Euler y los números

Fernando Chamizo Lorente

Universidad Autónoma de Madrid

http://www.uam.es/fernando.chamizo

Museo Nacional de Ciencia y Tecnología

29 de noviembre 2007

Las investigaciones de Euler en teoría de números

1. Divisibilidad de potencias
2. Distribución de los primos
3. Divisibilidad de formas cuadráticas
4. Último teorema de Fermat $n = 3, 4$
5. Números perfectos
6. La ecuación de Pell

Las investigaciones de Euler en teoría de números

1. Divisibilidad de potencias •
2. Distribución de los primos
3. Divisibilidad de formas cuadráticas •
4. Último teorema de Fermat $n = 3, 4$
5. Números perfectos •
6. La ecuación de Pell

Otros temas: Números convenientes, números amigos, teorema chino del resto, particiones, fracciones continuas, representación por formas cuadráticas.

Tres problemas de divisibilidad

[. . .] creo firmemente que no he desperdiciado mi trabajo y mi esfuerzo en investigar estas propiedades que contienen notables propiedades sobre los divisores de los números. Esta teoría de los divisores no es de uso vano sino que alguna vez podría mostrar alguna utilidad no despreciable en análisis.

Divisibilidad de potencias

Euler se interesó mucho por la sucesión de restos cuando dividimos las potencias de un número entre otro

$$a^0, \quad a^1, \quad a^2, \quad a^3, \quad a^4, \quad a^5, \quad \ldots \qquad \lfloor n$$

Factorizando, todo se puede reducir a los casos n primo o potencia de primo.

Divisibilidad de potencias

Euler se interesó mucho por la sucesión de restos cuando dividimos las potencias de un número entre otro

$$a^0, \quad a^1, \quad a^2, \quad a^3, \quad a^4, \quad a^5, \quad \ldots \qquad \lfloor n$$

Factorizando, todo se puede reducir a los casos n primo o potencia de primo.
La sucesión acaba siendo periódica porque sólo hay un número finito de restos.

Actividad: ¿cuáles son los posibles periodos?

Primo	Periodos
2	1
3	1, 2
5	1, 2, 4
7	1, 2, 3, 6

Primo	Periodos
11	1, 2, 5, 10
13	1, 2, 3, 4, 6, 12
...	...
467	1, 2, 233, 466

Ej.: Para $n = 5$

1^0	1^1	1^2	1^3	1^4 ...	2^0	2^1	2^2	2^3	2^4 ...
1	1	...			**1**	**2**	**4**	**3**	1

3^0	3^1	3^2	3^3	3^4 ...	4^0	4^1	4^2	4^3	4^4 ...
1	**3**	**4**	**2**	1	**1**	**4**	1	...	

Euler probó inicialmente los siguientes resultados para los restos cuando se divide a^k, $k = 0, 1, 2, \ldots$ entre n:

Si n es primo, los posibles periodos son divisores de $n - 1$.

Si n es potencia de un primo, p, los posibles periodos son divisores de $n - n/p$.

Más tarde logró probar que en el primer resultado todos los divisores de $n - 1$ realmente aparecen como periodos.

El resultado más conocido e influyente de Euler acerca de restos de potencias trata el caso compuesto general.

Congruencia de Euler-Fermat — Euler 1758

Teorema: Sean a y n coprimos y $\phi(n) = n\prod_{p|n}(1-1/p)$, entonces $a^{\phi(n)}$ deja resto 1 al ser dividido por n.

Ej.: Si $3, 5 \nmid a$ entonces 15 divide a $a^8 - 1$.

¿Matemáticas útiles e inútiles?

El criptosistema RSA rige la mayor parte de las transmisiones seguras por la red y está basado en que si $n = pq$, los restos de las potencias tienen como periodo un divisor de $r = (p-1)(q-1)$.

Si p y q son primos grandes (de cientos de *bits*)

$$\begin{array}{lcll} p, q & \xrightarrow{\text{fácil}} & n \text{ (y } r) & \dashrightarrow \text{ crear una clave} \\ p, q \text{ (y } r) & \xleftarrow{\text{difícil}} & n & \dashrightarrow \text{ romper una clave} \end{array}$$

Numerología en el siglo de las luces

Números perfectos

Se llama *número perfecto* al que coincide con la suma de sus divisores distintos de él mismo.

Ej.: $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$.

Numerología en el siglo de las luces

Números perfectos

Se llama *número perfecto* al que coincide con la suma de sus divisores distintos de él mismo.

Ej.: $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$.

Euler descubrió el octavo número perfecto.
Hasta la fecha (noviembre 2007) se conocen en total 44 números perfectos. El último de ellos cuenta con 19 616 714 cifras.

Actividad: elaborar una tabla con los primeros números perfectos y tratar de inferir una fórmula.

Los primeros números perfectos:

$$6, \quad 28, \quad 496, \quad 8128, \quad 33550336, \quad 8589869056, \quad \ldots$$

Euclides (s.IV-III a.d.C.), Euler (s.XVIII)

Los números perfectos pares son aquellos de la forma $2^{n-1}(2^n - 1)$ donde $2^n - 1$ es primo.

