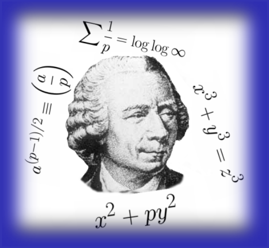
Euler y la Teoría de Números



Fernando Chamizo Lorente

Universidad Autónoma de Madrid
http://www.uam.es/fernando.chamizo

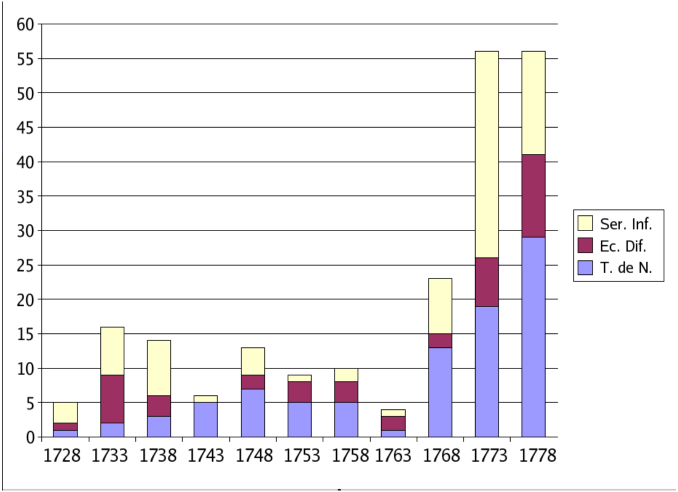
14 de febrero de 2007

Índice

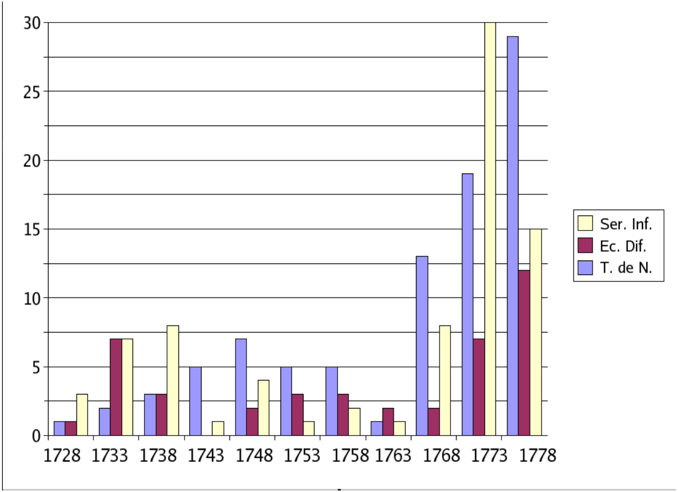
La Teoría de Números para Euler

"Una medida de la grandeza de Euler es que cuando uno estudia teoría de números tiene la impresión de que Euler estaba principalmente interesado en teoría de números pero cuando uno estudia series divergentes siente que las las series divergentes eran su mayor interés, cuando uno estudia ecuaciones diferenciales uno imagina que realmente las ecuaciones diferenciales eran su materia favorita, y así sucesivamente..." H.M. EDWARDS 1977.

La Teoría de Números para Euler



La Teoría de Números para Euler



La Teoría de Números para Euler

Euler 1765 — **Elementos de álgebra**

"Cuando el número de ecuaciones no se ajusta al de incógnitas [...] la materia es una rama particular del álgebra llamada *análisis indeterminado*".

"...usualmente se añade la condición de que los números buscados sean enteros y positivos, o al menos racionales [...]. Ocurre que esta parte del análisis frecuentemente requiere artificios ajustados a ella, los cuales hacen un gran servicio ejercitando el juicio de los principiantes y dándoles destreza en los cálculos".

Nota: Euler comenzó a escribir un libro de teoría de números.

La herencia de Fermat

Fermat
(1601-1665)

Euler
(1707-1783)

Lagrange
(1736-1813)

Legendre
(1752-1833)

Gauss
(1777-1855)

La herencia de Fermat

Con el criterio actual

Fermat
(1601-1665)

¿Demostraciones?

