O Santo Graal da Matemática *não* trará o desastre para a Internet

Paula Cristina Valença

14 de Março de 2007

Em como fiz batota

- mas o π é transcendente...

Em como fiz batota

- mas o π é transcendente...
- π? probabilidade de dois números aleatórios serem co-primos: $6/\pi^2$...

Em como fiz batota

- mas o π é transcendente...
- π? probabilidade de dois números aleatórios serem co-primos: $6/\pi^2$...
- π? probabilidade de um número ser "square-free": $6/\pi^2$...

Em como fiz batota

- mas o π é transcendente...
- π? probabilidade de dois números aleatórios serem co-primos: $6/\pi^2$...
- π? probabilidade de um número ser "square-free": $6/\pi^2$...
- ou podia falar da hipótese de Riemann e da distribuição dos números primos. A função chama-se $\pi(x)$...

Os primos: de Eratosthenes a Gauss

Os primos, a tabela periódica

Primos. . . ? *sim, números divisivéis só por 1 e eles próprios.*
Ok, e depois?

Theorem

Teorema Fundamental da Aritmética Todo o número inteiro positivo pode ser escrito de uma forma única como o produto de primos.

Ah, alicerces!

Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes

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

Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes

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

Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes

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

Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes

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

Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes

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

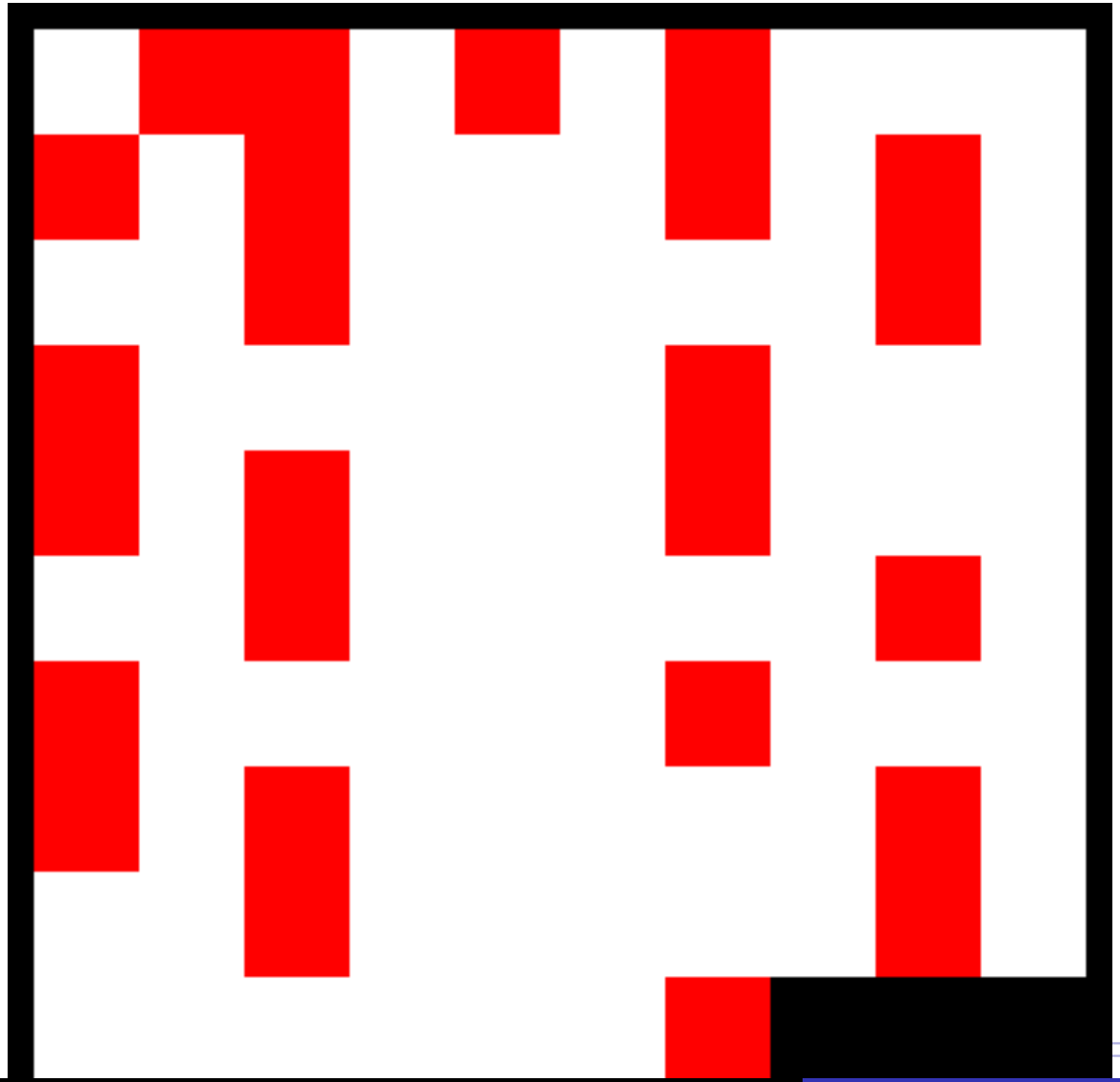
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97			

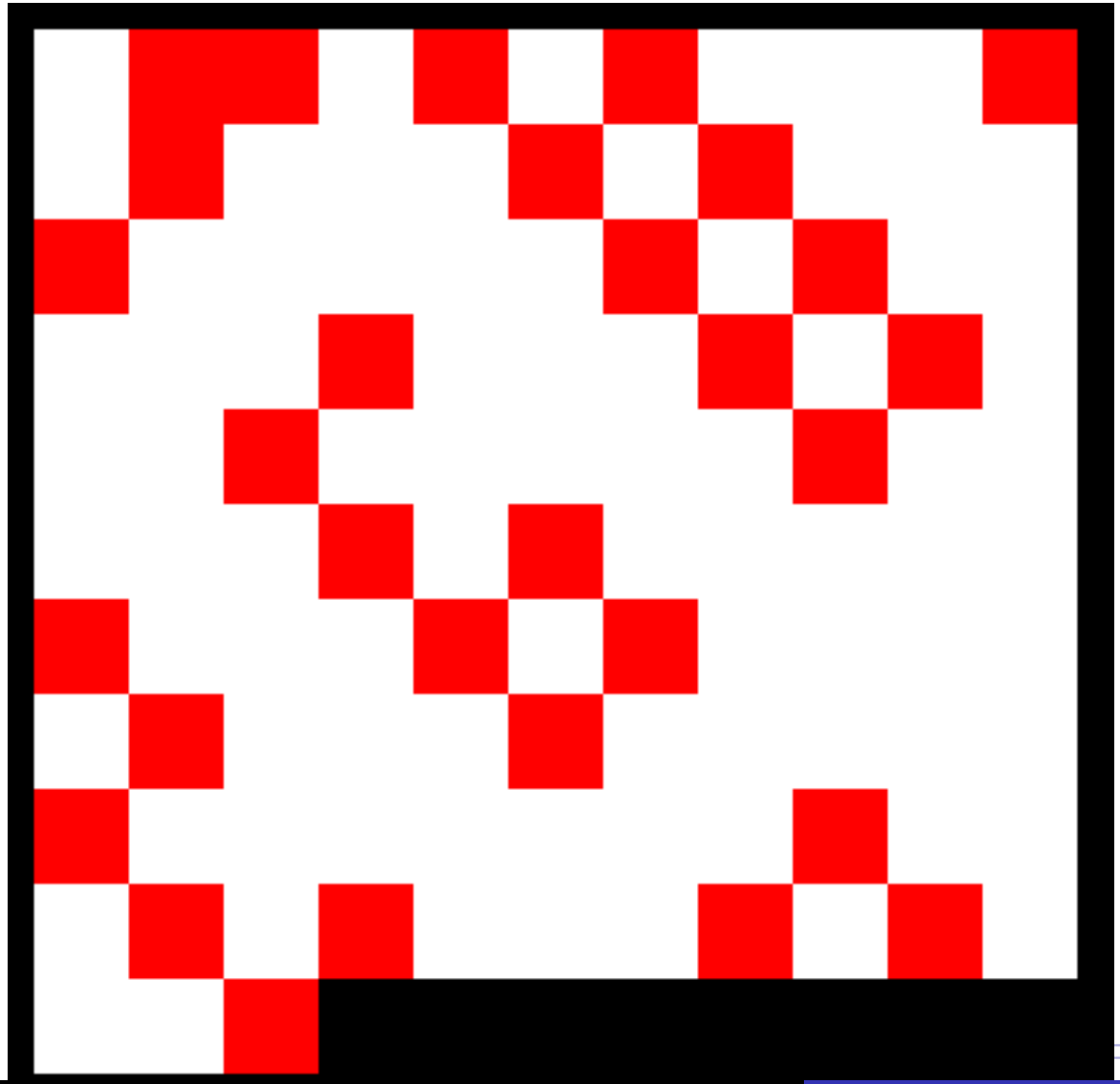
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



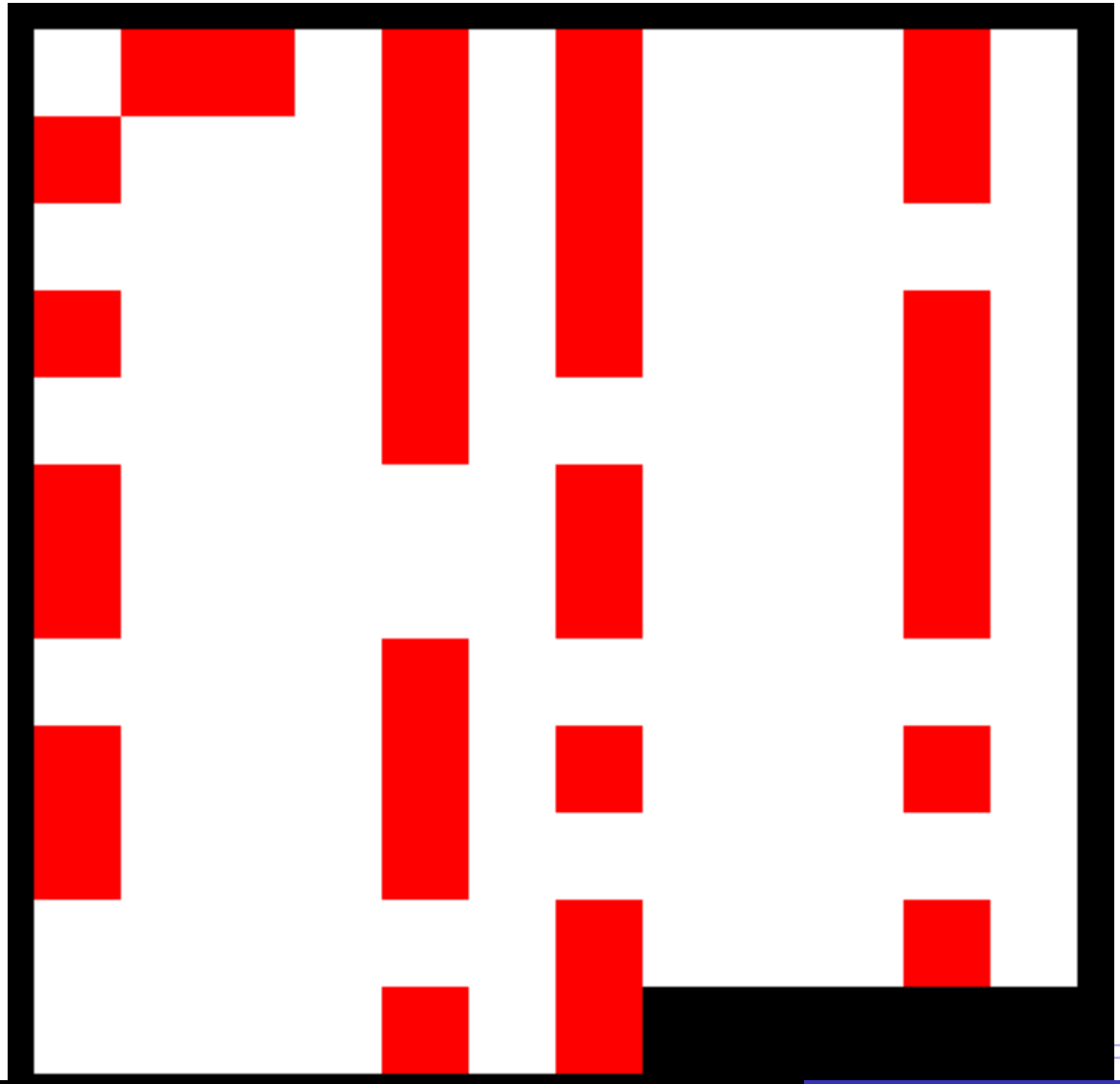
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



