O Fascínio dos Números Primos

António Machiavelo

Centro de Matemática da Universidade do Porto
Departamento de Matemática da FCUP

Universidade Popular do Porto

9 de Junho de 2010

A forma dos números

Figura: Duas maneiras diferentes de ver um quadrado de pontos.

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

$$1 + 2 + 3 + \cdots + (n - 1) + n + (n - 1) + \cdots + 3 + 2 + 1 = n^2$$

$$2 \times (1 + 2 + 3 + \cdots + n) = n^2 + n$$

$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2}$$

A forma dos números

Esta última relação pode também ser "vista" do modo seguinte:

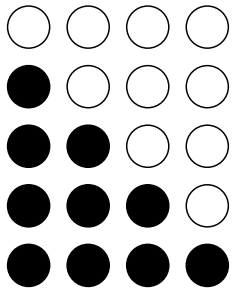


Figura: $2\,(1+2+\cdots+n) = n(n+1)$

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}$$

A tabuada

1	**2**	3	**4**	5	**6**
2	**4**	6	**8**	10	**12**
3	6	9	**12**	15	**18**
4	**8**	**12**	**16**	20	**24**
5	10	15	20	25	**30**
6	**12**	**18**	**24**	**30**	**36**

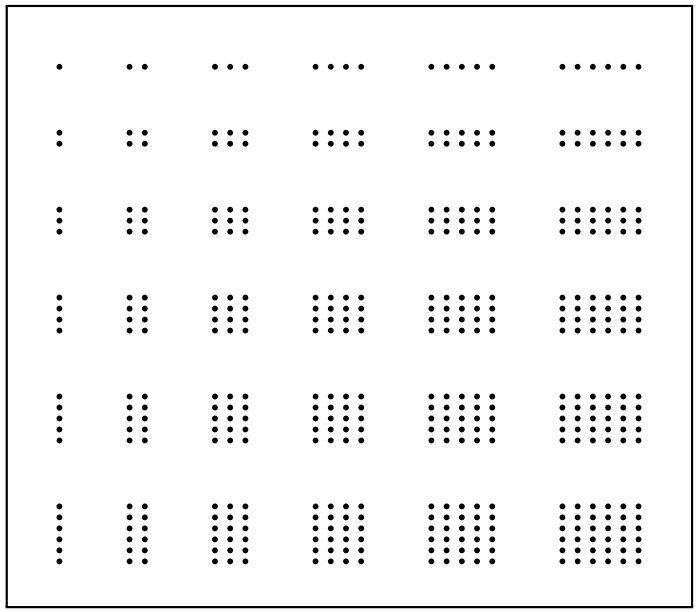


Tabela de multiplicação 6×6

A soma dos elementos de um "gnómon" é:

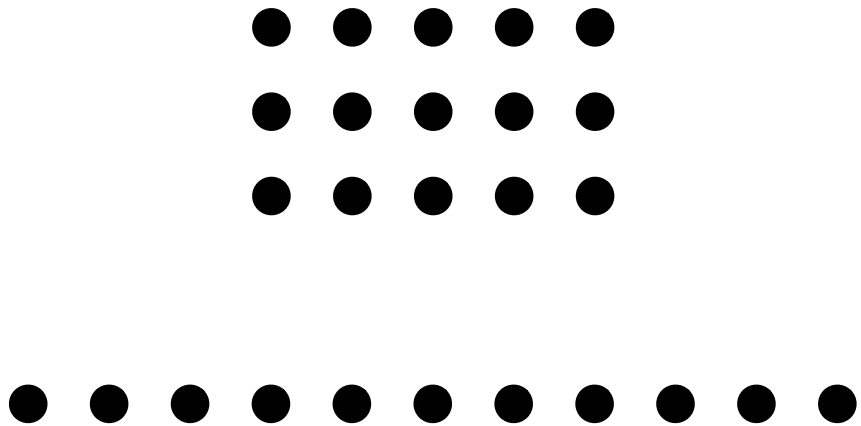
$$n\,(1+2+3+\cdots+(n-1)+n+(n-1)+\cdots+3+2+1) = n\cdot n^2 = n^3$$

Portanto: $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.

Os números primos

Um número natural maior do que 1 *diz-se* primo *se não puder ser escrito com um produto de dois números menores.*

Ou seja, se quando visto como um conjunto de pontos, estes não puderem ser dispostos num rectângulo que não seja uma linha.

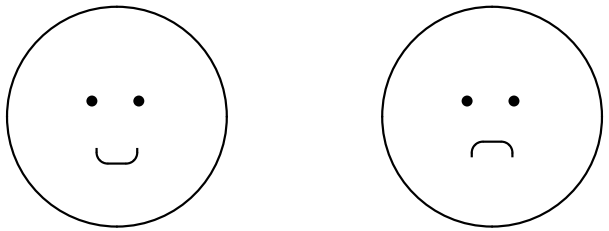


Os números primos

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,
101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191,
193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283,
293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401,
409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509,
521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631,
641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751,
757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877,
881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997,
1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091,
1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193,
1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291,
1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423,
1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, . . .

