Faculdade Ciências e Tecnologias
Departamento de Matemática
Actividades Matemáticas

A Primazia dos primos

Catarina Silva/ Pedro Ribeiro / José Gaspar

14 de Março de 2011

O que é um número primo ?

Um número primo é um número natural maior que 1 com exactamente dois divisores naturais distintos, o 1 e ele próprio.

Exemplos ?

E um número Composto ?

Um número composto é um número natural, maior que 1, que tem mais de dois divisores.

Exemplos ?

Um pouca de História/Aplicações

- Os números Primos e suas propriedades foram primeiramente estudados pelos antigos matemáticos Gregos.
- O primeiro algoritmo surgiu em 200 a.C.
- É no séc. XVII que estes números mágicos ganham interesse e tamanho. Com o passar dos anos surgiu a necessidade de registar os últimos números primos.
- Na actualidade, para além de tabelas, existem imensas fórmulas e algoritmos para achar primos gigantes. São estes primos que através de propriedades de factorização protegem chaves públicas.

Critérios de divisibilidade

- Se o número é divisível por 5, então termina em zero ou em 5.
- Se o número é divisível por 2, tem de ser par.
- Se o número é divisível por 3 , então a soma dos algarismos do número também o é.
- Um número é divisível por 7 quando a diferença entre o dobro do último algarismo e o número formado pelos restantes é divisível por 7.
- Um número é divisível por 11 quando a diferença entre a soma dos algarismos de ordem impar com os de ordem par é divisível por 11.
- Um número é divisível por 13 quando ao multiplicar o último algarismo por 9 e subtraindo ao restantante, obtemos um múltiplo de 13.

- Se um número n for composto, tem de certeza um factor primo $\leq \sqrt{n}$.

Exemplo, 131

$$\sqrt{131} = 11{,}446$$

$$131 \nmid 2\,, \qquad 131 \nmid 3, \qquad 131 \nmid 5\,, \qquad 131 \nmid 7, \qquad 131 \nmid 11$$

O número 131 não pode ser composto, logo é PRIMO

★1

Eratóstenes (276-194 a.C.)

Bibliotecário na grande biblioteca de Alexandria, é um dos homens mais brilhantes da antiguidade

- ✓ Um dos seus feitos foi a medição do raio da Terra, comparando sombras de dois mastros.
- ✓ Alguns trabalhos sobre teoria de números

Crivo de Eratóstenes (1)

