

# Aquilo que ainda não sabe(mo)s sobre números primos

José Carlos Santos

Seminário Diagonal — 2 de Novembro de 2011

# Números primos

- ▶ Um número primo é um número natural  $p > 1$  que não tem outros divisores além de 1 e de  $p$ .

# Números primos

- ▶ Um número primo é um número natural  $p > 1$  que não tem outros divisores além de 1 e de  $p$ .
- ▶ **Teorema (Euclides):** Há uma infinidade de números primos.

# Conjectura de Fermat

- ▶ Fermat constatou que os números  $F_n = 2^{2^n} + 1$  são primos quando  $0 \leq n \leq 4$ .

# Conjectura de Fermat

- ▶ Fermat constatou que os números  $F_n = 2^{2^n} + 1$  são primos quando  $0 \leq n \leq 4$ .
- ▶ Conjectura: são todos primos.

# Conjectura de Fermat

- ▶ Fermat constatou que os números  $F_n = 2^{2^n} + 1$  são primos quando  $0 \leq n \leq 4$ .
- ▶ Conjectura: são todos primos.
- ▶ Falso (Euler):  $641 \mid 2^{2^5} + 1$

# Conjectura de Fermat

- ▶ Fermat constatou que os números  $F_n = 2^{2^n} + 1$  são primos quando  $0 \leq n \leq 4$ .
- ▶ Conjectura: são todos primos.
- ▶ Falso (Euler):  $641 \mid 2^{2^5} + 1$
- ▶ Problemas em aberto:
  - ▶ Há algum  $F_n$  primo com  $n > 4$ ?

# Conjectura de Fermat

- ▶ Fermat constatou que os números  $F_n = 2^{2^n} + 1$  são primos quando  $0 \leq n \leq 4$ .
- ▶ Conjectura: são todos primos.
- ▶ Falso (Euler):  $641 \mid 2^{2^5} + 1$
- ▶ Problemas em aberto:
  - ▶ Há algum  $F_n$  primo com  $n > 4$ ?
  - ▶ Todos os  $F_n$  (com  $n > 4$ ) são compostos?

# Teorema dos números primos (1ª parte)

► Seja

$$\pi(x) = \# \{ \text{primos } p \mid p \leq x \}$$

# Teorema dos números primos (1ª parte)

- ▶ Seja

$$\pi(x) = \# \{ \text{primos } p \mid p \leq x \}$$

- ▶ Conjectura (Legendre):

$$\lim_{x \rightarrow +\infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

# Teorema dos números primos (1ª parte)

- ▶ Seja

$$\pi(x) = \# \{ \text{primos } p \mid p \leq x \}$$

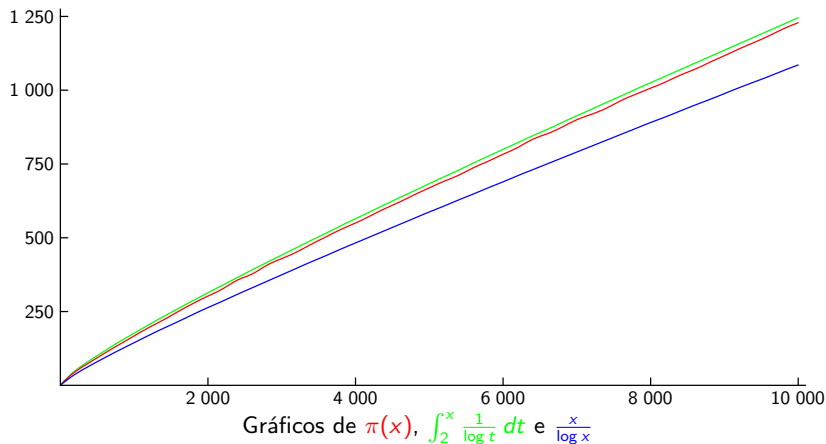
- ▶ Conjectura (Legendre):

$$\lim_{x \rightarrow +\infty} \frac{\pi(x)}{x / \log(x)} = 1.$$

- ▶ Conjectura (Gauss):

$$\lim_{x \rightarrow +\infty} \frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt} = 1.$$

# Teorema dos números primos (2ª parte)



## Teorema dos números primos (3ª parte)

- ▶ Chebyshev (1848) estudou o quociente  $\frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt}$  e provou que

## Teorema dos números primos (3ª parte)

- ▶ Chebyshev (1848) estudou o quociente  $\frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt}$  e provou que
  - ▶ se  $x \gg 0$ , o quociente está entre 0,89 e 1,11;

## Teorema dos números primos (3ª parte)

- ▶ Chebyshev (1848) estudou o quociente  $\frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt}$  e provou que
- ▶ se  $x \gg 0$ , o quociente está entre 0,89 e 1,11;
  - ▶ se tiver limite em  $+\infty$ , só pode ser 1.

## Teorema dos números primos (3ª parte)

- ▶ Chebyshev (1848) estudou o quociente  $\frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt}$  e provou que
  - ▶ se  $x \gg 0$ , o quociente está entre 0,89 e 1,11;
  - ▶ se tiver limite em  $+\infty$ , só pode ser 1.
- ▶ Riemann (1859) estabeleceu uma ponte entre a conjectura e a Análise Complexa.