Euler
(1707-1783)

Lagrange
(1736-1813)

Legendre
(1752-1833)

Gauss
(1777-1855)

La herencia de Fermat

Con el criterio actual

Fermat (1601-1665) — ¿Demostraciones?

Euler (1707-1783) — Demostraciones

Lagrange (1736-1813)

Legendre (1752-1833)

Gauss (1777-1855)

La herencia de Fermat

		Con el criterio actual
	Fermat (1601-1665)	¿Demostraciones?
	Euler (1707-1783)	Demostraciones
Lagrange (1736-1813)		
Legendre (1752-1833)	Gauss (1777-1855)	Demostraciones perfectas

La herencia de Fermat

		<u>Con el criterio actual</u>
	Fermat (1601-1665)	¿Demostraciones?
Lagrange (1736-1813)	**Euler** (1707-1783)	Demostraciones
Legendre (1752-1833)	Gauss (1777-1855)	Demostraciones perfectas

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

$$(a+1)^p = a^p + 1^p + p \cdot \text{cosas}$$

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

$(a+1)^p = a^p + 1^p + p \cdot \text{cosas} \Rightarrow$

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

$$(a+1)^p = a^p + 1^p + p \cdot \text{cosas} \Rightarrow a = 1,\ p|2^p - 2$$

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

$$(a+1)^p = a^p + 1^p + p \cdot \text{cosas} \Rightarrow a = 1,\ p | 2^p - 2$$
$$\Rightarrow a = 2,\ p | 3^p - 2^p + 2 - 3 \Rightarrow p | 3^p - 3, \text{ etc.}$$

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

"Corolario" 1732 (la explicación en 1747)

Factorización de F_5: $2^{2^5} + 1 = 641 \cdot 6700417$.

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

Congruencia de Euler-Fermat 1758

Si k y n son coprimos, k divide a $n^{\varphi(k)} - 1$.

$\varphi(k) =$ cantidad de números menores que k y coprimos con él.

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

Congruencia de Euler-Fermat 1758

Si k y n son coprimos, k divide a $n^{\varphi(k)} - 1$.

$\varphi(k) =$ cantidad de números menores que k y coprimos con él.

Números perfectos: $28 = 1 + 2 + 4 + 7 + 14$.

Divisibilidad

Pequeño teorema de Fermat 1736,1747,1758

Si p es primo, p divide a $n^p - n$.

Congruencia de Euler-Fermat 1758

Si k y n son coprimos, k divide a $n^{\varphi(k)} - 1$.

$\varphi(k) =$ cantidad de números menores que k y coprimos con él.

Veinte siglos después de Euclides

Todo número perfecto par es de la forma $2^n(2^{n+1} - 1)$.

Después de Euler

- Existen infinitos números para los que el recíproco del pequeño teorema de Fermat es falso (Alford, Granville, Pomerance 1994).
  Ej. $561 = 3 \cdot 11 \cdot 17$, $561 | a^{561} - a$ siempre que $\text{mcd}(a, 561) = 1$.

Después de Euler

- Existen infinitos números para los que el recíproco del pequeño teorema de Fermat es falso (Alford, Granville, Pomerance 1994).
  Ej. $561 = 3 \cdot 11 \cdot 17$, $561 | a^{561} - a$ siempre que $\mathrm{mcd}(a, 561) = 1$.

$0 < a < p$, restos al dividir por p de $a^1, a^2, a^3, \ldots, a^{p-1}$.
Si salen todos los restos se dice que a es raíz primitiva.

Después de Euler

- Existen infinitos números para los que el recíproco del pequeño teorema de Fermat es falso (Alford, Granville, Pomerance 1994).
  Ej. $561 = 3 \cdot 11 \cdot 17$, $561 | a^{561} - a$ siempre que $\text{mcd}(a, 561) = 1$.