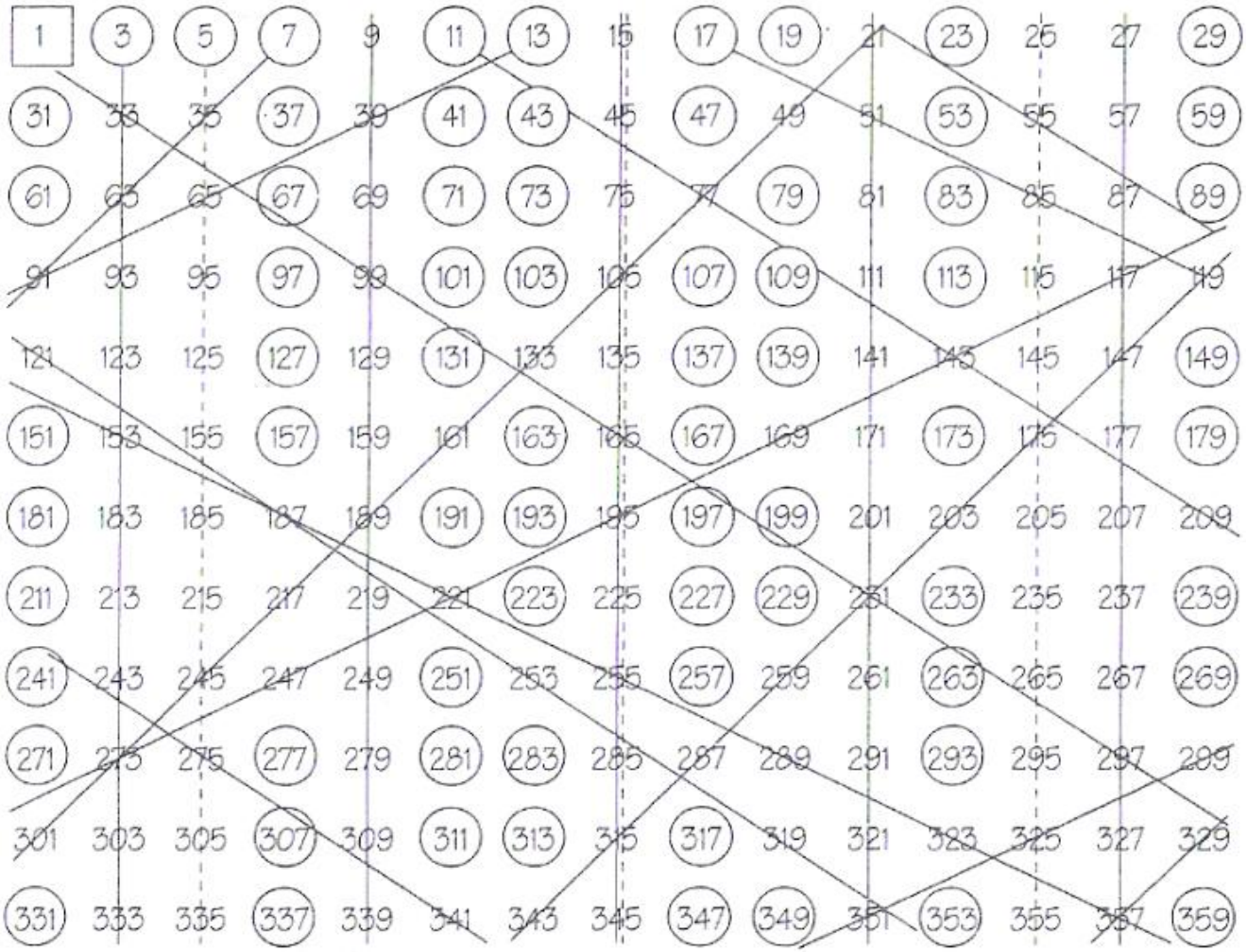
- Tal como o agricultor separa o trigo bom da moinha inútil, assim Eratóstenes usava o seu crivo para separar os preciosos números primos dos seus companheiros compostos

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	98	99	100

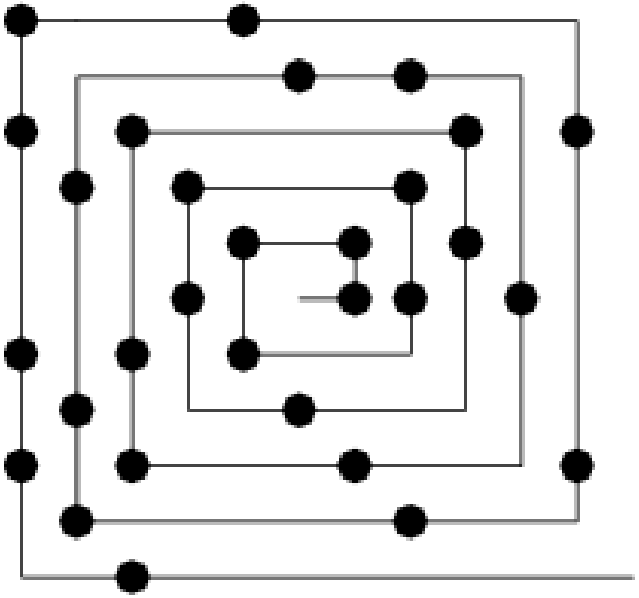
★ 3/2

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	38	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	98	99	100

Crivo de Eratóstenes (2)

