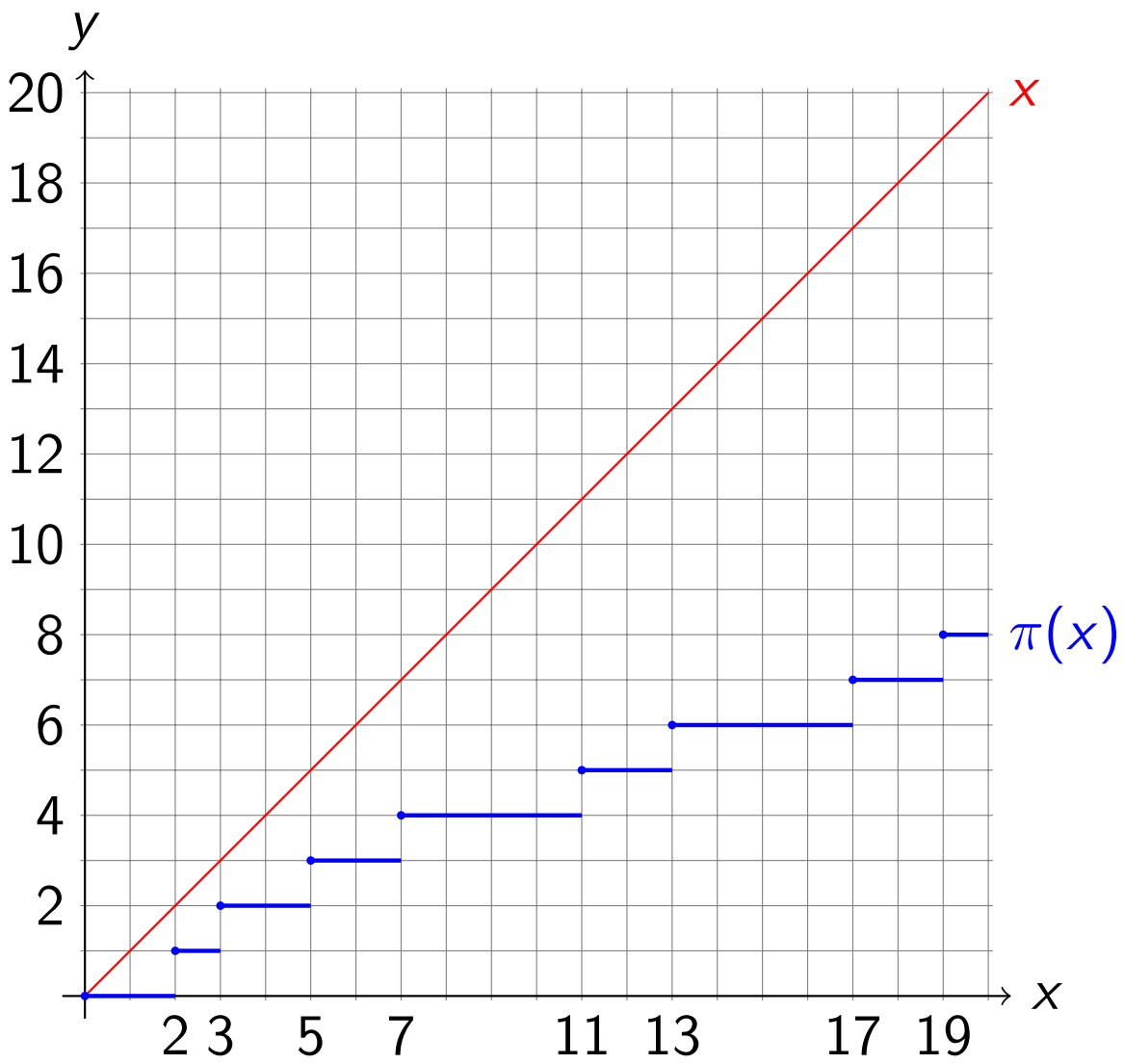
dove p^* indica il massimo numero primo che non supera n

Per esempio, $\theta(100) \approx 83.7$ e $\theta(1000) \approx 956.2$

Congettura (Variante della Congettura di Gauss–Legendre)