$0 < a < p$, restos al dividir por p de $a^1, a^2, a^3, \ldots, a^{p-1}$.
Si salen todos los restos se dice que a es raíz primitiva.
Ej. $a = 10$, $p = 7$, $p = 17$

$$\frac{1}{7} = 0'\overline{142857}\ldots \qquad \frac{1}{17} = 0'\overline{0588235294117647}\ldots$$

Después de Euler

- Existen infinitos números para los que el recíproco del pequeño teorema de Fermat es falso (Alford, Granville, Pomerance 1994).
  Ej. $561 = 3 \cdot 11 \cdot 17$, $561 | a^{561} - a$ siempre que $\mathrm{mcd}(a, 561) = 1$.

$0 < a < p$, restos al dividir por p de $a^1, a^2, a^3, \dots, a^{p-1}$.
Si salen todos los restos se dice que a es raíz primitiva.
Ej. $a = 10$, $p = 7$, $p = 17$

$$\frac{1}{7} = 0'\overline{142857}\dots \qquad \frac{1}{17} = 0'\overline{0588235294117647}\dots$$

857 94117647

Después de Euler

- Existen infinitos números para los que el recíproco del pequeño teorema de Fermat es falso (Alford, Granville, Pomerance 1994).
  Ej. $561 = 3 \cdot 11 \cdot 17$, $561 | a^{561} - a$ siempre que $\mathrm{mcd}(a, 561) = 1$.

$0 < a < p$, restos al dividir por p de $a^1, a^2, a^3, \dots, a^{p-1}$.
Si salen todos los restos se dice que a es raíz primitiva.
Ej. $a = 10$, $p = 7$, $p = 17$

$$\frac{1}{7} = 0'\overline{142857}\dots \qquad \frac{1}{17} = 0'\overline{0588235294117647}\dots$$

$$\frac{857}{999} \qquad \frac{94117647}{99999999}$$

Después de Euler

- Existen infinitos números para los que el recíproco del pequeño teorema de Fermat es falso (Alford, Granville, Pomerance 1994).
  Ej. $561 = 3 \cdot 11 \cdot 17$, $561 | a^{561} - a$ siempre que $\mathrm{mcd}(a, 561) = 1$.

$0 < a < p$, restos al dividir por p de $a^1, a^2, a^3, \ldots, a^{p-1}$.
Si salen todos los restos se dice que a es raíz primitiva.

- Hay exactamente $\varphi(p-1)$ raíces primitivas (Gauss 1801).

Después de Euler

- Existen infinitos números para los que el recíproco del pequeño teorema de Fermat es falso (Alford, Granville, Pomerance 1994).
  Ej. $561 = 3 \cdot 11 \cdot 17$, $561 | a^{561} - a$ siempre que $\mathrm{mcd}(a, 561) = 1$.

$0 < a < p$, restos al dividir por p de $a^1, a^2, a^3, \dots, a^{p-1}$.
Si salen todos los restos se dice que a es raíz primitiva.

- Hay exactamente $\varphi(p-1)$ raíces primitivas (Gauss 1801).

En el lado computacional:

- $F_k = 2^{2^k} + 1$ compuesto para $5 \le k \le 32$ (2001).
- Si hay números perfectos impares, tienen al menos 47 factores primos (2005).

El caso $n = 3$ de la ecuación de Fermat

$$\boxed{\text{Último teorema de Fermat: } x^n + y^n \neq z^n,\ n > 2.}$$

Fermat $\rightarrow n = 4$, Euler $\rightarrow n = 3, 4$.

El caso $n = 3$ de la ecuación de Fermat

Último teorema de Fermat: $x^n + y^n \neq z^n$, $n > 2$.

Fermat $\to$ $n = 4$, Euler $\to$ $n = 3, 4$.

Elementos de Álgebra — **Capítulo XV**

Cuestión 1: Se requiere encontrar dos cubos, x^3 e y^3, cuya suma sea un cubo.

