gamma colaboracións
Nº 13 Set 2014

Euler e a teoría de números

RICARDO MORENO CASTILLO

Este traballo está dedicado a expoñer moi someramente algunhas das aportacións de Euler no campo da teoría de números.

Palabras chave: Euler, Teoría de números.

Euler and number theory
This work concisely sets out some of the Euler's contributions in the field of Number Theory.

Key words: Euler, Number theory.

Euler, algúns datos biográficos

Na cidade suiza de Basilea, no ano 1707, chegou ao mundo Leonhard Euler, un dos máis importantes matemáticos da historia e, sen lugar a dúbidas, o máis prolífico. A súa bibliografía consta de 886 títulos, e a súa produción científica supuxo unha media dunhas 800 páxinas anuais. Seu pai, un pastor calvinista, esperaba que o fillo seguise o mesmo camiño, pero na universidade de Basilea tivo ocasión de tratar a Johann Bernoulli (1667-1748), e este encontro foi decisivo para decantarse polas Matemáticas. Aos vinte e tres anos incorporouse á Academia de San Petersburgo, fundada pola emperatriz Catalina I, e dende entón a revista da Academia foi publicando traballos de Euler, un tras outro, ata cincuenta anos despois da súa morte. En 1741 aceptou unha invitación de Federico, *o Grande* para formar parte da Academia de Berlín, pero a estancia en Prusia non foi demasiado feliz, e en 1766 volveu a Rusia. A partir de 1771 quedou completamente cego, pero esta circunstancia no interrompeu o ritmo das súas publicacións. Morreu repentinamente en 1783, á idade de setenta e seis anos. Laplace dicía con frecuencia: "Lede a Euler, lede a Euler, el é o mestre de todos nós". Non cabe mellor homenaxe.

Euler tocou case todos os rexistros da Matemática, e non hai ningunha rama dela na que non estea a súa pegada. A continuación veremos algúns dos seus descubrimentos na teoría de números.

Un problema da *Aritmética* de Diofanto

O problema 9 do libro II da *Aritmética* de Diofanto propón o seguinte. Dado un número racional que é suma de dous cadrados, encontrar outra expresión dese número como suma doutros dous cadrados. Euler demostrou que o problema ten infinitas solucións. En efecto, sexa $c = a^2 + b^2$, trátase de atopar todas as solucións da ecuación $c = x^2 + y^2$. Facemos $x = a + mu$ e $y = b - nu$, e chegamos ao seguinte:

$$u = \frac{2(bn - am)}{m^2 + n^2}.$$

Disto dedúcense facilmente todas as solucións do problema:

$$x = \frac{2bmn + a(n^2 - m^2)}{m^2 + n^2},$$
$$y = \frac{2amn + b(m^2 - n^2)}{m^2 + n^2}.$$

Con estas fórmulas podemos fabricar todas as solucións. Se collemos o caso concreto $13 = 2^2 + 3^3$ (que é o que aparece na *Aritmética*) estes son algúns dos valores posibles para x e y:

m	n	x	y
2	1	6/5	17/5
3	1	1/5	18/5
4	1	6/17	61/17
5	2	18/29	103/29
7	3	23/29	102/29

As ecuacións lineais

É cousa sabida que unha ecuación diofántica linear $ax + by = c$ ten solución se o máximo común divisor dos coeficientes a e b divide ao termo independente c. Por esta razón, sempre podemos imaxinar, sen merma ningunha de xeneralidade, que a e b son primos entre si. Tamén se sabía dende hai moito que, se temos unha solución $x = \alpha$ e $y = \beta$, temos infinitas, e ademais fáciles de encontrar: para calquera valor enteiro de t, os números $x = \alpha + bt$ e $y = \beta - at$ son unha nova solución. O que xa non é cousa tan trivial, se a e b son un pouco grandes, é atopar a primeira, a que permite dar con todas as demais. Euler descubriu un procedemento para calculala, consistente en despexar a incógnita de menor coeficiente, extraer despois da fracción a maior parte enteira, e fabricar co resto unha nova ecuación máis simple cá inicial. Imos ilustrar isto mediante un exemplo. Pensemos na ecuación $315x + 22y = 16$. A incógnita que leva o coeficiente menor é o y. Entón:

$$y = \frac{16 - 315x}{22} = \frac{16 - 7x}{22} - 14x.$$

Facemos $(16 - 7x)/22 = u$, e temos a ecuación $7x + 22u = 16$, e reiteramos o procedemento:

$$x = \frac{16 - 22u}{7} = \frac{2 - u}{7} + 2 - 3u.$$

Facemos $(2 - u)/7 = v$ e chegamos á ecuación $u + 7v = 2$. Se facemos (por exemplo) $v = 0$, temos que $u = 2$, $x = -4$ e $y = 58$.