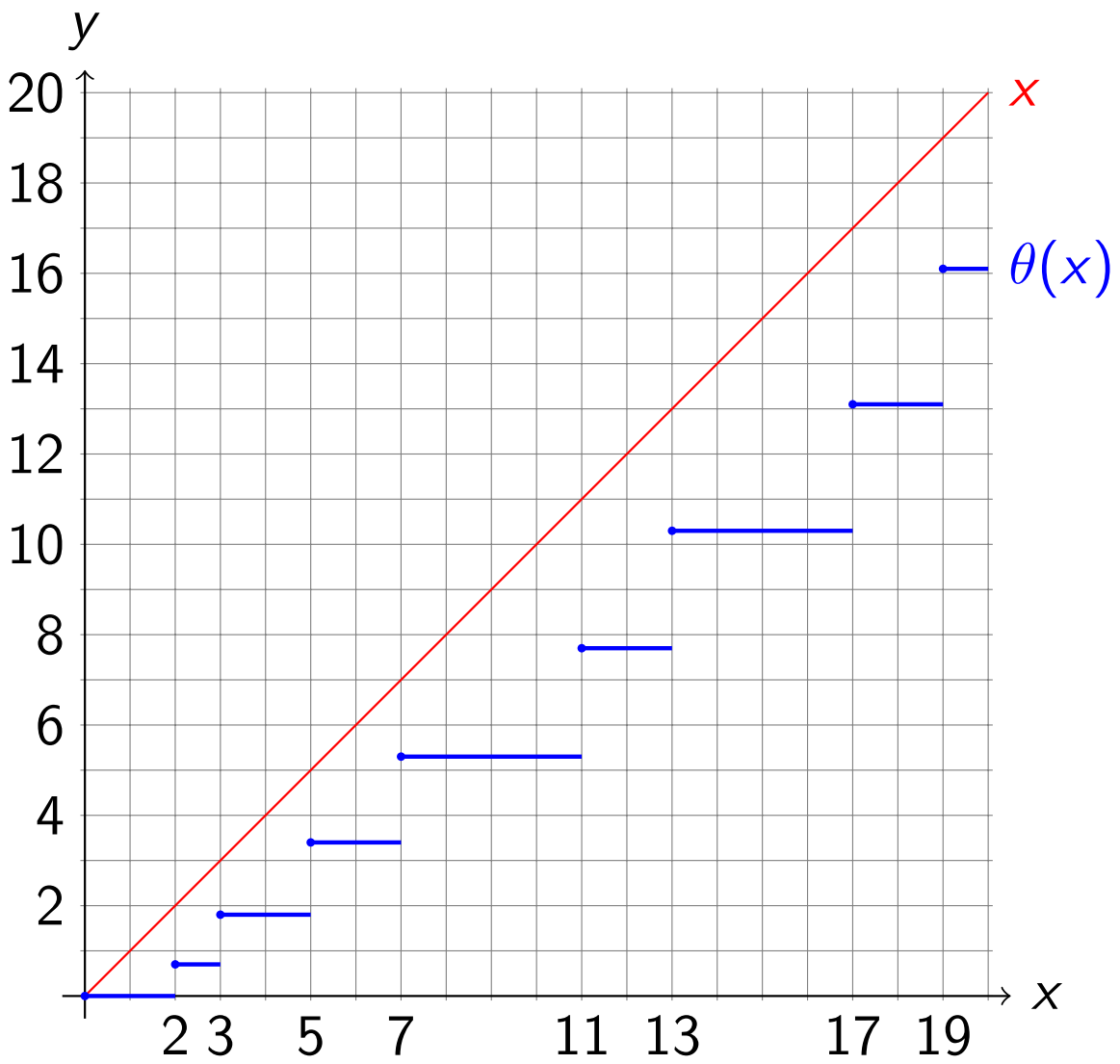
$$\theta(n) \sim n \qquad \textit{quando } n \to +\infty$$