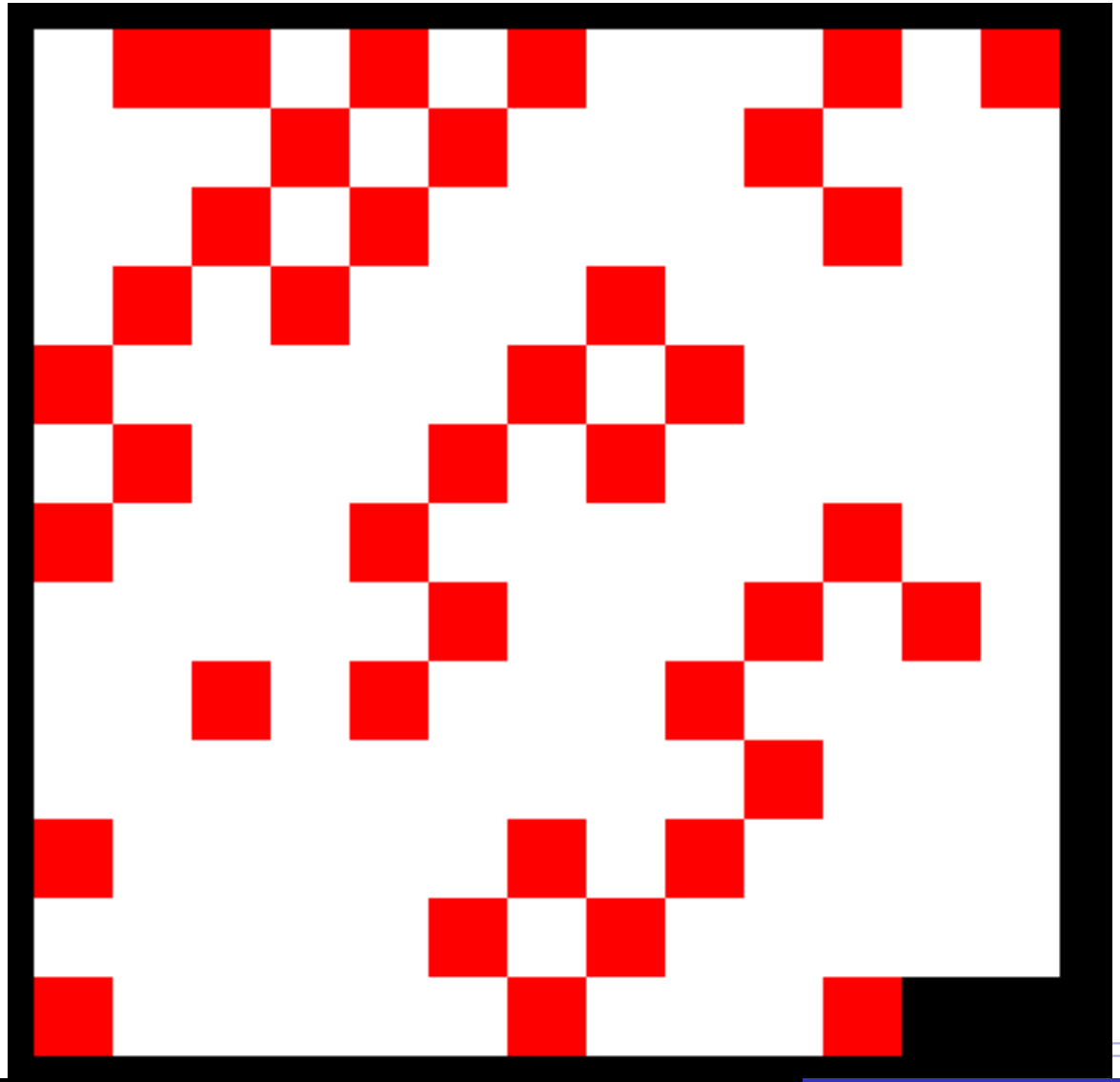
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



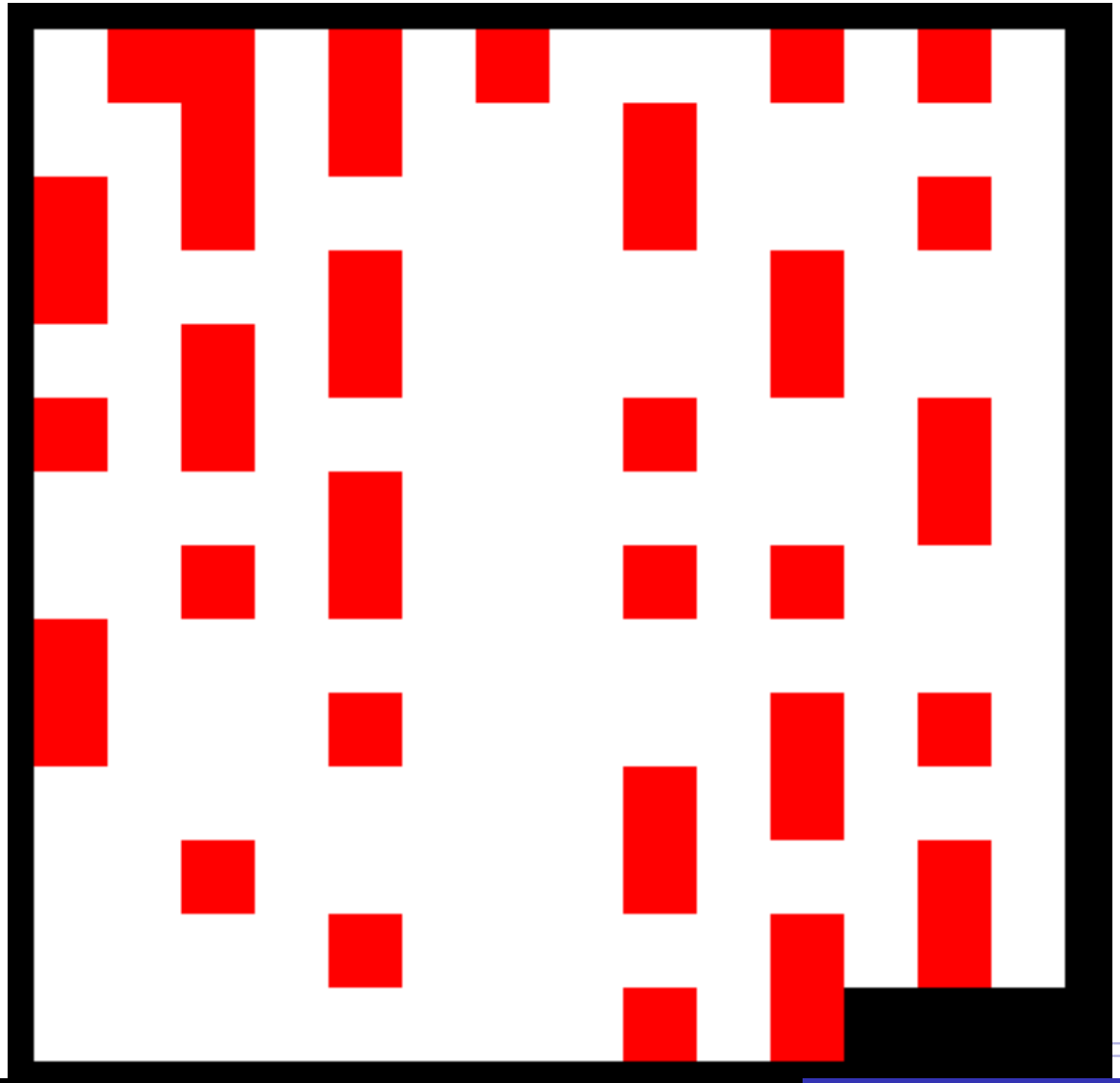
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