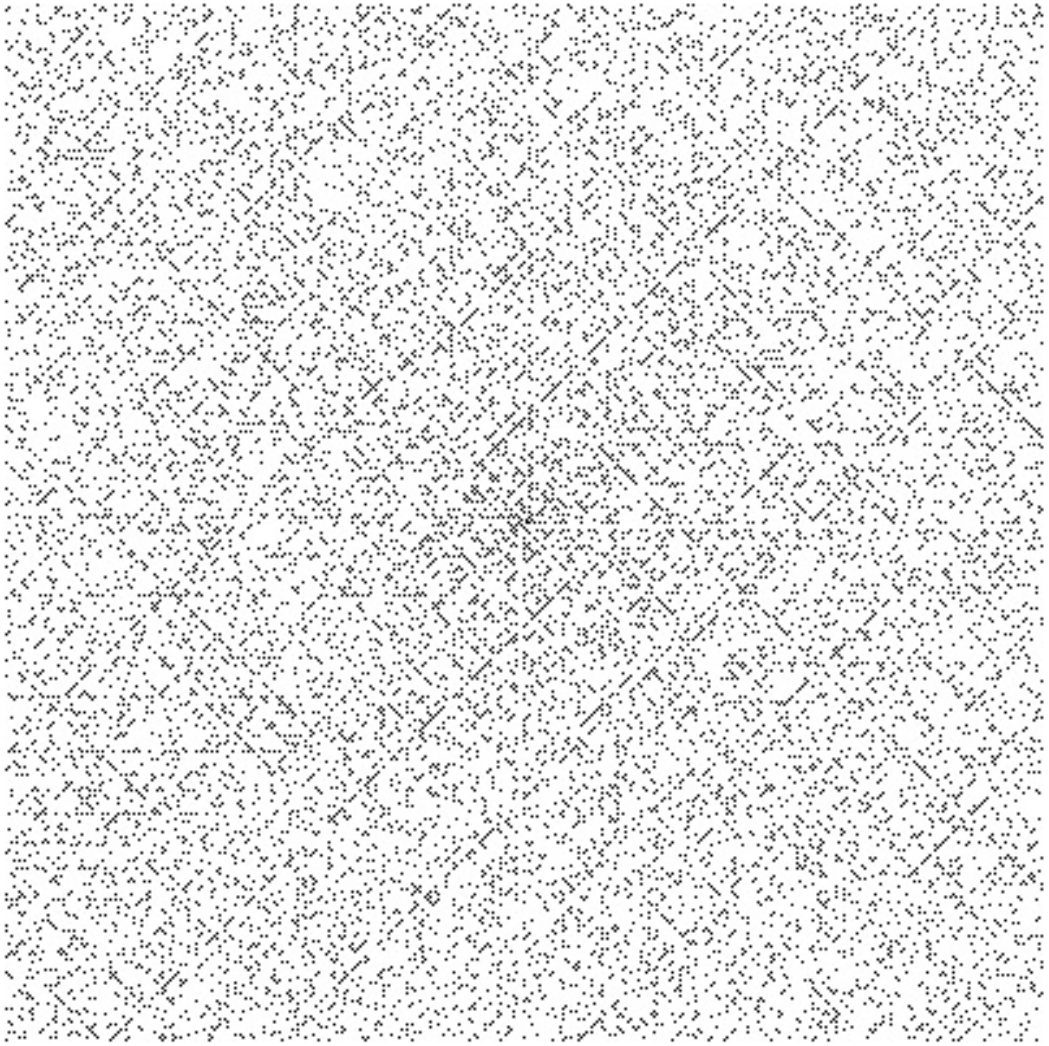


Espiral Ulam's (1)



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

Espiral Ulam's (2)



Euclides (330 a.C. – 260 a.C.)

Euclides foi um professor, **matemático e escritor** em Alexandria, muitas vezes referido como o "Pai da Geometria".

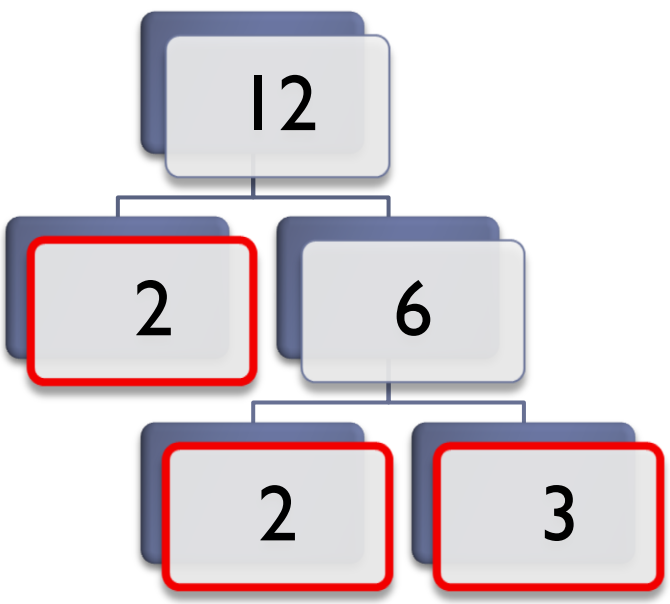
Elementos da Geometria (300 a.C.)