El caso $n = 3$ de la ecuación de Fermat

$$\boxed{\text{Último teorema de Fermat: } x^n + y^n \neq z^n,\ n > 2.}$$

Fermat $\rightarrow n = 4$,   Euler $\rightarrow n = 3, 4$.

Elementos de Álgebra — **Capítulo XV**

Cuestión 1: Se requiere encontrar dos cubos, x^3 e y^3, cuya suma sea un cubo.

242. Euler intenta sin éxito una especie de parametrización de la curva elíptica $x^3 + 1 = y^3$, como no puede hacerlo escribe:

El caso $n = 3$ de la ecuación de Fermat

$$\boxed{\text{Último teorema de Fermat: } x^n + y^n \neq z^n,\ n > 2.}$$

Fermat $\rightarrow$ $n = 4$, Euler $\rightarrow$ $n = 3, 4$.

Elementos de Álgebra Capítulo XV

Cuestión 1: Se requiere encontrar dos cubos, x^3 e y^3, cuya suma sea un cubo.

242. Euler intenta sin éxito una especie de parametrización de la curva elíptica $x^3 + 1 = y^3$, como no puede hacerlo escribe:

> por tanto podemos inferir, con cierto grado de certeza, que es imposible encontrar dos cubos cuya suma sea un cubo. Pero estaremos totalmente convencidos con la siguiente demostración.

Factorización única

$\boxed{x^3+y^3=z^3}$ solución mínima x, y, z.

Se puede suponer $x = p+q$, $y = p-q$, $4|p$, $\text{mcd}(p,q)=1$.

$$2p\cdot(p^2+3q^2)=z^3, \qquad \text{mcd}(2p,p^2+3q^2)=1 \quad (\text{si } 3 \not| p)$$

Factorización única

$\boxed{x^3 + y^3 = z^3}$ solución mínima x, y, z.
Se puede suponer $x = p + q$, $y = p - q$, $4|p$, $\text{mcd}(p, q) = 1$.

$$2p \cdot (p^2 + 3q^2) = z^3, \qquad \text{mcd}(2p, p^2 + 3q^2) = 1 \quad (\text{si } 3 \nmid p)$$

5. Para que el producto $p/4 \cdot (p^2 + 3q^2)$ pueda ser un cubo, cada uno de estos factores, a no ser que tenga un factor común, deben ser un cubo cada uno.

Factorización única

$\boxed{x^3 + y^3 = z^3}$ solución mínima x, y, z.

Se puede suponer $x = p + q$, $y = p - q$, $\quad 4|p$, $\mathrm{mcd}(p, q) = 1$.

$$2p \cdot (p^2 + 3q^2) = z^3, \qquad \mathrm{mcd}(2p, p^2 + 3q^2) = 1 \quad (\text{si } 3 \nmid p)$$

7. Para que $p^2 + 3q^2$ sea un cubo, sólo tenemos que suponer, como hemos visto antes: $p \pm q\sqrt{-3} = (t \pm u\sqrt{-3})^3$.

Factorización única

$\boxed{x^3+y^3=z^3}$ solución mínima x, y, z.

Se puede suponer $x=p+q,\ y=p-q,\qquad 4|p,\ \mathrm{mcd}(p,q)=1.$

$$2p\cdot(p^2+3q^2)=z^3,\qquad \mathrm{mcd}(2p,p^2+3q^2)=1\quad (\text{si } 3\nmid p)$$

7. Para que p^2+3q^2 sea un cubo, sólo tenemos que suponer, como hemos visto antes: $p\pm q\sqrt{-3}=(t\pm u\sqrt{-3})^3$.

$$\Rightarrow\qquad 2p=\underbrace{2t}_{h^3}\underbrace{(t+3u)}_{f^3}\underbrace{(t-3u)}_{g^3}$$

$$\Rightarrow\qquad h^3=f^3+g^3\quad \text{solución menor} \Rightarrow \text{contr.}$$

Después de Euler

Conjetura de Fermat $\longrightarrow$ 1630 aprox.