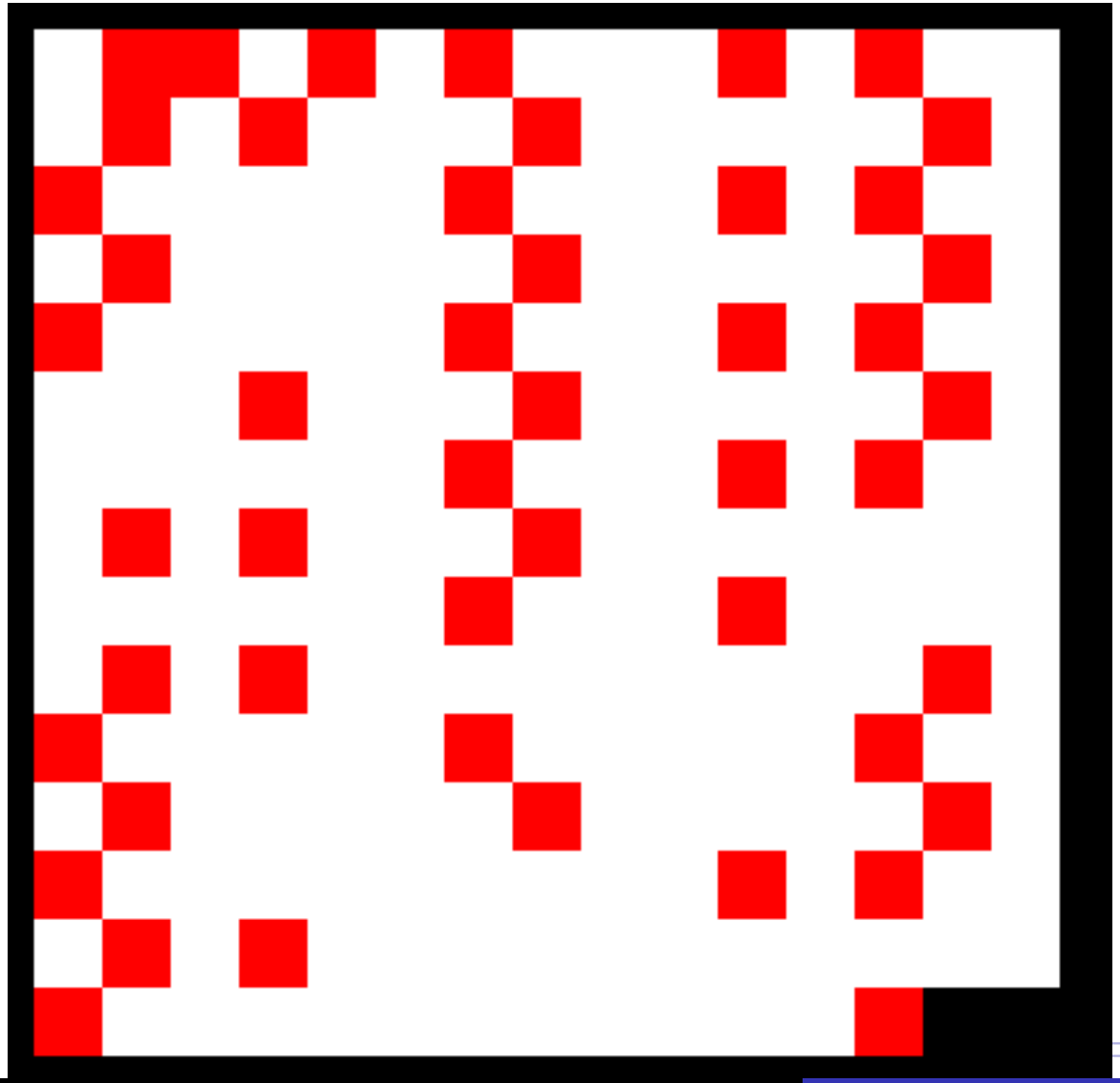
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



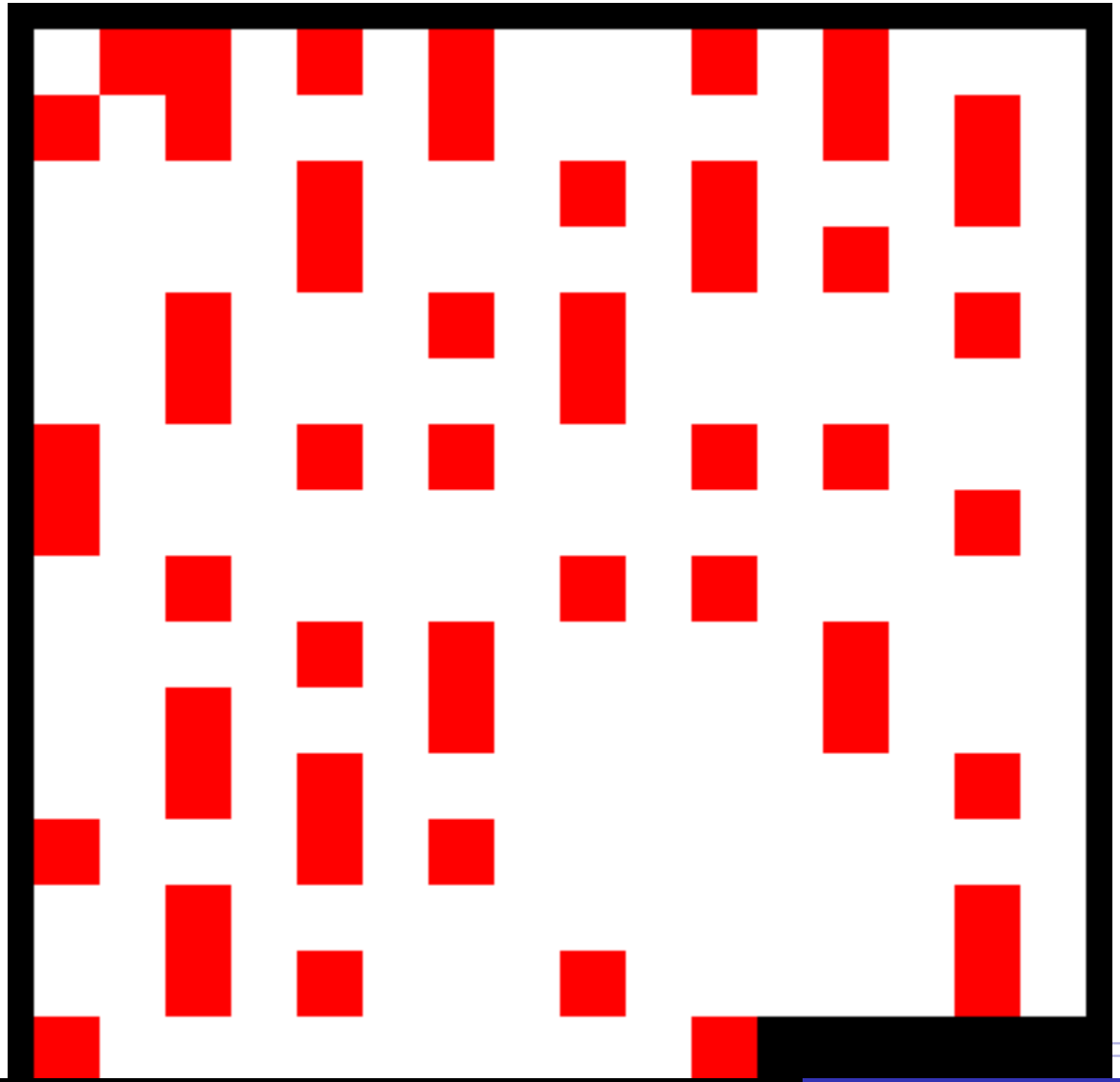
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



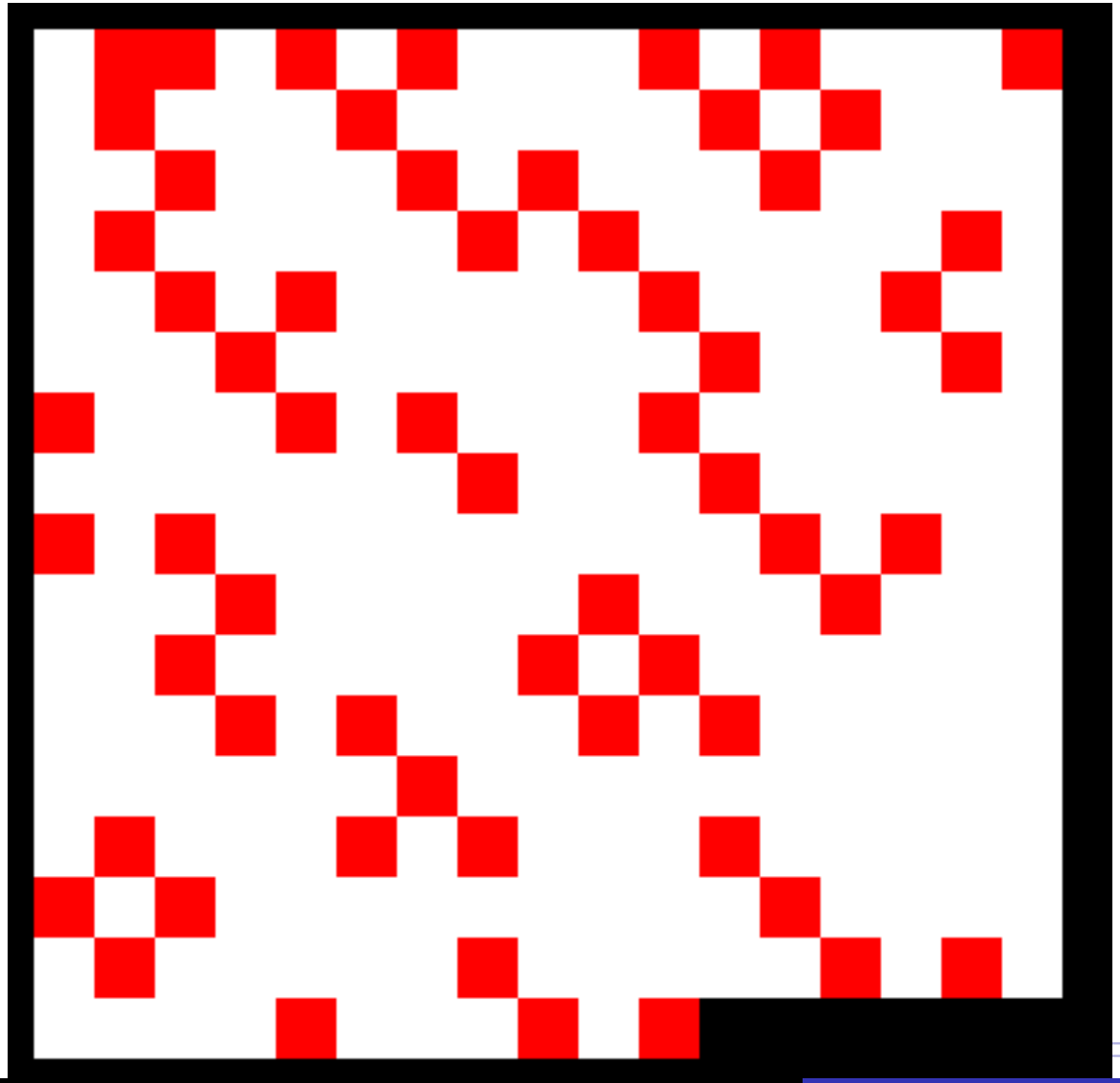
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