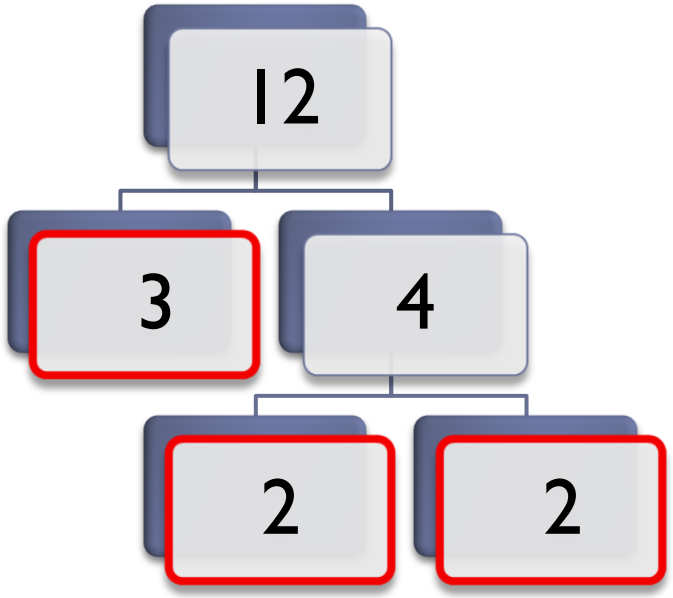
- Livro de Euclides, apresenta uma fundamentação teórica para teoria de números, ou seja a descoberta do seguinte resultado

> Cada número se decompõe num produto de factores primos de forma única

Vamos factorizar em Árvore!

- Consideremos o número 12 (por exemplo)





★ 4

Princípio de Euclides

Para provar que a factorização é unica recorre-se ao Princípio de Euclides, que diz o seguinte

> Um número primo não pode dividir um produto a menos que divida um dos factores

Se um número primo divide uma das factorizações divide certamente algum dos números primos da outra que , portanto, deverá ser ele próprio. Pode então cancelar-se este primo e repetir no remanescente o mesmo tipo de argumento. As duas factorizações podem então diferir, quando muito, na origem dos factores.

Há sempre novos primos!

- Euclides provou que os primos continuam sempre.

O que é que ele fez 

Considerou os primos, 2, 3, 5, 7,11,13 multiplicou-os e adicionou ao resultado obtido uma unidade.

★ 5/6

Marin Mersenne (1588 – 1648)

Marin Mersenne, padre matemático, teórico musical, , teólogo e filósofo francês. Ficou conhecido sobretudo pelo seu trabalho em Teoria dos Números.

- Numa carta a Frenicle de Bessy, Merssene discutiu a existencia de números primos da forma $2^n - 1$ e fez a surpreendente declaração de que

> $2^n - 1$ era primo para $n = 2,3,5,7,13,17,19,31,67,127,257$
> e **para mais nenhum valor de n inferior a 257**.

O que achas?

Ao longo dos tempos, **foram detectados** vários erros na afirmação de Mersenne, tendo ficado claro que tal **descoberta não passava de uma simples conjectura de pessoa culta.**

n	M_n	Digitos em M_n	Data de descobrimento	Descobridor
2	3	1	*antiguidade*	*antiguidade*
3	7	1	*antiguidade*	*antiguidade*
5	31	2	*antiguidade*	*antiguidade*
7	127	3	*antiguidade*	*antiguidade*
13	8.191	4	1456	*anônimo*
17	131.071	6	1588	Cataldi
19	524.287	6	1588	Cataldi
31	2.147.483.647	10	1772	Euler
61	2.305.843.009.213.693.951	19	1883	Pervushin
89	618970019...449.562.111	27	1911	Powers
107	162259276...010.288.127	33	1914	Powers
127	170141183...884.105.727	39	1876	Lucas
521	686479766...115.057.151	157	30 de janeiro de 1952	Robinson
607	531137992...031.728.127	183	30 de janeiro de 1952	Robinson
1.279	104079321...168.729.087	386	25 de junho de 1952	Robinson
2.203	147597991...697.771.007	664	7 de outubro de 1952	Robinson
2.281	446087557...132.836.351	687	9 de outubro de 1952	Robinson
3.217	259117086...909.315.071	969	8 de setembro de 1957	Riesel
4.253	190797007...350.484.991	1.281	3 de novembro de 1961	Hurwitz
4.423	285542542...608.580.607	1.332	3 de novembro de 1961	Hurwitz
9.689	478220278...225.754.111	2.917	11 de maio de 1963	Gillies