Sobre a cantidade de números menores ca un número dado que son primos con el

Inspirándose na criba de Eratóstenes, Euler ideou un método para saber, dado un número n, cantos números hai menores que n que sexan primos con el. Consideremos a seguinte función entre números enteiros:

$$\varphi(n) = \text{cantidade de números} \leq n \,(\text{que sexan primos con } n)$$

Sexa $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ a descomposición de n en factores primos. Da sucesión $\{1, 2, \ldots, n\}$ eliminamos todos os números divisibles por p_1, que son en total n/p_1, e quedan $n - n/p_1$. De entre eles tachamos os múltiplos de p_2, que son $(n - n/p_1)/p_2$, e calculamos cantos quedan:

$$n - \frac{n}{p_1} - \frac{n - n/p_1}{p_2} = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

Reiterando o razoamento ata chegar a p_k, temos a fórmula:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Por exemplo, se para $n = 100$, como $100 = 2^2 \times 5^2$, temos que:

$$\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 40$$

Outro exemplo: $333{,}333 = 3^2 \times 7 \times 11 \times 13 \times 37$, logo:

$$\varphi(333\,333) = 333\,333\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{37}\right) = 155\,520$$

A infinitude dos números primos

Xa sabemos dende Euclides (proposición 20 do libro X dos *Elementos*) que hai infinitos números primos. Euler demostrou isto utilizando series infinitas, dando así os primeiros pasos na teoría analítica de números. Para cada primo p considerou a igualdade:

$$\left(1 - \frac{1}{p}\right)^{-1} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots$$

Despois, multiplicou membro a membro todas as igualdades así obtidas. Cada sumando do segundo membro do produto é o inverso dun produto de potencias de números primos, e como todo número enteiro n é un produto de potencias de números primos, sucede o seguinte:

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots\right) = \sum_{n=1}^{\infty} \frac{1}{n}$$

Se o número de primos fose finito, o produto da esquerda tamén sería finito, e a a serie da dereita converxería. Pero sabemos (xa dende o século XIV) que non é así.

Os números congruentes

Para un mellor entendemento do que segue, convén falar algo de números *congruentes*. Dous números enteiros a e b son congruentes respecto doutro enteiro m se a súa diferenza é múltiplo de m (ou o que é igual, se dan idéntico resto ao seren divididos entre m). Isto escríbese desta maneira: $a \equiv b \pmod{m}$. O máis pequeno número positivo congruente con a respecto de m chámase o resto de a en relación a m, e é xustamente o resto de dividir a por m. As congruencias conservan as operacións aritméticas. Isto quere dicir que se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, tamén sucede que $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$. O concepto de número congruente non foi definido dun modo explícito ata o século XVIII, pero foi tacitamente utilizado dende moito antes. Esta maneira de comportarse as congruencias, case como se fosen igualdades (poden ser sumadas e multiplicadas membro a membro), permite crear unha álxebra que, en certas cousas, parécese á álxebra tradicional, pero que noutras difire claramente dela. Pensemos na ecuación $x^2 \equiv 3 \pmod{11}$. Os números 5 e 6 cumpren a ecuación, logo son solucións. Agora ben, os números 16, 27, 38, ... , tamén a cumpren, pero como son congruentes entre si e con 5, non se consideran soluciones distintas del. O mesmo sucede cos números 17, 28, 39, ... , que son congruentes con 6. En cambio, 5 e 6 si son solucións distintas porque non son congruentes. Curiosamente, dicir que a ecuación teña solucións equivale a dicir que o 3, que como número enteiro carece de raíz cadrada, na álxebra das congruencias módulo 11 si que a ten.

Non é esta a única cousa chamativa que sucede coas congruencias. Por exemplo, a ecuación $x^2 \equiv 1 \pmod{8}$ ten como solucións a 1, 3, 5 e 7, catro solucións distintas (enténdase: non congruentes) para una ecuación de segundo grao. O teorema fundamental da álxebra clásica, segundo o cal o número de solucións dunha ecuación non pode exceder o grao desta, non sempre funciona na álxebra de congruencias.