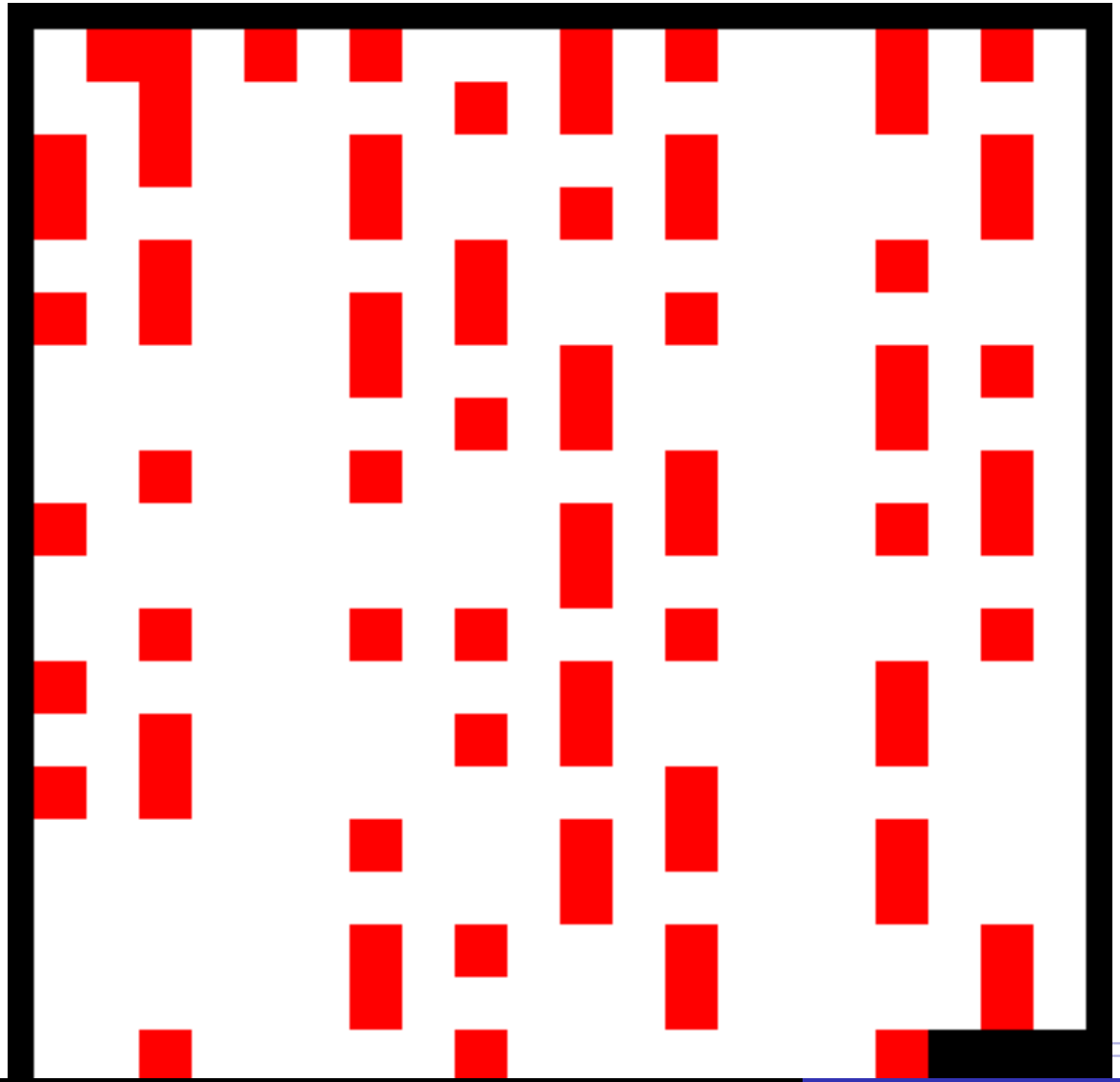
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



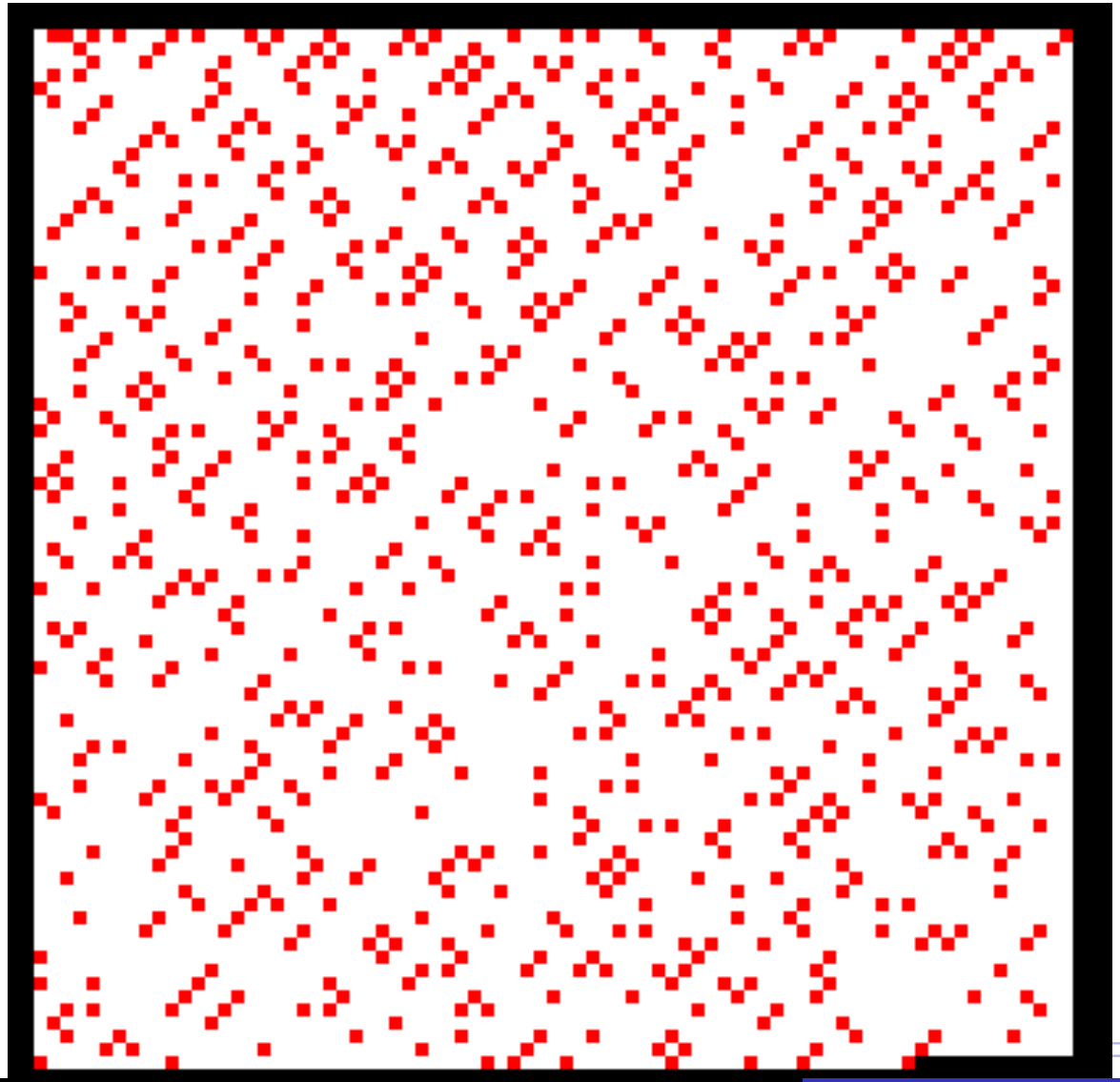
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



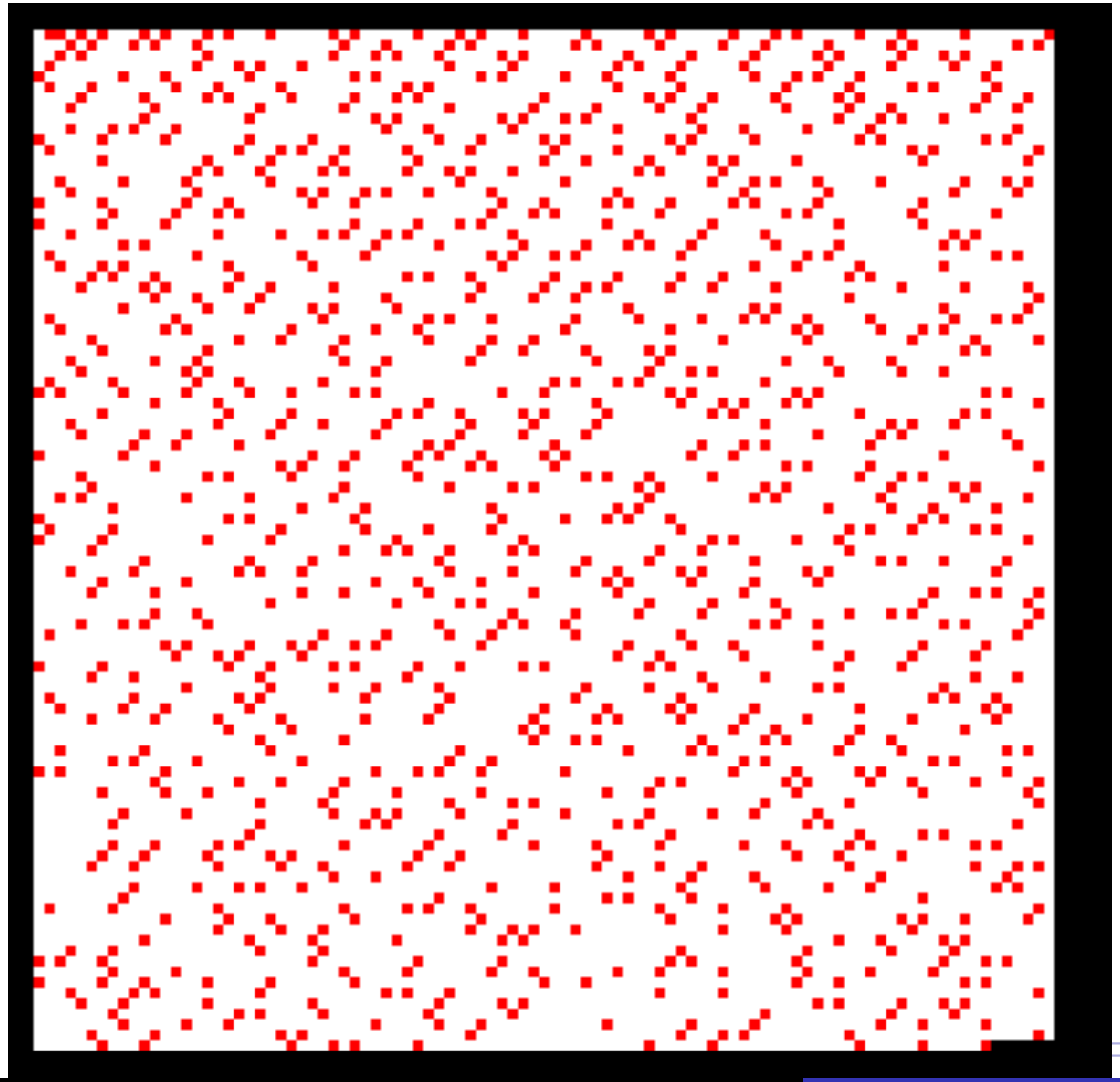
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