Después de Euler

Conjetura de Fermat $\longrightarrow$ 1630 aprox.

- E. Kummer (1847) $\longrightarrow$ Teoría de ideales. El teorema es cierto para exponentes primos regulares.

Después de Euler

Conjetura de Fermat $\longrightarrow$ 1630 aprox.

- E. Kummer (1847) $\longrightarrow$ Teoría de ideales. El teorema es cierto para exponentes primos regulares.
- G. Faltings (1983). El teorema es cierto salvo un número finito de soluciones para cada n.

Después de Euler

Conjetura de Fermat $\longrightarrow$ 1630 aprox.

- E. Kummer (1847) $\longrightarrow$ Teoría de ideales. El teorema es cierto para exponentes primos regulares.
- G. Faltings (1983). El teorema es cierto salvo un número finito de soluciones para cada n.
- A. Wiles (1994) $\longrightarrow$ Conjetura de Shimura-Taniyama-Weil. Demostración general.

La ecuación de Pell

$$Q(x,y) = n \Rightarrow$$
$$ax^2 - by^2 = n \Rightarrow x^2 - Ay^2 = m \Rightarrow \text{sol. part. } x^2 - Ay^2 = 1.$$

La ecuación de Pell

$$Q(x,y) = n \Rightarrow$$
$$ax^2 - by^2 = n \Rightarrow x^2 - Ay^2 = m \Rightarrow \text{sol. part. } x^2 - Ay^2 = 1.$$

Cuando se ha encontrado uno de estos valores es fácil deducir de él infinitos [...] es suficiente saber uno, digamos el menor; y Pell, un escritor inglés, nos ha enseñado a encontrarlo con un ingenioso método.

La ecuación de Pell

$$Q(x,y)=n \Rightarrow$$
$$ax^2-by^2=n \Rightarrow x^2-Ay^2=m \Rightarrow \text{sol. part. } x^2-Ay^2=1.$$

Euler 1733

$$\begin{array}{rcl}
x_1^2=13x_2^2+1 & \xrightarrow{x_1\approx x_2\sqrt{13}} & x_1=3x_2+x_3 \\
4x_2^2=6x_2x_3+x_3^2-1 & \xrightarrow{x_2\approx x_3\sqrt{6/4}} & x_2=x_3+x_4 \\
\dots\dots & \dots\dots\dots\dots & \dots\dots \\
x_{11}^2=6x_{11}x_{12}+4x_{12}^2+1 & &
\end{array}$$

La ecuación de Pell

$$Q(x,y)=n\Rightarrow$$
$$ax^2-by^2=n\Rightarrow x^2-Ay^2=m\Rightarrow \text{sol. part. } x^2-Ay^2=1.$$

Euler 1733

$$\begin{array}{rcl}
x_1^2=13x_2^2+1 & \xrightarrow{x_1\approx x_2\sqrt{13}} & x_1=3x_2+x_3\\
4x_2^2=6x_2x_3+x_3^2-1 & \xrightarrow{x_2\approx x_3\sqrt{6/4}} & x_2=x_3+x_4\\
\cdots\cdots & \cdots\cdots\cdots\cdots & \cdots\cdots\\
x_{11}^2=6x_{11}x_{12}+4x_{12}^2+1 & \leftrightsquigarrow & \Delta=13x_{12}^2+1
\end{array}$$

La ecuación de Pell

$$Q(x,y)=n \Rightarrow$$
$$ax^2-by^2=n \Rightarrow x^2-Ay^2=m \Rightarrow \text{sol. part. } x^2-Ay^2=1.$$

Euler 1733

$$x_1^2=13x_2^2+1 \xrightarrow{x_1\approx x_2\sqrt{13}} x_1=3x_2+x_3$$
$$4x_2^2=6x_2x_3+x_3^2-1 \xrightarrow{x_2\approx x_3\sqrt{6/4}} x_2=x_3+x_4$$
$$\cdots\cdots \qquad \cdots\cdots\cdots\cdot \qquad \cdots\cdots$$
$$x_{11}^2=6x_{11}x_{12}+4x_{12}^2+1 \quad \leftrightsquigarrow \text{Sol. triv. } x_{12}=0,\ x_{11}=1$$

La ecuación de Pell

$Q(x,y)=n \Rightarrow$
$ax^2-by^2=n \Rightarrow x^2-Ay^2=m \Rightarrow$ sol. part. $x^2-Ay^2=1$.