Euler e as conxecturas de Fermat

Entre as conxecturas que Fermat deixou abertas, están as tres seguintes: todo número da forma $2^{2^n} + 1$ é primo, a ecuación $x^n + y^n = z^n$ (con $n \geq 3$) non ten solución entre os números enteiros, e para todo primo p e todo número enteiro a non divisible por p sucede que $a^{p-1} \equiv 1(\text{mod } p)$ (este último resultado chámase *o pequeno teorema de Fermat*). Euler demostrou a terceira; a segunda, no caso particular $n = 3$, e refutou a primeira. Poñendo en xogo a súa incrible habilidade para o cálculo, chegou á descomposición:

$$2^{2^5} + 1 = 4\,294\,967\,297 = 6\,700\,417 \times 641$$

Hoxe sabemos que para $5 \leq n \leq 16$, o número $2^{2^n} + 1$ é composto, e non se sabe de máis primos de Fermat despois dos cinco primeiros. Algúns matemáticos opinan (aínda que non está demostrado) que eses cinco son os únicos que hai.

Unha ampliación do pequeno teorema de Fermat

Xa se falou da función, introducida por Euler, que asigna a cada número n outro número $\varphi(n)$ igual á cantidade de números primos con n que hai por debaixo del. Esta cantidade foi chamada por Édouard Lucas, un matemático francés que viviu entre os anos 1842 e 1891, o *indicador de n*. Pois ben, Euler demostrou que se n é primo con a, entón $a^{\varphi(n)} \equiv 1(\text{mod } n)$. De aquí sae, como caso particular, o pequeno teorema de Fermat, porque se p é un número primo, $\varphi(p) = p - 1$.

Non se entrará na demostración, pero si se comprobará nun caso concreto, por exemplo con $a = 23$ e $n = 100$ (e xa sabemos que $\varphi(100) = 40$):

$$23^2 \equiv 29(\text{mod } 100)$$

$$23^4 \equiv 29^2 \equiv 41(\text{mod } 100)$$

$$23^8 \equiv 41^2 \equiv 81 (\text{mod } 100)$$
$$23^{16} \equiv 81^2 \equiv 61 (\text{mod } 100)$$
$$23^{32} \equiv 61^2 \equiv 21 (\text{mod } 100)$$

Como $81 \times 21 \equiv 1 (\text{mod } 100)$, multiplicamos as congruencias terceira e quinta, e temos que $23^{40} \equiv 1 (\text{mod} 100)$.

Este resultado é útil para resolver certas ecuacións de congruencia. Supoñamos que a é un número primo con n, e interesa resolver a ecuación:

$$ax \equiv b (\text{mod } n)$$

Entón a solución é o número $x = ba^{\varphi(n)-1}$ (e por suposto, calquera outro número congruente con el módulo n):

$$aba^{\varphi(n)-1} - b = b(a^{\varphi(n)} - 1) = \text{múltiplo de } n$$

Para ilustrar o procedemento, resolverase a ecuación $13x \equiv 7 (\text{mod } 25)$. Como $\varphi(25) = 20$, unha solución é $x = 7 \times 13^{19}$, pero convén encontrar a máis pequena:

$$13 \equiv 13 (\text{mod } 25)$$
$$13^2 \equiv 19 (\text{mod } 25)$$
$$13^4 \equiv 19^2 \equiv 11 (\text{mod } 25)$$
$$13^8 \equiv 11^2 \equiv 21 (\text{mod } 25)$$
$$13^{16} \equiv 21^2 \equiv 16 (\text{mod } 25)$$

Multiplicamos a primeira, a segunda e a última, e temos que $13^{19} \equiv 2 (\text{mod } 25)$, logo $7 \times 13^{19} \equiv 14 (\text{mod } 25)$, e 14 é a menor solución.

Referencias bibliográficas

[1] C. Boyer, *Historia de la Matemática*, Alianza Editorial, Madrid, 1992.

[2] Diofanto, *La Aritmética y el libro sobre los números poligonales*, Editorial Nivola, Madrid, 2007.

[3] W. Dunham, *Euler. El maestro de todos los matemáticos*, Editorial Nivola, Madrid, 2000.

[4] R. Moreno, *Historia de la teoría elemental de números*, Editorial Nivola, Madrid, 2013.

RICARDO MORENO CASTILLO

Catedrático de instituto xubilado

<moreno_castillo@hotmail.es>