Il grafico della funzione π



$$\pi(x) = \sum_{p \leq x} 1$$

Il grafico della funzione θ



$$\theta(x) = \sum_{p \leq x} \log(p)$$

Il Teorema dei Numeri Primi

Diamo due versioni equivalenti del Teorema dei Numeri Primi

Teorema (Hadamard, de la Vallée Poussin (1896))

$$\pi(n) \sim \frac{n}{\log(n)} \qquad \textit{e anche} \qquad \theta(n) \sim n$$

Il Teorema dei Numeri Primi

Diamo due versioni equivalenti del Teorema dei Numeri Primi

Teorema (Hadamard, de la Vallée Poussin (1896))

$$\pi(n) \sim \frac{n}{\log(n)} \qquad \textit{e anche} \qquad \theta(n) \sim n$$

La dimostrazione del Teorema dei Numeri Primi è stata data seguendo in dettaglio le idee nell'articolo di Riemann del 1859

Il Teorema dei Numeri Primi

Diamo due versioni equivalenti del Teorema dei Numeri Primi

Teorema (Hadamard, de la Vallée Poussin (1896))

$$\pi(n) \sim \frac{n}{\log(n)} \qquad \textit{e anche} \qquad \theta(n) \sim n$$

La dimostrazione del Teorema dei Numeri Primi è stata data seguendo in dettaglio le idee nell'articolo di Riemann del 1859

Resta il problema quantitativo della bontà dell'approssimazione: quanto è grande lo *scarto* $|\theta(n) - n|$?

La Congettura di Riemann

Congettura (Riemann)

Per ogni numero intero $n \geq 2$ si ha

$$\left|\theta(n) - n\right| \leq 100\sqrt{n}\log^2(n)$$

La Congettura di Riemann

Congettura (Riemann)

Per ogni numero intero $n \geq 2$ si ha

$$\left|\theta(n) - n\right| \leq 100\sqrt{n}\log^2(n)$$

Per esempio

$$\theta(500\,000) \approx 499\,318.12$$

La Congettura di Riemann

Congettura (Riemann)

Per ogni numero intero $n \geq 2$ si ha

$$\left|\theta(n) - n\right| \leq 100\sqrt{n}\log^2(n)$$

Per esempio

$$\theta(500\,000) \approx 499\,318.12$$

Dunque la differenza vale ≈ 681.88

La Congettura di Riemann

Congettura (Riemann)

Per ogni numero intero $n \geq 2$ si ha

$$\left|\theta(n) - n\right| \leq 100\sqrt{n}\log^2(n)$$

Per esempio

$$\theta(500\,000) \approx 499\,318.12$$

Dunque la differenza vale ≈ 681.88. Per gli interi $n \leq 500\,000$ la massima differenza si ha per $n_0 = 463\,180$, per cui

$$\theta(463\,180) \approx 461\,975.38$$

La Congettura di Riemann

Congettura (Riemann)

Per ogni numero intero $n \geq 2$ si ha

$$\left|\theta(n) - n\right| \leq 100\sqrt{n}\log^2(n)$$

Per esempio

$$\theta(500\,000) \approx 499\,318.12$$

Dunque la differenza vale ≈ 681.88. Per gli interi $n \leq 500\,000$ la massima differenza si ha per $n_0 = 463\,180$, per cui

$$\theta(463\,180) \approx 461\,975.38$$

La differenza vale $\approx 1\,204.62$

La Congettura di Riemann

Congettura (Riemann)

Per ogni numero intero $n \geq 2$ si ha

$$\left|\theta(n) - n\right| \leq 100\sqrt{n}\log^2(n)$$

Per esempio

$$\theta(500\,000) \approx 499\,318.12$$

Dunque la differenza vale ≈ 681.88. Per gli interi $n \leq 500\,000$ la massima differenza si ha per $n_0 = 463\,180$, per cui

