



## Aplicación dun *PEQUENO* *TEOREMA*

María Wonenburger



Hai 25 séculos os chineses deron o que crían que era unha regra infalible para saber se un número natural é primo.

A regra afirmaba que **n é primo se, e só se, n é divisor de  $2^n - 2$ .**

Supoñemos que a razón para crer nesta regra era que foi comprobada para diversos valores de **n**.

Debido á complexidade do número  $2^n - 2$  cando **n** é grande, é difícil crer que os chineses comprobaran a súa regra para moitos valores de **n**.

Durante máis de 23 séculos creuse nesta regra que foi comprobada para **n ≤ 300**.

En 1640 o francés **Pierre de Fermat**<sup>1</sup> estableceu o seguinte teorema tamén coñecido como **PEQUENO TEOREMA de Fermat**:

**Supoñamos que p é un número primo, entón  $a^p - a$  é divisible por p. Se p non é un divisor de a entón  $a^{p-1} - 1$  é divisible por p.**

Cando **p > 2** podemos facer **a = 2** e o teorema di que  $2^{p-1} - 1$  é divisible por **p**, así como  $2 \cdot (2^{p-1} - 1) = 2^p - 2$ .

Porén, a regra chinesa non é verdade na outra dirección.

É dicir, do feito de que **n sexa un divisor de  $2^{n-1} - 1$  non podemos deducir que n é un número primo.**

Pois en 1819, **F. Sarrus** sinalou que  $2^{340} - 1$  é **divisible por 341 = 11 · 31**

Para demostrar este resultado, estableceremos a propiedade que se **a-b é divisible por m,  $a^n - b^n$  tamén é divisible por m.**

Pois de **a = b + mr** obtemos:

$$\begin{aligned} a^n &= (b + mr)^n = b^n + \binom{n}{1} b^{n-1} mr + \dots + \binom{n}{i} b^{n-i} m^i r^i + \dots + m^n r^n \\ &= b^n + m \left[ \binom{n}{1} b^{n-1} r + \dots + \binom{n}{i} b^{n-i} m^{i-1} r^i + \dots + m^{n-1} r^n \right] \end{aligned}$$

Isto é,  **$a^n - b^n = m t$**

Tomemos o número **341 = 11 · 31**. Polo **PEQUENO TEOREMA** sabemos que  $2^{10} - 1$  é divisible por **11**. Elevando a potencia **34**, sabemos que  $(2^{10})^{34} - 1^{34} = 2^{340} - 1$  é divisible por **11**, así como  $2^{341} - 2$ .

Aplicamos de novo a propiedade demostrada, partindo de  $2^5 - 1 = 32 - 1 = 31$ , e elevando a **68** obtemos que

$$(2^5)^{68} - 1^{68} = 2^{340} - 1$$

é divisible por **340**, así como  $2(2^{340} - 1) = 2^{341} - 2$ . Por tanto  $2^{341} - 2$  é divisible polo produto **11 · 31**.

A comprobación deste resultado levaríanos a traballar co número  $2^{341} - 2$ , que consta de **103 cifras**.

### Referencias:

Ore, O. (1948): *Number theory and its history*. Mc Graw Hill, New York.

Stark, H. M. (1970): *An introduction to number theory*. Markhan Publishing Corporation, Chicago.

<sup>1</sup> Segundo **Ore**, a **Pierre de Fermat** debe de concedérselle a honra de ser considerado o fundador da **Teoría de Números** como unha ciencia sistemática.