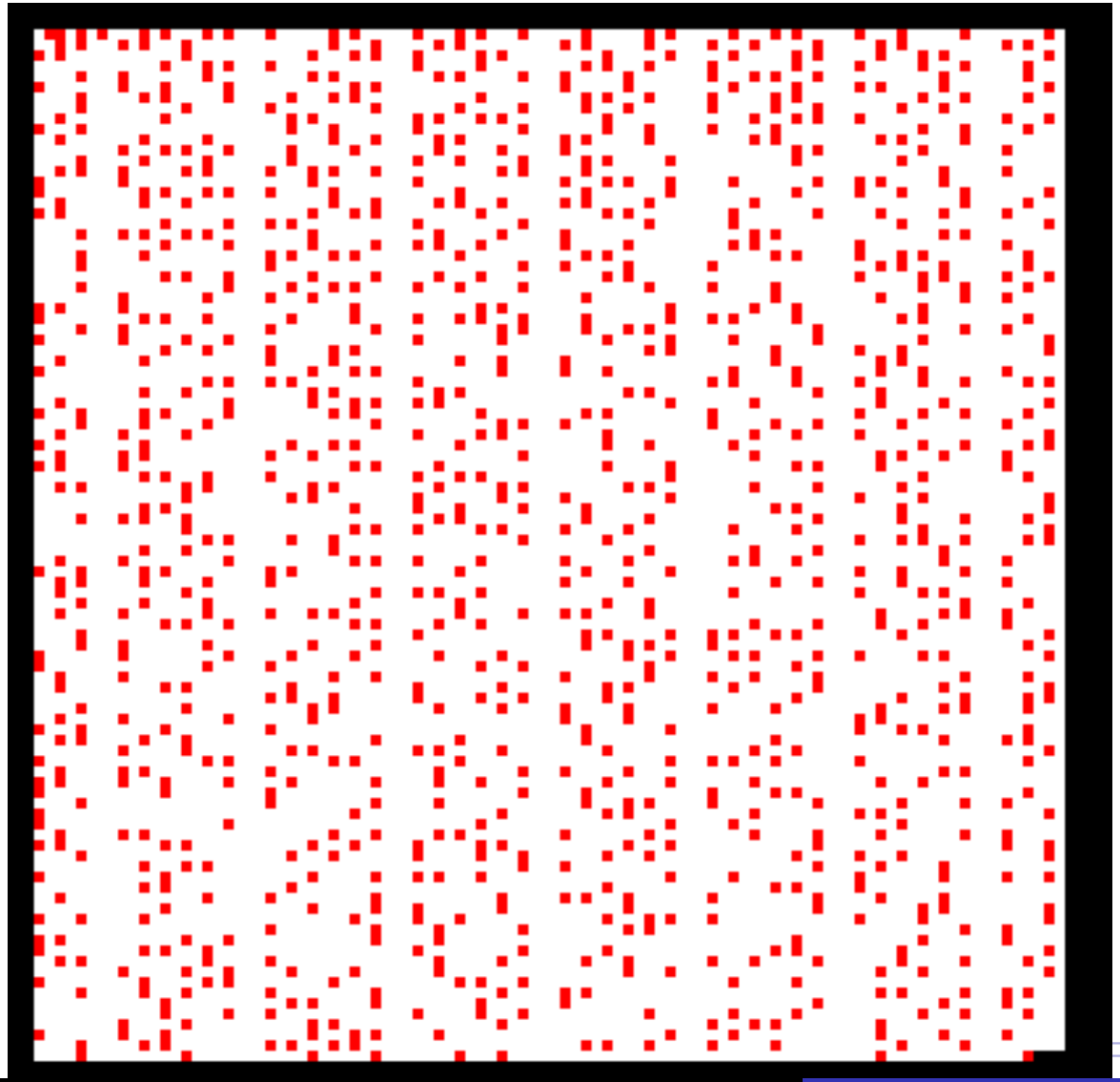
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



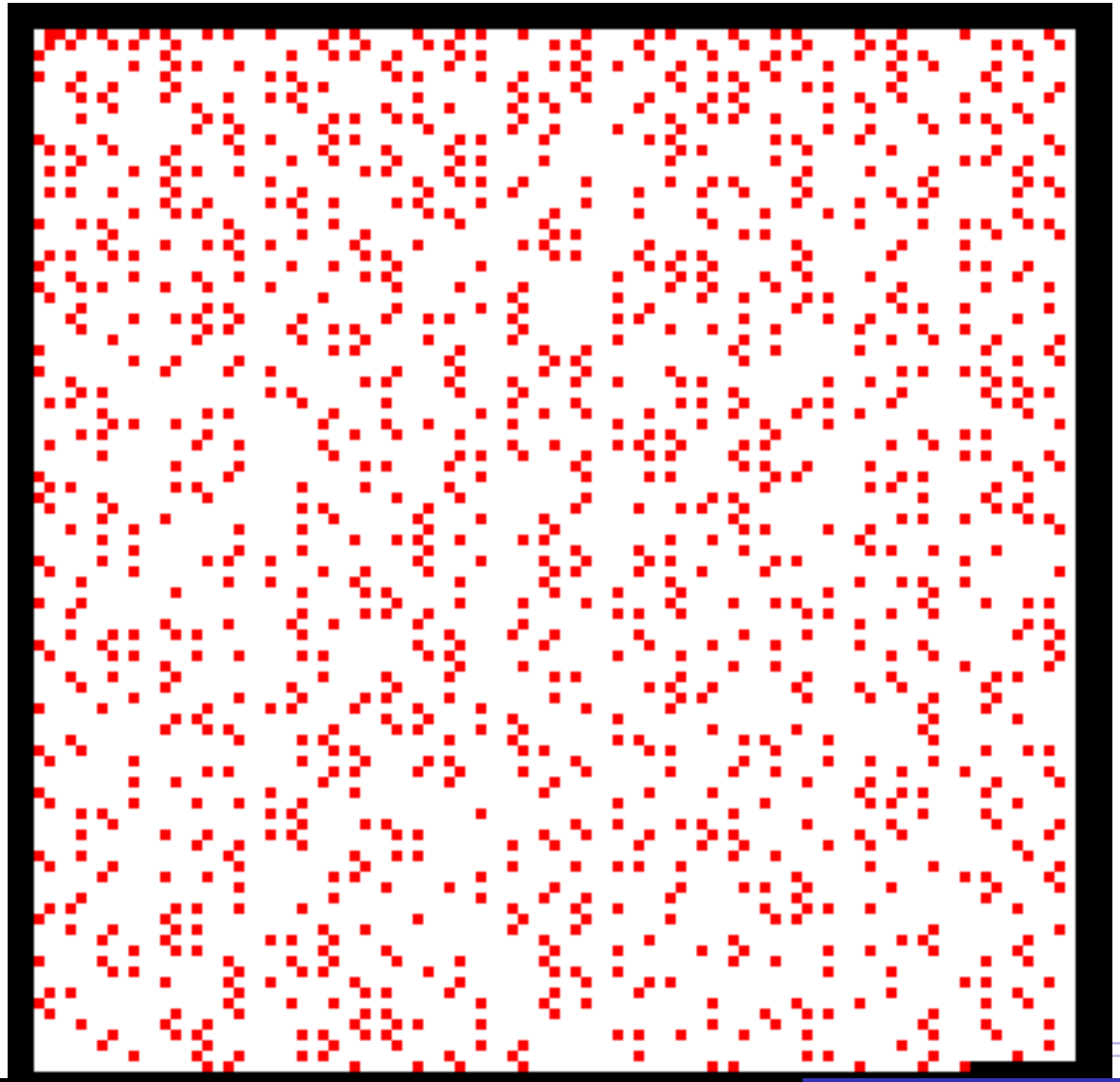
Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



Os primos: de Eratosthenes a Gauss

O "corte" de Eratosthenes



Os primos: de Eratosthenes a Gauss

A fórmula mágica

- há padrões?

Os primos: de Eratosthenes a Gauss

A fórmula mágica

- há padrões?
- há alguma fórmula mágica que me dê todos os primos?

Os primos: de Eratosthenes a Gauss

A fórmula mágica

- há padrões?
- há alguma fórmula mágica que me dê todos os primos?
- . . . e só alguns? Eu ouvi falar dos primos de Fermat $(2^{2^n} + 1)$ e de Mersenne. . .

Os primos: de Eratosthenes a Gauss

Mudando de estratégia

- Gauss e as suas tabelas de logaritmos e primos

Os primos: de Eratosthenes a Gauss

Mudando de estratégia

- Gauss e as suas tabelas de logaritmos e primos
- e se eu contar o número de primos até x?

Os primos: de Eratosthenes a Gauss

Mudando de estratégia

- Gauss e as suas tabelas de logaritmos e primos
- e se eu contar o número de primos até x?
- vou chamar "o número de primos até x" de $\pi(x)$!

Os primos: de Eratosthenes a Gauss

Mudando de estratégia

- Gauss e as suas tabelas de logaritmos e primos
- e se eu contar o número de primos até x?
- vou chamar "o número de primos até x" de $\pi(x)$!
- $\ldots \sim \frac{x}{\log x}$?

Os primos: de Eratosthenes a Gauss

Mudando de estratégia

- Gauss e as suas tabelas de logaritmos e primos
- e se eu contar o número de primos até x?
- vou chamar "o número de primos até x" de $\pi(x)$!
- $\ldots \sim \frac{x}{\log x}$?
- $\frac{\pi(x)}{x/\log x} \longrightarrow 1$!

Os primos: de Eratosthenes a Gauss

Mudando de estratégia

- Gauss e as suas tabelas de logaritmos e primos
- e se eu contar o número de primos até x?
- vou chamar "o número de primos até x" de $\pi(x)$!
- $\ldots \sim \frac{x}{\log x}$?
- $\frac{\pi(x)}{x/\log x} \longrightarrow 1$!
- . . . mas o erro ainda é grande. . .

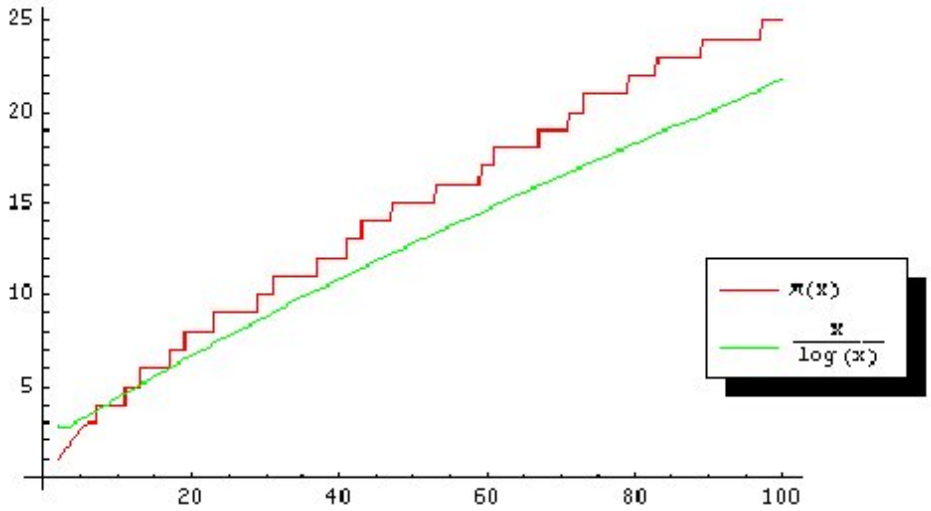
Os primos: de Eratosthenes a Gauss

Mudando de estratégia

- Gauss e as suas tabelas de logaritmos e primos
- e se eu contar o número de primos até x?
- vou chamar "o número de primos até x" de $\pi(x)$!
- $\ldots \sim \frac{x}{\log x}$?
- $\frac{\pi(x)}{x/\log x} \longrightarrow 1$!
- . . . mas o erro ainda é grande. . .
- $\ldots \sim Li(x) = \int_2^x \frac{dt}{\log t}$?