$$\theta(463\,180) \approx 461\,975.38$$

La differenza vale $\approx 1\,204.62$ e il rapporto

$$\frac{\left|\theta(n_0) - n_0\right|}{\sqrt{n_0}\log^2(n_0)} \approx 0.0104$$

La forma ottimale del Teorema dei Numeri Primi

Oggi è noto che

$$|\theta(n) - n| \leq 100 \frac{n}{\exp\left(\sqrt{\log(n)}\right)}$$

per tutti gli interi n da un certo punto in poi

La forma ottimale del Teorema dei Numeri Primi

Oggi è noto che

$$|\theta(n) - n| \leq 100 \frac{n}{\exp\left(\sqrt{\log(n)}\right)}$$

per tutti gli interi n da un certo punto in poi

La Congettura di Riemann afferma che

$$|\theta(n) - n| \leq 100\sqrt{n}\log^2(n)$$

La forma ottimale del Teorema dei Numeri Primi

Oggi è noto che

$$|\theta(n) - n| \leq 100 \frac{n}{\exp\left(\sqrt{\log(n)}\right)}$$

per tutti gli interi n da un certo punto in poi

La Congettura di Riemann afferma che

$$|\theta(n) - n| \leq 100\sqrt{n}\log^2(n)$$

Il matematico britannico John E. Littlewood ha dimostrato nel 1914 che (approssimativamente)

$$|\theta(n) - n| \geq \sqrt{n}$$

per infiniti interi n

La forma ottimale del Teorema dei Numeri Primi

Oggi è noto che

$$|\theta(n) - n| \leq 100 \frac{n}{\exp\left(\sqrt{\log(n)}\right)}$$

per tutti gli interi n da un certo punto in poi

La Congettura di Riemann afferma che

$$|\theta(n) - n| \leq 100\sqrt{n}\log^2(n)$$

Il matematico britannico John E. Littlewood ha dimostrato nel 1914 che (approssimativamente)

$$|\theta(n) - n| \geq \sqrt{n}$$

per infiniti interi n

Accenniamo ad un problema connesso: qual è la massima distanza possibile tra numeri primi consecutivi?

I problemi di Landau (International Congress of Mathematicians; Cambridge, 1912)

1. Problema binario di Goldbach: se $n \geq 6$ è pari, allora esistono due numeri primi dispari p_1 e p_2 tali che $n = p_1 + p_2$ (parzialmente risolto: Helfgott 2013, problema ternario)

I problemi di Landau (International Congress of Mathematicians; Cambridge, 1912)

1. Problema binario di Goldbach: se $n \geq 6$ è pari, allora esistono due numeri primi dispari p_1 e p_2 tali che $n = p_1 + p_2$ (parzialmente risolto: Helfgott 2013, problema ternario)
2. Primi gemelli: esistono infiniti numeri primi p per cui $p + 2$ è primo (parzialmente risolto: Zhang, Maynard 2013)

I problemi di Landau (International Congress of Mathematicians; Cambridge, 1912)

1. Problema binario di Goldbach: se $n \geq 6$ è pari, allora esistono due numeri primi dispari p_1 e p_2 tali che $n = p_1 + p_2$ (parzialmente risolto: Helfgott 2013, problema ternario)
2. Primi gemelli: esistono infiniti numeri primi p per cui $p + 2$ è primo (parzialmente risolto: Zhang, Maynard 2013)
3. Esistono infiniti numeri primi p per cui $p + 2$ e $p + 6$ sono simultaneamente primi

I problemi di Landau (International Congress of Mathematicians; Cambridge, 1912)

1. Problema binario di Goldbach: se $n \geq 6$ è pari, allora esistono due numeri primi dispari p_1 e p_2 tali che $n = p_1 + p_2$ (parzialmente risolto: Helfgott 2013, problema ternario)
2. Primi gemelli: esistono infiniti numeri primi p per cui $p + 2$ è primo (parzialmente risolto: Zhang, Maynard 2013)
3. Esistono infiniti numeri primi p per cui $p + 2$ e $p + 6$ sono simultaneamente primi
4. Primi tra quadrati consecutivi: per $n \geq 2$, esiste un numero primo fra n^2 ed $(n + 1)^2$ (quasi risolto se è vera la Congettura di Riemann)

I problemi di Landau (International Congress of Mathematicians; Cambridge, 1912)

1. Problema binario di Goldbach: se $n \geq 6$ è pari, allora esistono due numeri primi dispari p_1 e p_2 tali che $n = p_1 + p_2$ (parzialmente risolto: Helfgott 2013, problema ternario)
2. Primi gemelli: esistono infiniti numeri primi p per cui $p + 2$ è primo (parzialmente risolto: Zhang, Maynard 2013)
3. Esistono infiniti numeri primi p per cui $p + 2$ e $p + 6$ sono simultaneamente primi
4. Primi tra quadrati consecutivi: per $n \geq 2$, esiste un numero primo fra n^2 ed $(n + 1)^2$ (quasi risolto se è vera la Congettura di Riemann)
5. Il polinomio $n^2 + 1$ assume valore primo per infiniti interi n ($n = 1$, 2, 4, 6, 10, 14, 16, 20, 26, . . . ?)