## Teorema dos números primos (3ª parte)

- ▶ Chebyshev (1848) estudou o quociente  $\frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt}$  e provou que
  - ▶ se  $x \gg 0$ , o quociente está entre 0,89 e 1,11;
  - ▶ se tiver limite em  $+\infty$ , só pode ser 1.
- ▶ Riemann (1859) estabeleceu uma ponte entre a conjectura e a Análise Complexa.
- ▶ Hadamard e de la Vallée-Poussin (1896) demonstraram a conjectura

## Teorema dos números primos (3ª parte)

- ▶ Chebyshev (1848) estudou o quociente  $\frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt}$  e provou que
  - ▶ se  $x \gg 0$ , o quociente está entre 0,89 e 1,11;
  - ▶ se tiver limite em  $+\infty$ , só pode ser 1.
- ▶ Riemann (1859) estabeleceu uma ponte entre a conjectura e a Análise Complexa.
- ▶ Hadamard e de la Vallée-Poussin (1896) demonstraram a conjectura usando Análise Complexa.

## Teorema dos números primos (3ª parte)

- ▶ Chebyshev (1848) estudou o quociente  $\frac{\pi(x)}{\int_2^x \frac{1}{\log t} dt}$  e provou que
  - ▶ se  $x \gg 0$ , o quociente está entre 0,89 e 1,11;
  - ▶ se tiver limite em  $+\infty$ , só pode ser 1.
- ▶ Riemann (1859) estabeleceu uma ponte entre a conjectura e a Análise Complexa.
- ▶ Hadamard e de la Vallée-Poussin (1896) demonstraram a conjectura usando Análise Complexa.
- ▶ Demonstração elementar: Atle Selberg e Pal Erdős (1949).

# Postulado de Bertrand

*Para cada número natural  $n$ , existe algún número primo  $p$  tal que  $n < p < 2n$ .*

# Postulado de Bertrand

*Para cada número natural  $n$ , existe algum número primo  $p$  tal que  $n < p < 2n$ .*

$n$	primos entre $n$ e $2n$
1.000	135
2.000	247
4.000	457
8.000	855
16.000	1.570

História:

1845: Conjeturado por Joseph Bertrand.

# Postulado de Bertrand

*Para cada número natural  $n$ , existe algum número primo  $p$  tal que  $n < p < 2n$ .*

$n$	primos entre $n$ e $2n$
1.000	135
2.000	247
4.000	457
8.000	855
16.000	1.570

História:

1845: Conjeturado por Joseph Bertrand.

1850: Demonstrado por Chebyshev.

# Postulado de Bertrand

*Para cada número natural  $n$ , existe algum número primo  $p$  tal que  $n < p < 2n$ .*

$n$	primos entre $n$ e $2n$
1.000	135
2.000	247
4.000	457
8.000	855
16.000	1.570

História:

1845: Conjeturado por Joseph Bertrand.

1850: Demonstrado por Chebyshev.

1919: Nova demonstração (Ramanujan).

# Postulado de Bertrand

*Para cada número natural  $n$ , existe algum número primo  $p$  tal que  $n < p < 2n$ .*

$n$	primos entre $n$ e $2n$
1.000	135
2.000	247
4.000	457
8.000	855
16.000	1.570

História:

1845: Conjeturado por Joseph Bertrand.

1850: Demonstrado por Chebyshev.

1919: Nova demonstração (Ramanujan).

1931: Nova demonstração (Erdős).

# Problemas de Landau (1912)

- ▶ Conjectura de Goldbach

# Problemas de Landau (1912)

- ▶ Conjectura de Goldbach
- ▶ Conjectura dos primos gémeos

# Problemas de Landau (1912)

- ▶ Conjectura de Goldbach
- ▶ Conjectura dos primos gémeos
- ▶ Conjectura de Legendre

# Problemas de Landau (1912)

- ▶ Conjectura de Goldbach
- ▶ Conjectura dos primos gémeos
- ▶ Conjectura de Legendre
- ▶ Há uma infinidade de primos da forma  $n^2 + 1$ ?

# Problemas resolvidos

- ▶ Teste AKS (2002)

# Problemas resolvidos

- ▶ Teste AKS (2002)
- ▶ Teorema de Green-Tao (2004)

# Distribuição dos números primos

Se  $k \in \mathbb{N}$ , há sempre um primo entre  $kn$  e  $(k + 1)n$ ?

# Distribuição dos números primos

Se  $k \in \mathbb{N}$ , há sempre um primo entre  $kn$  e  $(k + 1)n$ ?

- ▶  $k = 1$ : sim (postulado de Bertrand)

# Distribuição dos números primos

Se  $k \in \mathbb{N}$ , há sempre um primo entre  $kn$  e  $(k + 1)n$ ?

- ▶  $k = 1$ : sim (postulado de Bertrand)
- ▶  $k = 2$ : sim (El Bachraoui, 2006)

# Distribuição dos números primos

Se  $k \in \mathbb{N}$ , há sempre um primo entre  $kn$  e  $(k + 1)n$ ?

- ▶  $k = 1$ : sim (postulado de Bertrand)
- ▶  $k = 2$ : sim (El Bachraoui, 2006)
- ▶  $k = 3$ : sim (Andy Loo, 2011)

# Distribuição dos números primos

Se  $k \in \mathbb{N}$ , há sempre um primo entre  $kn$  e  $(k + 1)n$ ?

- ▶  $k = 1$ : sim (postulado de Bertrand)
- ▶  $k = 2$ : sim (El Bachraoui, 2006)
- ▶  $k = 3$ : sim (Andy Loo, 2011)