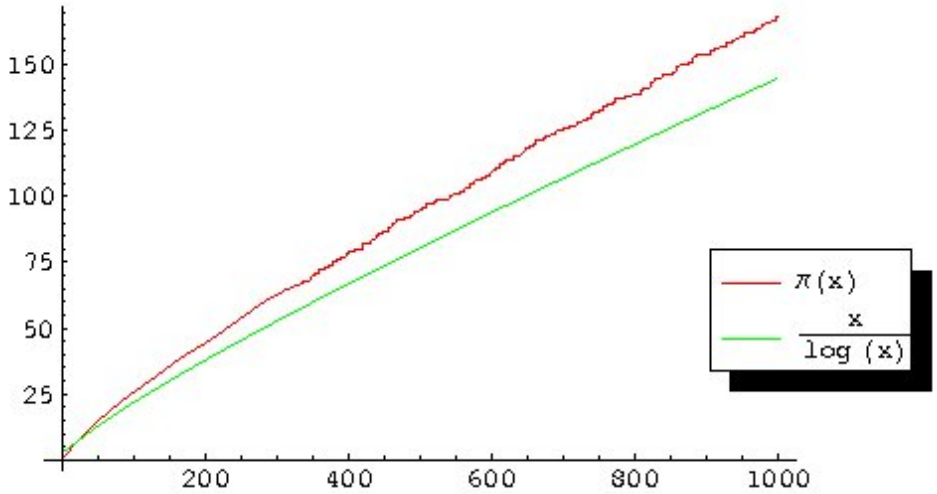
Os primos: de Eratosthenes a Gauss

testemos. . .



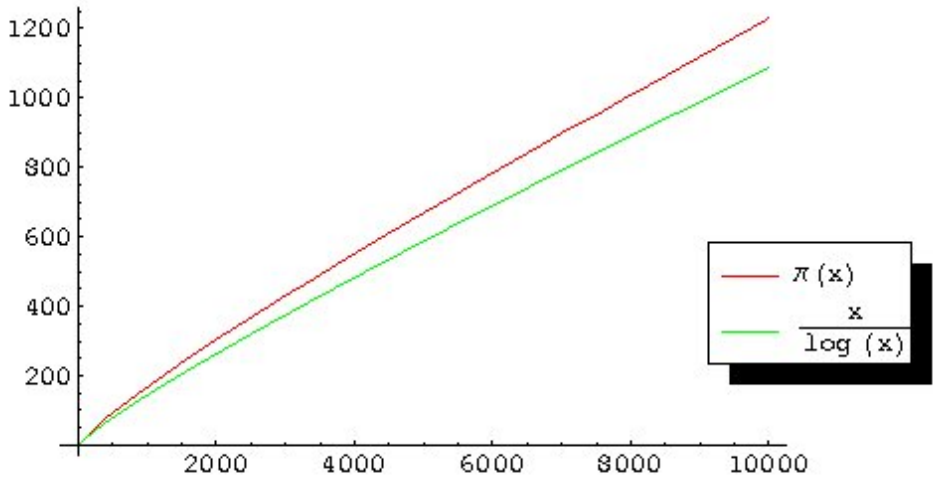
Os primos: de Eratosthenes a Gauss

testemos. . .



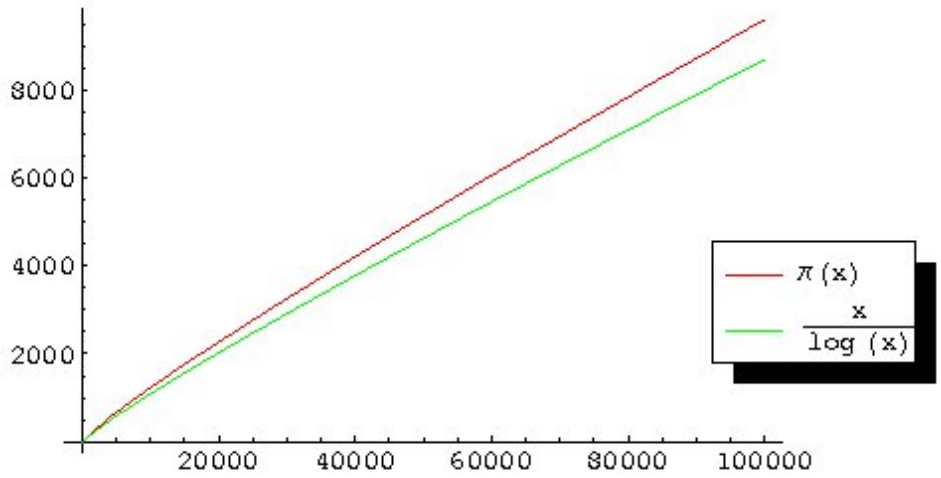
Os primos: de Eratosthenes a Gauss

testemos. . .



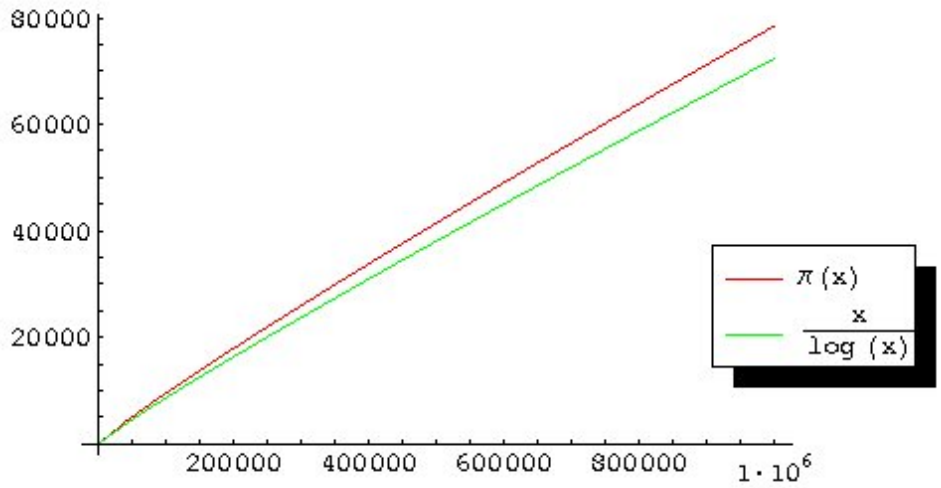
Os primos: de Eratosthenes a Gauss

testemos. . .



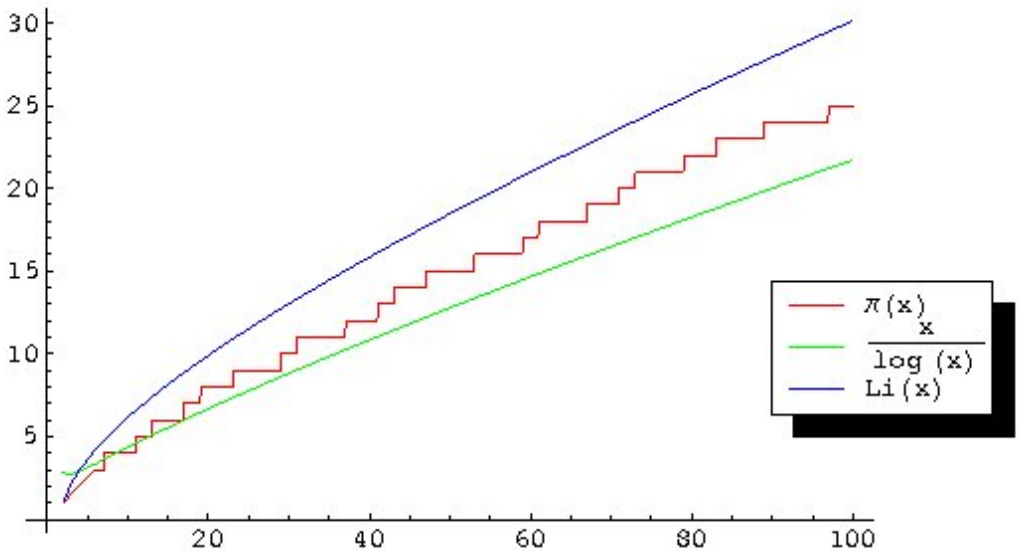
Os primos: de Eratosthenes a Gauss

testemos. . .



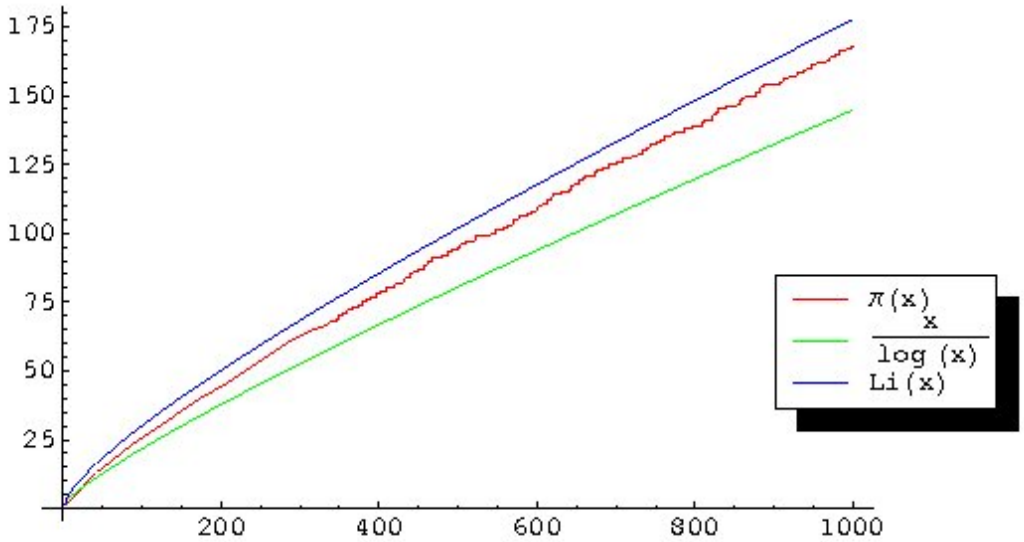
Os primos: de Eratosthenes a Gauss

testemos. . .



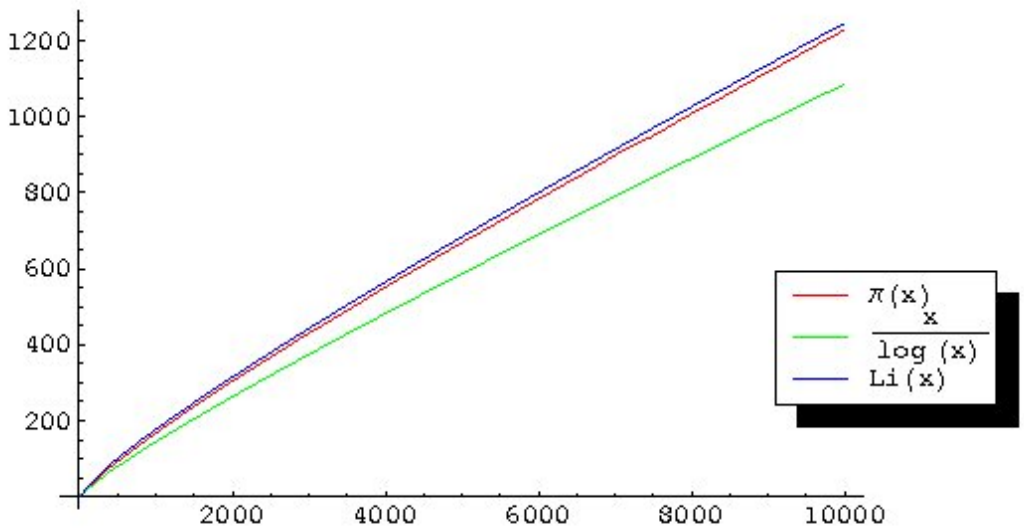
Os primos: de Eratosthenes a Gauss

testemos. . .