Applicazioni dei numeri primi: la Crittografia

1. Riconoscere i numeri primi. Piccolo Teorema di Fermat, Miller-Rabin, AKS (Agrawal, Kayal, Saxena)

Applicazioni dei numeri primi: la Crittografia

1. Riconoscere i numeri primi. Piccolo Teorema di Fermat, Miller-Rabin, AKS (Agrawal, Kayal, Saxena)
2. Determinare numeri primi grandi

Applicazioni dei numeri primi: la Crittografia

1. Riconoscere i numeri primi. Piccolo Teorema di Fermat, Miller-Rabin, AKS (Agrawal, Kayal, Saxena)
2. Determinare numeri primi grandi
3. Crittografia a chiave pubblica (RSA, ElGamal, . . .)

Applicazioni dei numeri primi: la Crittografia

1. Riconoscere i numeri primi. Piccolo Teorema di Fermat, Miller-Rabin, AKS (Agrawal, Kayal, Saxena)
2. Determinare numeri primi grandi
3. Crittografia a chiave pubblica (RSA, ElGamal, . . .)
4. Protocolli crittografici: PEC, denaro elettronico, . . .

Applicazioni dei numeri primi: la Crittografia

1. Riconoscere i numeri primi. Piccolo Teorema di Fermat, Miller-Rabin, AKS (Agrawal, Kayal, Saxena)
2. Determinare numeri primi grandi
3. Crittografia a chiave pubblica (RSA, ElGamal, . . .)
4. Protocolli crittografici: PEC, denaro elettronico, . . .
5. Generazione di sequenze pseudo-casuali per le simulazioni

Applicazioni dei numeri primi: la Crittografia

1. Riconoscere i numeri primi. Piccolo Teorema di Fermat, Miller-Rabin, AKS (Agrawal, Kayal, Saxena)
2. Determinare numeri primi grandi
3. Crittografia a chiave pubblica (RSA, ElGamal, . . .)
4. Protocolli crittografici: PEC, denaro elettronico, . . .
5. Generazione di sequenze pseudo-casuali per le simulazioni

Grazie!

La serie geometrica

Se $q \in (-1, 1)$ allora

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

◂ Torna indietro

La serie geometrica

Se $q \in (-1, 1)$ allora

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

Per esempio, per $q = 1/10$ abbiamo

$$\begin{aligned} 1.11111\ldots &= 1 + \frac{1}{10} + \frac{1}{100} + \frac{1}{1\,000} + \frac{1}{10\,000} + \frac{1}{100\,000} + \ldots \\ &= \frac{1}{1 - 1/10} = \frac{10}{9} \end{aligned}$$

◂ Torna indietro

I coefficienti binomiali

Ricordiamo che i numeri

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} \qquad \text{per } k = 0, 1, \ldots, m$$

sono interi positivi

Torna indietro

I coefficienti binomiali

Ricordiamo che i numeri

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} \qquad \text{per } k = 0, 1, \ldots, m$$

sono interi positivi. Ci interessa in particolare il coefficiente binomiale "centrale" per il quale valgono le disuguaglianze

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq 2^{2n}$$

◂ Torna indietro

I coefficienti binomiali

Ricordiamo che i numeri

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} \qquad \text{per } k = 0, 1, \ldots, m$$