22	9.941	346088282...789.463.551	2.993	16 de maio de 1963	Gillies
23	11.213	281411201...696.392.191	3.376	2 de junho de 1963	Gillies
24	19.937	431542479...968.041.471	6.002	4 de março de 1971	Tuckerman
25	21.701	448679166...511.882.751	6.533	30 de outubro de 1978	Noll & Nickel
26	23.209	402874115...779.264.511	6.987	9 de fevereiro de 1979	Noll
27	44.497	854509824...011.228.671	13.395	8 de abril de 1979	Nelson & Slowinski
28	86.243	536927995...433.438.207	25.962	25 de setembro de 1982	Slowinski
29	110.503	521928313...465.515.007	33.265	25 de setembro de 1988	Colquitt & Welsh
30	132.049	512740276...730.061.311	39.751	20 de setembro de 1983	Slowinski
31	216.091	746093103...815.528.447	65.050	6 de setembro de 1985	Slowinski
32	756.839	174135906...544.677.887	227.832	19 de setembro de 1992	Slowinski & Gage
33	859.433	129498125...500.142.591	258.716	10 de janeiro de 1994	Slowinski & Gage
34	1.257.787	412245773...089.366.527	378.632	3 de setembro de 1996	Slowinski & Gage
35	1.398.269	814717564...451.315.711	420.921	13 de novembro de 1996	GIMPS / Joel Armengaud
36	2.976.221	623340076...729.201.151	895.932	24 de agosto de 1997	GIMPS / Gordon Spence
37	3.021.377	127411683...024.694.271	909.526	27 de janeiro de 1998	GIMPS / Roland Clarkson
38	6.972.593	437075744...924.193.791	2.098.960	1 de junho de 1999	GIMPS / Nayan Hajratwala
39	13.466.917	924947738...256.259.071	4.053.946	14 de novembro de 2001	GIMPS / Michael Cameron
40*	20.996.011	125976895...855.682.047	6.320.430	17 de novembro de 2003	GIMPS / Michael Shafer
41*	24.036.583	299410429...733.969.407	7.235.733	15 de maio de 2004	GIMPS / Josh Findley
42*	25.964.951	122164630...577.077.247	7.816.230	18 de fevereiro de 2005	GIMPS / Martin Nowak
43*	30.402.457	315416475...652.943.871	9.152.052	15 de dezembro de 2005	GIMPS / Curtis Cooper & Steven Boone [1]
44*	32.582.657	124575026...053.967.871	9.808.358	4 de setembro de 2006	GIMPS / Curtis Cooper & Steven Boone [2]
45*	37.156.667	202254406...308.220.927	11.185.272	6 de setembro de 2008	GIMPS / Hans-Michael Elvenich
46*	42.643.801	169873516...562.314.751	12.837.064	12 de abril de 2009	GIMPS / Odd M. Strindmo
47*	43.112.609	316470269...697.152.511	12.978.189	23 de agosto de 2008	GIMPS / Edson Smith

Numeros Perfeitos

- Diz- se que um número é perfeito se

São iguais à soma de todos os números menores do que eles e que o dividem exactamente

Por exemplo:

$$6 = 1 + 2 + 3$$

★ 7

Pierre de Fermat (1601- 1665)

Fermat estudou direito, foi conselheiro do Rei no parlamento de Toulouse até ser atingido pela peste.
Foi conhecido por ser matemático amador/profissional.
Contribuiu para o cálculo infinitesimal, teoria de números e das probabilidades.
Nunca na sua inteira vida publicou algo.

★ 8

- Fermat conjecturou, em 1640 que todos os números da forma $2^{2^m}+1$ eram primos.
- De facto Fermat já tinha testado para m inferior a 5 que tal se verificava.
- Por serem números muito grandes, só mais tarde, Euler descobre que o próximo número de Fermat era composto

n=5→4294967297=641 x 6700417

- Na actualidade os únicos primos de Fermat conhecidos são

3; 5; 17; 257; 65537;

★ 9/10