Euler 1733

$$x_1^2 = 13x_2^2+1 \xrightarrow{x_1\approx x_2\sqrt{13}} x_1 = 3x_2+x_3$$

$$4x_2^2 = 6x_2x_3+x_3^2-1 \xrightarrow{x_2\approx x_3\sqrt{6/4}} x_2 = x_3+x_4$$

$$\ldots\ldots \qquad \ldots\ldots\ldots\ldots \qquad \ldots\ldots$$

$$x_{11}^2 = 6x_{11}x_{12}+4x_{12}^2+1 \quad \leftrightsquigarrow \quad \text{Sol. triv. } x_{12}=0,\ x_{11}=1$$

$$x_{10} \mapsto \ldots \mapsto x_3 \mapsto x_2 \mapsto x_1 \rightsquigarrow 1 \mapsto \ldots \mapsto 109 \mapsto 108 \mapsto 649$$

$\Rightarrow \boxed{649^2-13\cdot 180^2=1}$ (1759, fracciones continuas)

Representación por formas cuadráticas

Carta a N. Beguelin 1778

Todos los números contenidos de una sola forma en $x^2 + y^2$ son primos o dobles de primos donde x e y son primos entre sí. He observado que otras expresiones similares de la forma $nx^2 + y^2$ gozan de la misma propiedad dando a la letra n valores *convenientes*.

Representación por formas cuadráticas

Carta a N. Beguelin 1778

Todos los números contenidos de una sola forma en $x^2 + y^2$ son primos o dobles de primos donde x e y son primos entre sí. He observado que otras expresiones similares de la forma $nx^2 + y^2$ gozan de la misma propiedad dando a la letra n valores *convenientes*.

Euler calculó una tabla de 65 números convenientes y los empleó para construir primos de hasta 8 dígitos.

Representación por formas cuadráticas

Carta a N. Beguelin 1778

Todos los números contenidos de una sola forma en $x^2 + y^2$ son primos o dobles de primos donde x e y son primos entre sí. He observado que otras expresiones similares de la forma $nx^2 + y^2$ gozan de la misma propiedad dando a la letra n valores *convenientes*.

Desde el punto de vista actual la explicación radica en la estructura del grupo de clases. Para los números convenientes la representación por primos se puede decidir con congruencias sencillas.

Representación por formas cuadráticas

Carta a N. Beguelin 1778

Todos los números contenidos de una sola forma en $x^2 + y^2$ son primos o dobles de primos donde x e y son primos entre sí. He observado que otras expresiones similares de la forma $nx^2 + y^2$ gozan de la misma propiedad dando a la letra n valores *convenientes*.

Desde el punto de vista actual la explicación radica en la estructura del grupo de clases. Para los números convenientes la representación por primos se puede decidir con congruencias sencillas.

$$\boxed{\begin{array}{c} p = x^2 + 5y^2 \quad \Leftrightarrow \quad 20|p-1 \text{ ó } 20|p-9 \\ p = x^2+13y^2 \Leftrightarrow 52|p-a \text{ para algún } a \in \{1, 9, 17, 25, 29, 49\} \end{array}}$$

<ins>Ej</ins>. $109 = 8^2 + 5 \cdot 3^2$, $20|109 - 9$, $\quad 233 = 5^2 + 13 \cdot 4^2$, $52|233 - 25$.

Reciprocidad cuadrática

p, q primos distintos mayores que dos.

Ley de reciprocidad cuadrática — Conjetura 1772

Si p es de la forma $4mq + (2r+1)^2$ entonces q y $-q$ son de la forma $np + s^2$.