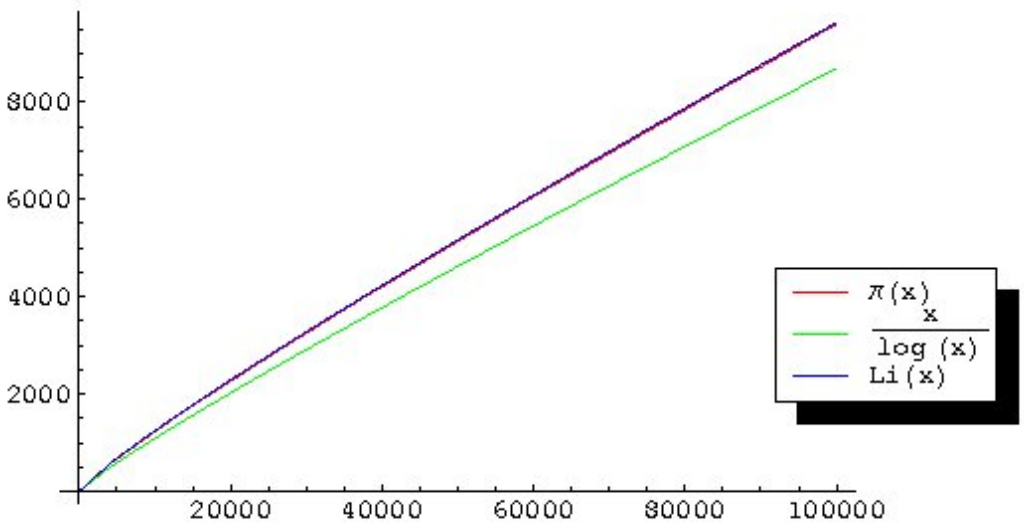
Os primos: de Eratosthenes a Gauss

testemos. . .



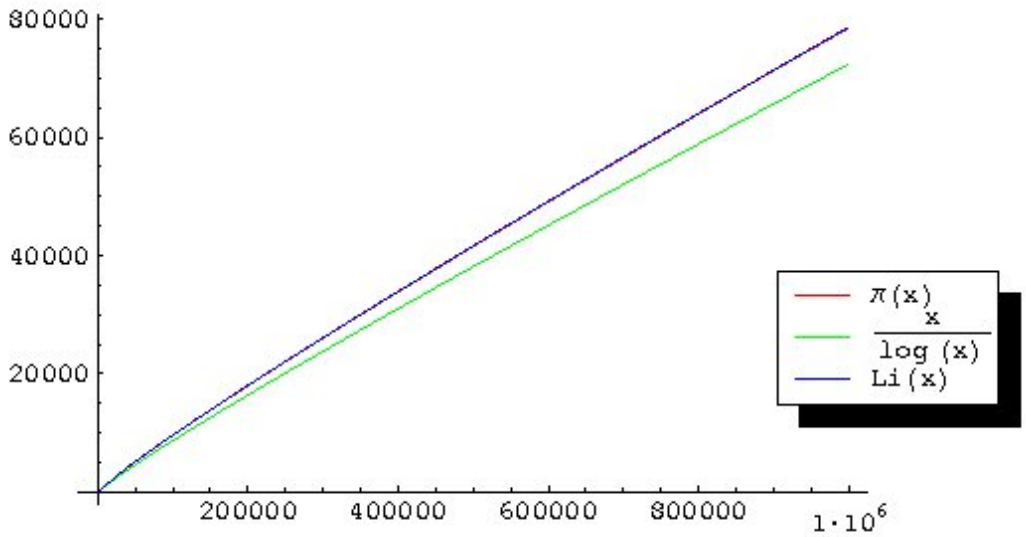
Os primos: de Eratosthenes a Gauss

testemos. . .



Os primos: de Eratosthenes a Gauss

testemos. . .



Riemann, o aluno de Gauss

A misteriosa função Zeta de Riemann...

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad Re(s) > 1 \tag{1}$$

Riemann, o aluno de Gauss

A misteriosa função Zeta de Riemann...

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad Re(s) > 1 \tag{1}$$

- $\zeta(1) = \sum \frac{1}{n}$ - séries harmonianas, $\rightarrow \infty$

Riemann, o aluno de Gauss

A misteriosa função Zeta de Riemann...

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad Re(s) > 1 \tag{1}$$

- $\zeta(1) = \sum \frac{1}{n}$ - séries harmonianas, $\rightarrow \infty$
- $\zeta(2) = \sum \frac{1}{n^2}$ - série de Basel , converge... para $\pi^2/6$ (disse o Euler!)

Riemann, o aluno de Gauss

A misteriosa função Zeta de Riemann...

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad Re(s) > 1 \tag{1}$$

- $\zeta(1) = \sum \frac{1}{n}$ - séries harmonianas, $\rightarrow \infty$
- $\zeta(2) = \sum \frac{1}{n^2}$ - série de Basel , converge... para $\pi^2/6$ (disse o Euler!)
- $\zeta(s)$ converge!

Riemann, o aluno de Gauss

A misteriosa função Zeta de Riemann...

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad Re(s) > 1 \tag{1}$$

- $\zeta(1) = \sum \frac{1}{n}$ - séries harmonianas, $\rightarrow \infty$
- $\zeta(2) = \sum \frac{1}{n^2}$ - série de Basel , converge... para $\pi^2/6$ (disse o Euler!)
- $\zeta(s)$ converge!
- ...e é igual a $\prod_p \frac{1}{(1-p^{-s})}$

Riemann, o aluno de Gauss

A misteriosa função Zeta de Riemann...

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad Re(s) > 1 \tag{1}$$

- $\zeta(1) = \sum \frac{1}{n}$ - séries harmonianas, $\rightarrow \infty$
- $\zeta(2) = \sum \frac{1}{n^2}$ - série de Basel , converge... para $\pi^2/6$ (disse o Euler!)
- $\zeta(s)$ converge!
- ...e é igual a $\prod_p \frac{1}{(1-p^{-s})}$
- ...e depois?

Riemann, o aluno de Gauss

Olha o π !

- Probabilidade de dois números aleatórios serem co-primos? $1/\zeta(2)$

Riemann, o aluno de Gauss

Olha o π !

- Probabilidade de dois números aleatórios serem co-primos? $1/\zeta(2)$
- Probabilidade de um número aleatório ser square-free? $1/\zeta(2)$

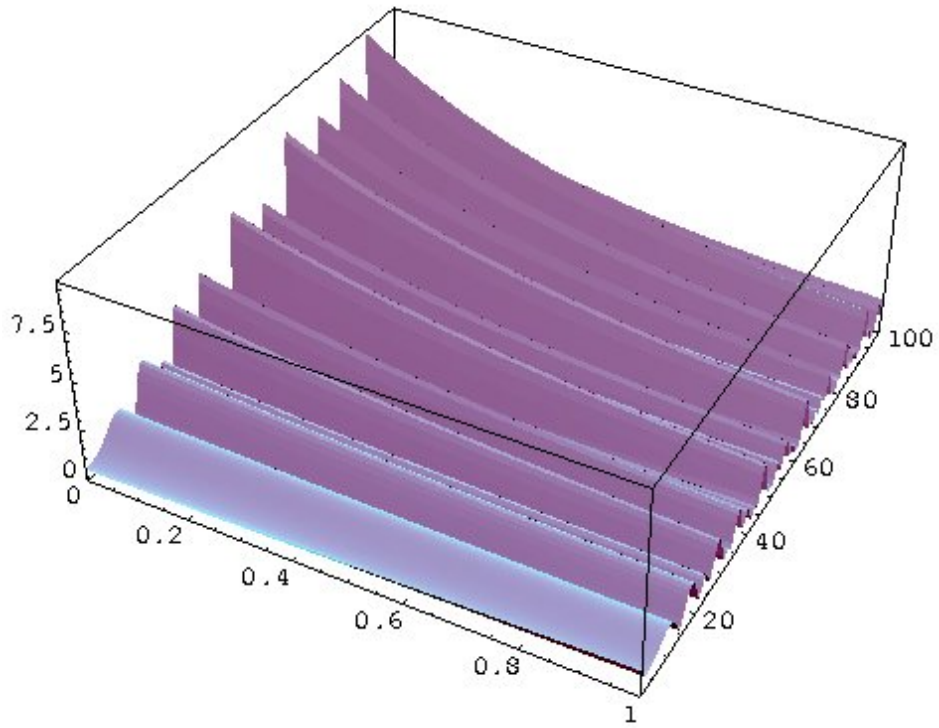
Riemann, o aluno de Gauss

Olha o π !

- Probabilidade de dois números aleatórios serem co-primos? $1/\zeta(2)$
- Probabilidade de um número aleatório ser square-free? $1/\zeta(2)$
- . . . mas que tem isto a ver com o outro π, o $\pi(x)$?

Riemann, o aluno de Gauss

Riemann e as suas abstracções



. . . se o gráfico diz uma coisa, e a equação diz outra, em quem acreditar?

Riemann, o aluno de Gauss

Riemann e as suas abstracções

- extender a definição para $Re(s) < 1$

Riemann, o aluno de Gauss

Riemann e as suas abstracções

- extender a definição para $Re(s) < 1$
- $$\zeta(s) = 2^s \pi^{s-1} \Gamma(1-s) \zeta(1-s) sin(\pi s/2) \qquad (2)$$

Riemann, o aluno de Gauss

Riemann e as suas abstracções

- extender a definição para $Re(s) < 1$
- $$\zeta(s) = 2^s \pi^{s-1} \Gamma(1-s) \zeta(1-s) sin(\pi s/2) \qquad (2)$$
- zeros triviais quando $sin(\pi s/2) = 0$: $-2, -4, -6, \ldots$

Riemann, o aluno de Gauss

Riemann e as suas abstracções

- extender a definição para $Re(s) < 1$
- $$\zeta(s) = 2^s \pi^{s-1} \Gamma(1-s) \zeta(1-s) sin(\pi s/2) \qquad (2)$$
- zeros triviais quando $sin(\pi s/2) = 0$: $-2, -4, -6, \ldots$
- $Re(s) < 0$? simples!