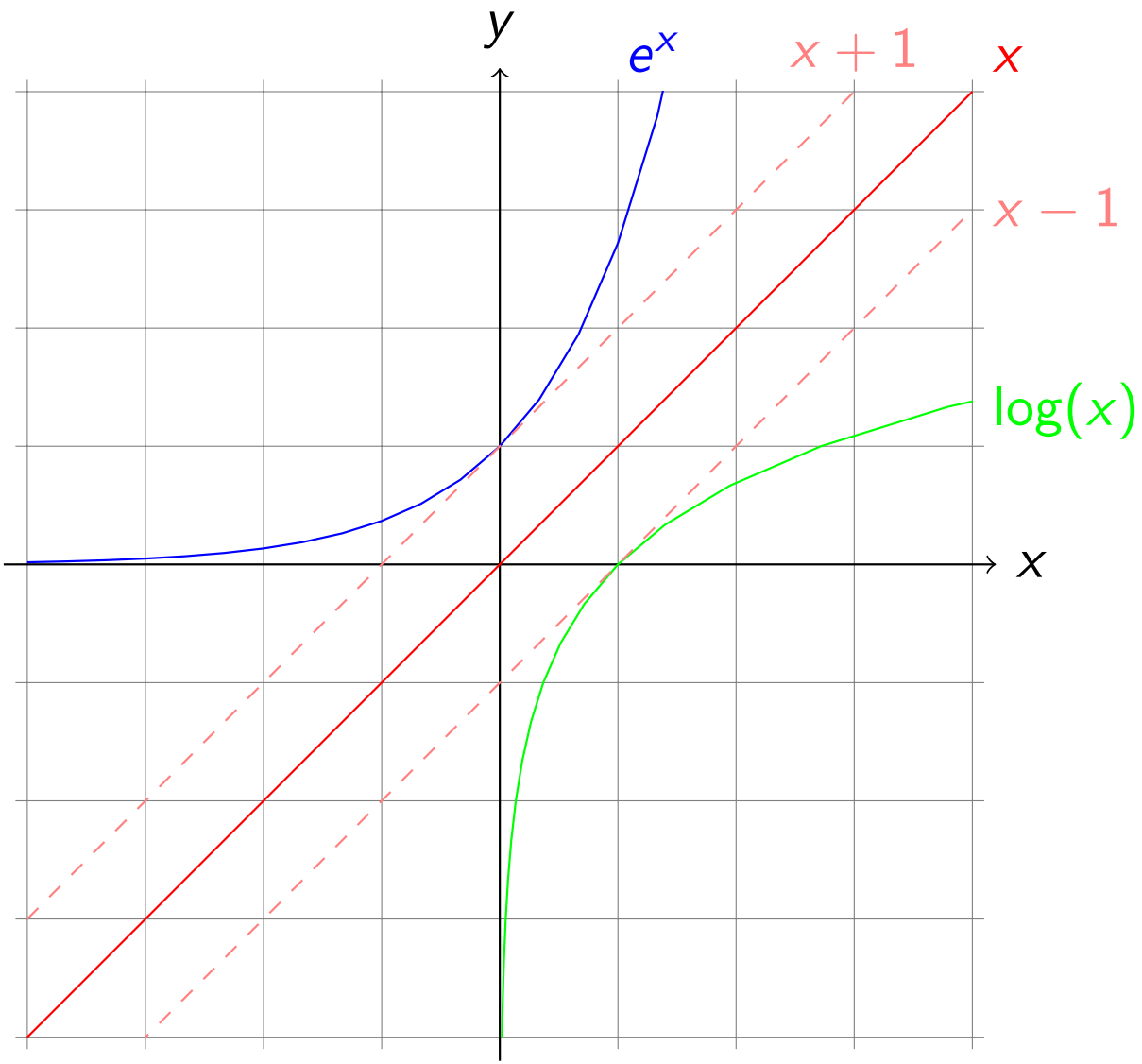
sono interi positivi. Ci interessa in particolare il coefficiente binomiale "centrale" per il quale valgono le disuguaglianze

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq 2^{2n}$$

La seconda dipende dal fatto che la somma di tutti gli elementi sulla $2n$-esima riga del Triangolo di Tartaglia vale 2^{2n}. La prima dipende dal fatto che sulla stessa riga ci sono $2n+1$ elementi di cui quello centrale è il massimo.