Los primeros números perfectos:

$$6, \quad 28, \quad 496, \quad 8128, \quad 33550336, \quad 8589869056, \quad \ldots$$

Euclides (s.IV-III a.d.C.), Euler (s.XVIII)

Los números perfectos pares son aquellos de la forma $2^{n-1}(2^n - 1)$ donde $2^n - 1$ es primo.

$$2^1 \quad \boxed{2^2} \quad \boxed{2^3} \quad 2^4 \quad \boxed{2^5} \quad 2^6 \quad \boxed{2^7} \quad \ldots$$

$$\downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$$

$$6 \qquad 28 \qquad 496 \qquad 8128 \quad \ldots$$

Nota: Existen algoritmos muy eficientes para saber si $2^n - 1$ es primo.

Problemas sin resolver:

- ¿Existe algún número perfecto impar?
- ¿Verdaderamente hay infinitos valores de n para los que $2^n - 1$ es primo?

Euler dijo del primer problema que era muy difícil y dio un resultado acerca de la factorización que deberían tener los hipotéticos números perfectos impares. Se cree que no existen.

Divisibilidad de Formas Cuadráticas

Euler 1748

59 "teoremas experimentales" acerca de la divisibilidad de $x^2 + Cy^2$ cuando se dan valores (coprimos) a x e y.

Reducciones que Euler conocía:

- Se puede prescindir de la segunda variable tomando $y = 1$.
- Los casos importantes son $C = 1$ y $C =$primo.

Nota: Supondremos $C > 0$.

Experimentos de Euler $\longrightarrow$ los factores primos al descomponer $x^2 + C$, $x \in \mathbb{N}$, no son arbitrarios. Se agrupan en familias.

Actividad: estudiar estas familias.

Experimentos de Euler $\longrightarrow$ los factores primos al descomponer $x^2 + C$, $x \in \mathbb{N}$, no son arbitrarios. Se agrupan en familias.

Actividad: estudiar estas familias.

Polinomio	Factores primos $p \neq 2, C$
$x^2 + 1$	$p = 4n + 1$
$x^2 + 2$	$p = 8n + 1,\ 8n + 3$
$x^2 + 3$	$p = 6n + 1$
$x^2 + 5$	$p = 20n + 1,\ 20n + 3,\ 20n + 7,\ 20n + 9$
$x^2 + 7$	$p = 14n + 1,\ 14n + 9,\ 14n + 11$

Ej. $(x^2+1,\ p=4n+1,\ p=2)$

$$8^2+1=5\times 13, \qquad 20^2+1=401, \qquad 30^2+1=17\times 53,$$
$$1636^2+1=17\times 29\times 61\times 89$$
$$2007^2+1=2\times 5^2\times 13\times 6197, \qquad \boxed{4n+3\nmid x^2+1}$$

Ej. $(x^2+7,\ p=14n+1,\ 14n+9,\ 14n+11,\ p=2,7)$

$$10^2+7=107, \qquad 20^2+7=11\times 37, \qquad 30^2+7=907,$$
$$2007001\nmid x^2+7, \qquad \boxed{14n+3\nmid x^2+7}$$

Para cada par de primos $p, q \neq 2$, Euler se percató de una extraña simetría de la cual se deducía casi todo lo que se proponía.

Reciprocidad cuadrática (Demostración: Gauss 1801)

1. Si $4|p-1$ y $4|q-1$:

$$\begin{array}{c} p \text{ posible factor} \\ \text{primo de } x^2+q \end{array} \iff \begin{array}{c} q \text{ posible factor} \\ \text{primo de } x^2+p \end{array}$$

2. En el resto de los casos:

$$\begin{array}{c} p \text{ posible factor} \\ \text{primo de } x^2+q \end{array} \iff \begin{array}{c} q \text{ no es posible factor} \\ \text{primo de } x^2+p \end{array}$$

Ej. $p = 14n+3 \nmid x^2+7 \Leftrightarrow 7$ es posible factor de $x^2+14n+3$.
Lo es, basta tomar $x = 2$.

Referencias

Historia

- W. Dunham. *Euler. El maestro de todos los matemáticos*. Nivola 2000.
- B. Torrecillas Jover. *Fermat. El mago de los números*. Nivola 1999.
- C.E. Sandifer. *The early mathematics of Leonhard Euler*. Mathematical Association of America, 2007.
- C.E. Sandifer. How Euler Did It. (MAA online) `http://www.maa.org/news/howeulerdidit.html`

Esta charla en formato PDF está en `http://www.uam.es/fernando.chamizo`

Referencias

Textos

- Rosen, K. H. *Elementary number theory and its applications*. 4th edition. Addison-Wesley, Reading, MA, 2000.
- Cilleruelo F.J.; Córdoba A.*La teoría de los números*. Mondadori, Madrid 1992.
- Vinogradov, I.M. *Fundamentos de la Teoría de los Números*. MIR, 1977.
- Hardy, G. H.; Wright, E. M. *An introduction to the theory of numbers*. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.