Riemann, o aluno de Gauss

Riemann e as suas abstracções

- extender a definição para $Re(s) < 1$
- $$\zeta(s) = 2^s \pi^{s-1} \Gamma(1-s) \zeta(1-s) sin(\pi s/2) \qquad (2)$$
- zeros triviais quando $sin(\pi s/2) = 0$: $-2, -4, -6, \ldots$
- $Re(s) < 0$? simples!
- $0 \leq Re(s) \leq 1$? a tira crítica. . . onde todos os zeros não triviais estão

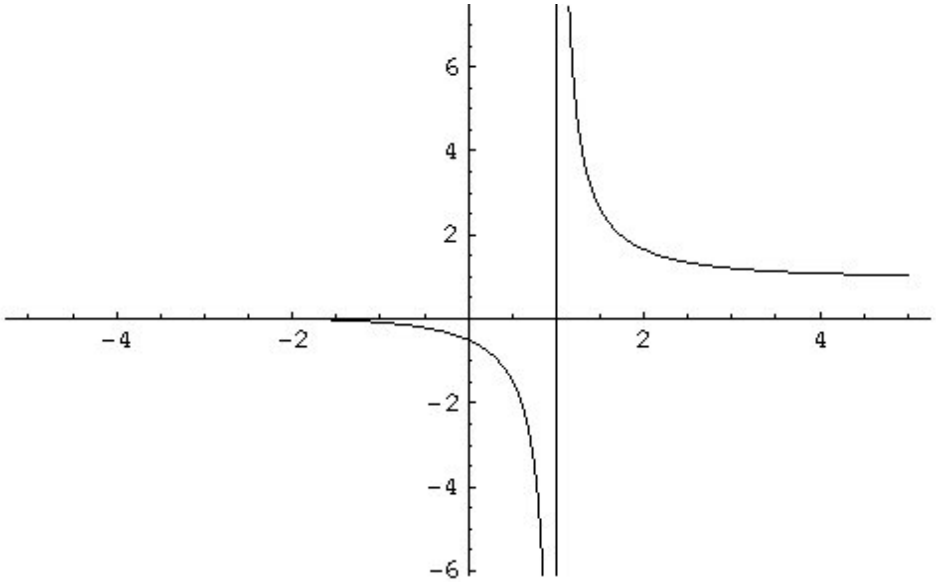
Riemann, o aluno de Gauss

Riemann e as suas abstracções

- extender a definição para $Re(s) < 1$
- $$\zeta(s) = 2^s \pi^{s-1} \Gamma(1-s) \zeta(1-s) sin(\pi s/2) \qquad (2)$$
- zeros triviais quando $sin(\pi s/2) = 0$: $-2, -4, -6, \ldots$
- $Re(s) < 0$? simples!
- $0 \leq Re(s) \leq 1$? a tira crítica. . . onde todos os zeros não triviais estão
- **Desafio para a audiência**: prove que todos os zeros tem $Re(s) = 1/2$, isto é, são da forma $s = 1/2 + it$, para um t qualquer. . .

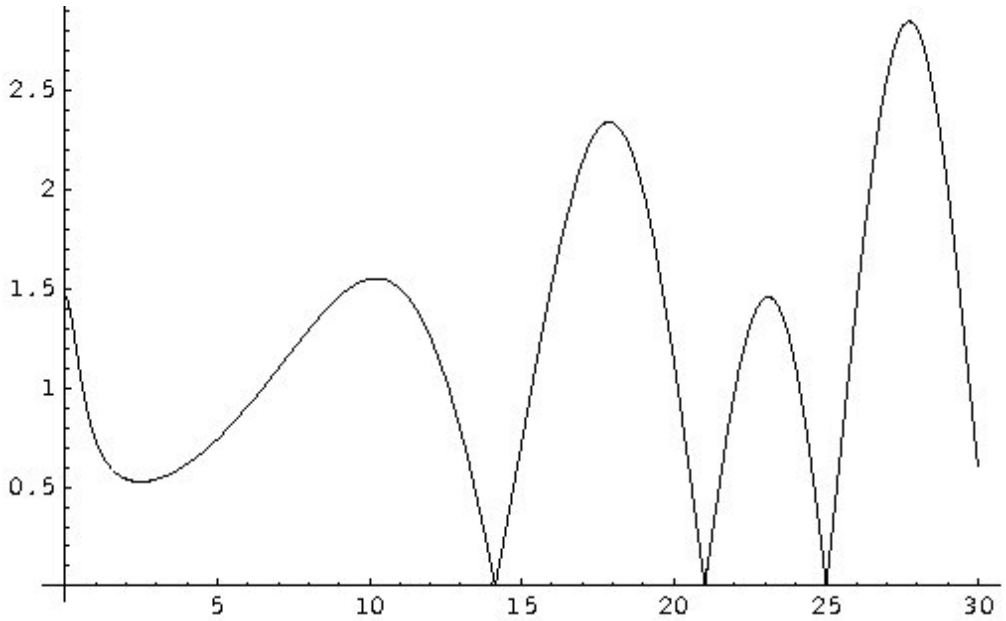
Riemann, o aluno de Gauss

Imagens talvez ajudem. . .



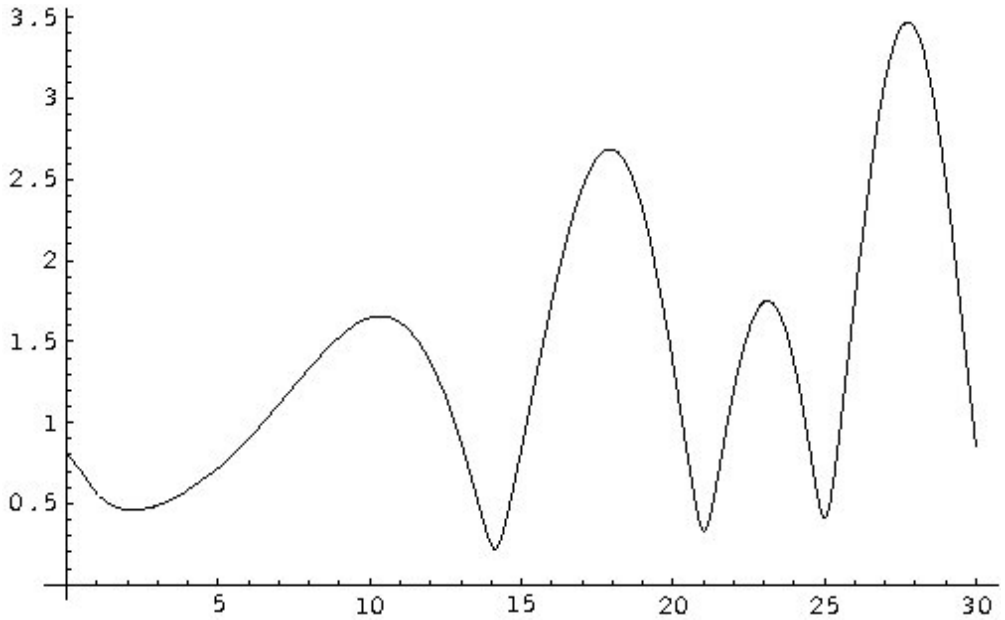
Riemann, o aluno de Gauss

Imagens talvez ajudem. . .



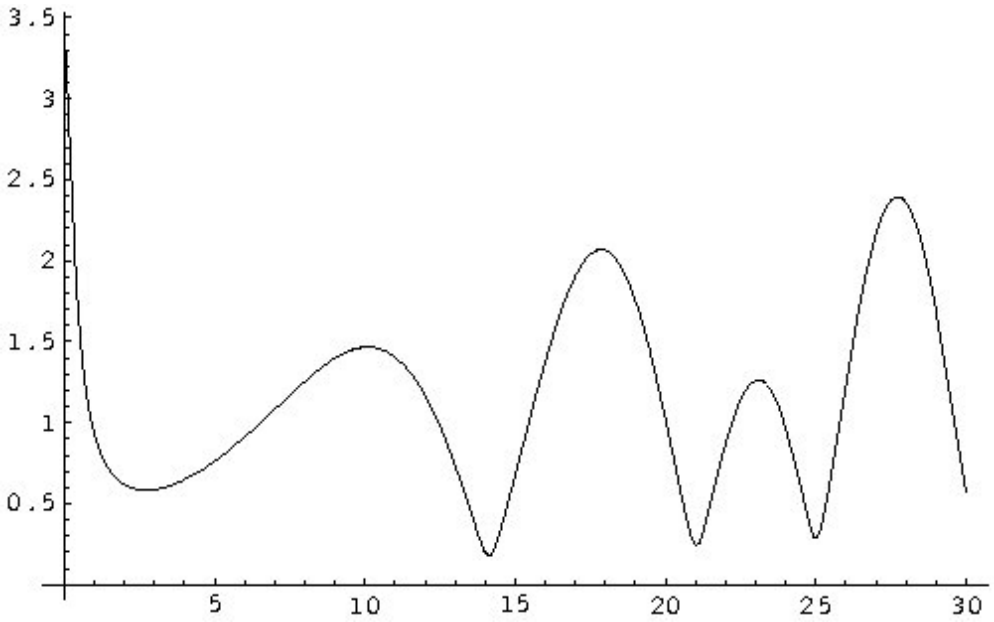
Riemann, o aluno de Gauss

Imagens talvez ajudem. . .



Riemann, o aluno de Gauss

Imagens talvez ajudem. . .



Riemann, o aluno de Gauss

E depois?!

- Riemann mostra que há uma expressão que relaciona $\pi(x)$ e $\zeta(s)$ *precisamente!*

Riemann, o aluno de Gauss

E depois?!

- Riemann mostra que há uma expressão que relaciona $\pi(x)$ e $\zeta(s)$ *precisamente!*
- daí, definiu 2 funções, $R(x)$ e $R'_{\omega}(x)\ldots$

Riemann, o aluno de Gauss

E depois?!

- Riemann mostra que há uma expressão que relaciona $\pi(x)$ e $\zeta(s)$ *precisamente!*
- daí, definiu 2 funções, $R(x)$ e $R'_{\omega}(x)\ldots$
- $R(x)$ é parecida com $Li(x)\ldots$

Riemann, o aluno de Gauss

E depois?!

- Riemann mostra que há uma expressão que relaciona $\pi(x)$ e $\zeta(s)$ *precisamente!*
- daí, definiu 2 funções, $R(x)$ e $R'_\omega(x)\ldots$
- $R(x)$ é parecida com $Li(x)\ldots$
- $R'_\omega(x)$ é o erro, calculado com base nos zeros ω de $\zeta(s)$

Riemann, o aluno de Gauss

uma melhor aproximação do erro

- sem a hipótese de Riemann?
  $\sim O(x \exp(-A \log(x)^{3/5}/(\log\log(x)^{1/5})))$

Riemann, o aluno de Gauss

uma melhor aproximação do erro

- sem a hipótese de Riemann?
  $\sim O(x \exp(-A \log(x)^{3/5}/(\log\log(x)^{1/5})))$
- com a hipótese de Riemann? $\leq C\sqrt{x}\log x$

Mas falemos de coisas práticas

- RSA e a dificuldade de factorizar $n = pq$, p, q primos de 512 bits...

Mas falemos de coisas práticas

- RSA e a dificuldade de factorizar $n = pq$, p, q primos de 512 bits...
- testar se um número é primo?

Mas falemos de coisas práticas

- RSA e a dificuldade de factorizar $n = pq$, p, q primos de 512 bits...
- testar se um número é primo?
- a hipótese generalisada... a diferença entre procurar ao calha e procurar por ordem... um número gerador

Mas falemos de coisas práticas

- RSA e a dificuldade de factorizar $n = pq$, p, q primos de 512 bits...
- testar se um número é primo?
- a hipótese generalisada... a diferença entre procurar ao calha e procurar por ordem... um número gerador
- matrizes aleatórias e o GUE... mas não me perguntem...

Perguntas

E uma boa noite de sono. . .