Padrões e abstracção

Abstracção e reconhecimento de padrões...



... são a especialidade do *Homo Sapiens*.

Quantos há?

Euclides (c. −250): *Há uma infinidade de números primos !!!*

Demonstração:

1. Todo o número (natural) tem algum divisor primo...
   ... que pode eventualmente ser ele próprio...
2. Se um número é divisível por um dado número maior do que um, então o número seguinte não o é.

Considere-se o número:

$$1000 \times 999 \times 998 \times \cdots \times 4 \times 3 \times 2 + 1.$$

Por (1), tem um divisor primo que, por (2), tem de ser > 1000.

Conclusão: existe um número primo maior do que 1000!
Mas o que se fez para o número 1000 pode ser feito para um outro número qualquer! QED!

Um resultado fundamental

Todo o número natural pode ser escrito, de uma só maneira, a menos da ordem dos factores, como um produto de números primos:

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_t^{e_t} \qquad (p_i \text{ primos }, e_i \in \mathbb{N})$$

$$C_8 H_{10} N_4 O_2$$

Substâncias $\leftrightarrow$ Elementos

Moléculas $\leftrightarrow$ Átomos

Números $\leftrightarrow$ Primos

Números de Fermat

Pierre de Fermat (1601, 1607 ou 1608–1665):

Para todo $n \in \mathbb{N}_0$, o número $F_n = 2^{2^n} + 1$ é primo.

Sabe-se ser verdade para: $n = 0, 1, 2, 3, 4.$

$$F_4 = 2^{2^4} + 1 = 65537 \quad ; \quad F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$$

Sabe-se ser falsa para: $n = 5, 6, 7, \ldots, 31, 32,$ e mais alguns...

Desconhece-se para: $n = 33, 34, 35, 40, 41, 44, 45, 46, 47, 49, 50, \ldots$

Composto, mas não se conhece nenhum factor: $n = 20, 24.$

Observação: F_{33} tem 2 585 827 973 algarismos!

http://www.prothsearch.net/fermat.html

Primos de Mersenne

Mersenne (1588–1648):

Um primo de Mersenne é um número primo da forma $M_p = 2^p - 1$.

Número Perfeito: um número que é igual à soma dos seus divisores, excluíndo o próprio.

Euclides (c. –250): *Se n é um número tal que* $2^n - 1$ *é primo, então o número* $2^{n-1}(2^n - 1)$ *é um número perfeito.*
Euler (1707–1783): *Se n é um número perfeito par, então tem a forma descrita pelo resultado de Euclides.*

Questões:

- Para que valores de n é que $2^n - 1$ é um número primo?
- Existem números perfeitos ímpares?

Primos de Mersenne

Não é difícil ver que: n composto $\Longrightarrow$ $2^n - 1$ composto.

Primos de Mersenne conhecidos: $2^p - 1$ for $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976211, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609.

A descoberta, a 23 de Agosto de 2010, do primo de Mersenne $2^{43\,112\,609} - 1$, um gigante com 12 978 189 algarismos, valeu ao grupo GIMPS o "Cooperative Computing Award" de \$100,000 da *Electronic Frontier Foundation* .

`http://www.mersenne.org/`
`http://www.eff.org/awards/coop`

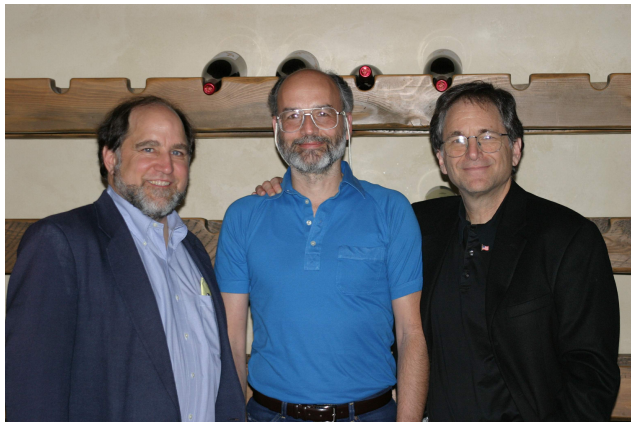
Fermat e Criptografia

Números perfeitos $\rightsquigarrow$ Primos de Mersenne $\rightsquigarrow$ "Pequeno" teorema de Fermat

"Pequeno" teorema de Fermat

Para todo o primo p e para todo $a \in \mathbb{Z}$ que não é divisível por p, tem-se:

$$a^{p-1} \equiv 1 \pmod{p}$$



SRA & RSA...

Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman

O problema da factorização

$$7432339208719 \times 341117531003194129 = ?$$

$$2^{101} - 1 = 2535301200456458802993406410751 = ? \times ??$$

$$\begin{aligned}\mathrm{RSA}_{2048} = \; & 25\,195\,908\,475\,657\,893\,494\,027\,183\,240\,048\,398\,571\,429\,282\,126\,204\,032 \\ & 027\,777\,137\,836\,043\,662\,020\,707\,595\,556\,264\,018\,525\,880\,784\,406\,918\,290\,641\,249 \\ & 515\,082\,189\,298\,559\,149\,176\,184\,502\,808\,489\,120\,072\,844\,992\,687\,392\,807\,287\,776 \\ & 735\,971\,418\,347\,270\,261\,896\,375\,014\,971\,824\,691\,165\,077\,613\,379\,859\,095\,700\,097 \\ & 330\,459\,748\,808\,428\,401\,797\,429\,100\,642\,458\,691\,817\,195\,118\,746\,121\,515\,172\,654 \\ & 632\,282\,216\,869\,987\,549\,182\,422\,433\,637\,259\,085\,141\,865\,462\,043\,576\,798\,423\,387 \\ & 184\,774\,447\,920\,739\,934\,236\,584\,823\,824\,281\,198\,163\,815\,010\,674\,810\,451\,660\,377 \\ & 306\,056\,201\,619\,676\,256\,133\,844\,143\,603\,833\,904\,414\,952\,634\,432\,190\,114\,657\,544 \\ & 454\,178\,424\,020\,924\,616\,515\,723\,350\,778\,707\,749\,817\,125\,772\,467\,962\,926\,386\,356 \\ & 373\,289\,912\,154\,831\,438\,167\,899\,885\,040\,445\,364\,023\,527\,381\,951\,378\,636\,564\,391 \\ & 212\,010\,397\,122\,822\,120\,720\,357\end{aligned}$$

Alguns mistérios

Existe mais algum primo de Fermat?...

Existe uma infinidade de primos de Mersenne?...

Existe uma infinidade de primos gémeos?...

Dirichlet (1837): Se $\text{mdc}(a, b) = 1$, então existe uma infinidade de primos da forma $an + b$ ($n \in \mathbb{N}$).

Existe uma infinidade de primos da forma $n^2 + 1$?...

Conjectura de Goldbach

Christian Goldbach (1690–1764) $\rightarrow$ Leonhard Euler (1707–1783):

[1742] *Todo o número par maior do que 2 pode ser escrito como uma soma de dois números primos.*

- $4 = 2+2 \quad ; \quad 6 = 3+3 \quad ; \quad 8 = 3+5$
- $10 = 3 + 7 = 5 + 5$
- $\ldots$
- $48 = 5 + 43 = 7 + 41 = 11 + 37 = 17 + 31 = 19 + 29$
- $\ldots$

`http://wims.unice.fr/wims/wims.cgi?module=tool/number/goldbach.en`

Conjectura de Goldbach

Versão "fraca": *Todo o número ímpar maior do que* 5 *pode ser escrito como soma de* 3 *números primos.*

- Lev Šnirel'man (1930): $\exists c \in \mathbb{N}$ tal que todo o número suficientemente grande é soma de, no máximo, c primos.
  Klimov (1969): $c = 6 \times 10^9$; Riesel e Vaughan (1982): $c = 19$.
- Vinogradov (1937): versão fraca é verdadeira para $n > 3^{3^{15}}$.
- Olivier Ramaré (1995): Todos os números pares podem ser escritos como uma soma de não mais de 6 primos.
- Tomás Oliveira e Silva (5/1/2010): A conjectura "forte" é válida para todos os números pares $\leq 20 \times 10^{17}$.

`http://www.ieeta.pt/~tos/goldbach.html`.

Porquê?

Porque...

... é divertido!

... é um desafio!

... testa os nossos limites intelectuais!

... ajuda a desenvolver os instrumentos necessários para ultrapassar esses limites!

Para saber mais...

- Chris Caldwell, *The Prime Pages*, `http://www.ieeta.pt/~tos/goldbach.html`
- Apostolos Doxiadis, **Uncle Petros and Goldbach's Conjecture**, Bloomsbury (USA) and Faber and Faber (UK), 2000; Europa-América, 2001.
- Tomás Oliveira e Silva, *Goldbach conjecture verification*, `http://www.ieeta.pt/~tos/goldbach.html`
- Paulo Ribenboim, **The Book of Prime Number Records**, Springer, 1989
- Paulo Ribenboim, **The Little Book of Big Primes**, Springer, 1999.
- Paulo Ribenboim, **The Little Book of Bigger Primes**, Springer, 2004.