Torna indietro

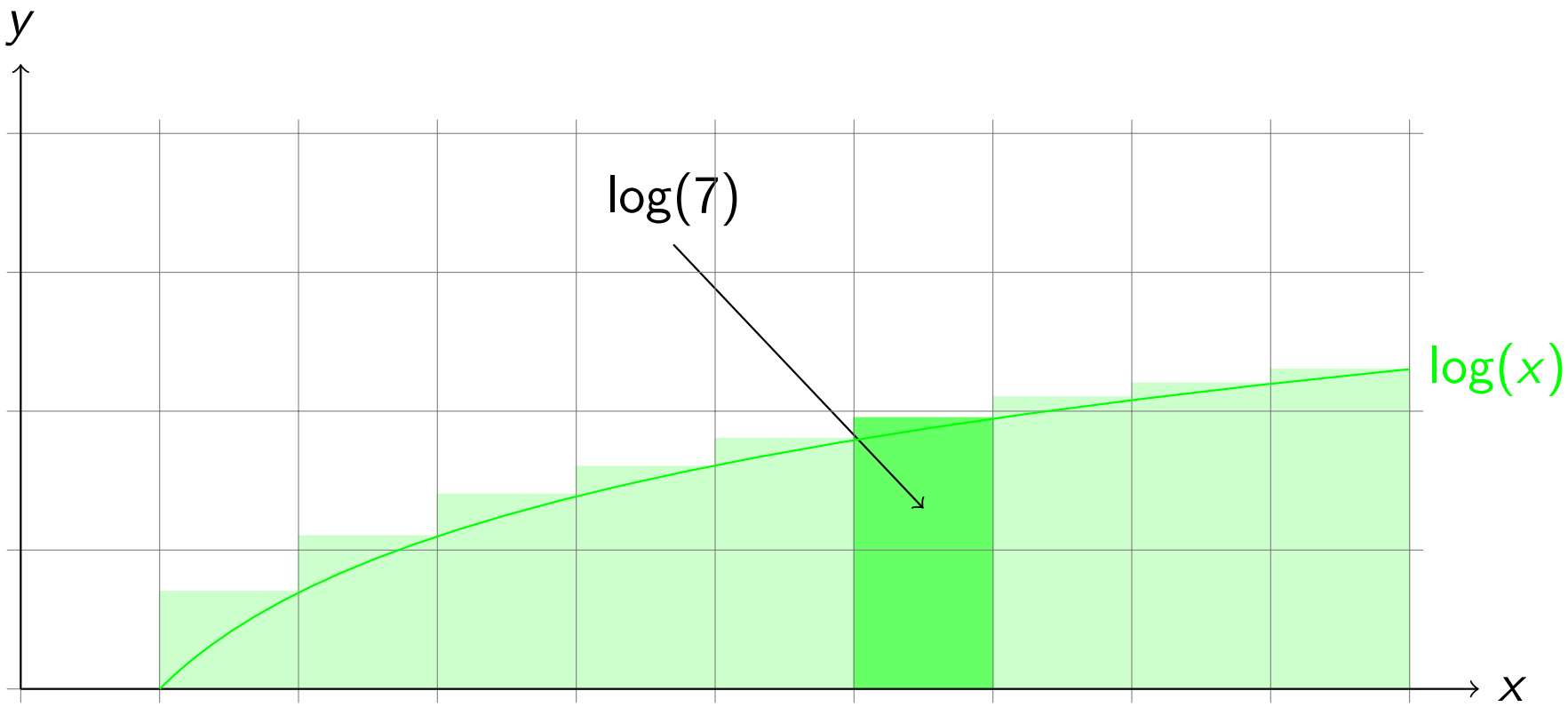
Le funzioni esponenziale e logaritmo



$$\lim_{t \to 0} \frac{\log(1+t)}{t} = 1$$

Torna indietro

La formula di Stirling

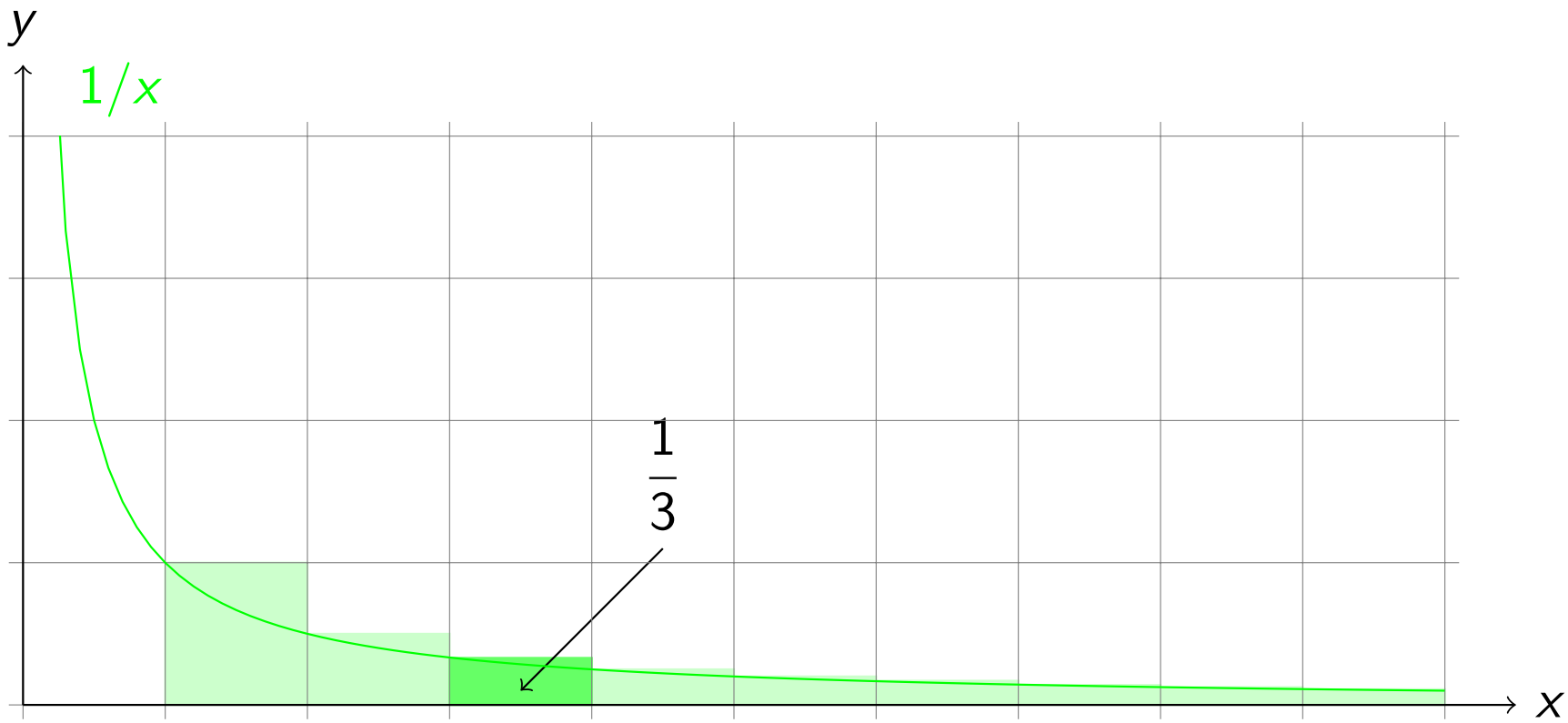


Per N grande si ha

$$\log(N!) = \log(1) + \log(2) + \log(3) + \cdots + \log(N) \sim N\log(N) - N$$

Torna indietro

La serie armonica



Per N grande si ha

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N} \sim \log(N)$$

La serie armonica, II

$$
\begin{aligned}
&1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}\\
=&1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)\\
&\quad+\left(\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}\right)\\
\geq&1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}=1+\frac{1}{2}\log_2(16)
\end{aligned}
$$

Torna indietro

La serie armonica, II

$$
\begin{aligned}
&1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}\\
=&1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)\\
&+\left(\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}\right)\\
\geq&1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}=1+\frac{1}{2}\log_2(16)
\end{aligned}
$$

In generale

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{2^k}\geq 1+\frac{1}{2}\cdot k$$

Torna indietro