Reciprocidad cuadrática

p, q primos distintos mayores que dos.

Ley de reciprocidad cuadrática — Conjetura 1772

Si p es de la forma $4mq + (2r+1)^2$ entonces q y $-q$ son de la forma $np + s^2$.

Con un lenguaje más sencillo:

$$\text{Si } 8|(p-1)(q-1)$$
$$p|x^2 - q \ \text{ tiene solución } \Leftrightarrow q|x^2 - p \ \text{ tiene solución}$$

Reciprocidad cuadrática

p, q primos distintos mayores que dos.

Ley de reciprocidad cuadrática Conjetura 1772

Si p es de la forma $4mq + (2r+1)^2$ entonces q y $-q$ son de la forma $np + s^2$.

Con un lenguaje más sencillo:

Si $8 | (p-1)(q-1)$

$$p | x^2 - q \ \text{ tiene solución } \Leftrightarrow q | x^2 - p \ \text{ tiene solución}$$

Si $8 \nmid (p-1)(q-1)$

$$p | x^2 - q \ \text{ tiene solución } \Leftrightarrow q | x^2 - p \ \text{ no tiene solución}$$

Reciprocidad cuadrática

p, q primos distintos mayores que dos.

Ley de reciprocidad cuadrática — Conjetura 1772

Si p es de la forma $4mq + (2r+1)^2$ entonces q y $-q$ son de la forma $np + s^2$.

Con un lenguaje más sencillo:

$$\begin{aligned}
&\text{Si } 8|(p-1)(q-1)\\
&\qquad p|x^2-q \ \text{ tiene solución } \ \Leftrightarrow q|x^2-p \ \text{ tiene solución}\\
&\text{Si } 8\nmid(p-1)(q-1)\\
&\qquad p|x^2-q \ \text{ tiene solución } \ \Leftrightarrow q|x^2-p \ \text{ no tiene solución}
\end{aligned}$$

Ej: $41|x^2-5$ para $x=13$, $\quad 5|x^2-41$ para $x=1$

Después de Euler

- Gauss (1801) demostró la ley de reciprocidad y creó una teoría de formas cuadráticas (clases, géneros, composición).

Después de Euler

- Gauss (1801) demostró la ley de reciprocidad y creó una teoría de formas cuadráticas (clases, géneros, composición).
- Artin (1927) dio una formulación muy general de la ley de reciprocidad que se aplica a extensiones de cuerpos.

Después de Euler

- Gauss (1801) demostró la ley de reciprocidad y creó una teoría de formas cuadráticas (clases, géneros, composición).
- Artin (1927) dio una formulación muy general de la ley de reciprocidad que se aplica a extensiones de cuerpos.
- Actualmente se sabe que falta como mucho un número idóneo en la tabla de Euler (Chowla 1934) y que, si existe, debe ser mayor que cien millones.

Los albores de los métodos analíticos

Diversas observaciones sobre series infinitas 1744

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\dots\cdot\frac{p}{p-1}\cdot\dots \quad = \quad \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\dots$$

Los albores de los métodos analíticos

Diversas observaciones sobre series infinitas 1744

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\cdots\cdot\frac{p}{p-1}\cdot\ldots = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots$$

$$\prod(1-p^{-1})^{-1} = \sum\frac{1}{n}$$

Los albores de los métodos analíticos

Diversas observaciones sobre series infinitas 1744

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\cdots\cdot\frac{p}{p-1}\cdot\cdots = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots$$

$$\prod(1-p^{-1})^{-1} = \sum\frac{1}{n} = x$$

Los albores de los métodos analíticos

Diversas observaciones sobre series infinitas 1744

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\dots\cdot\frac{p}{p-1}\cdot\ldots = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\dots$$

$$\prod(1-p^{-1})^{-1} = \sum\frac{1}{n} = x$$

$$\left.\begin{aligned} x &= \sum\frac{1}{n} \\ \frac{1}{2}x &= \sum\frac{1}{2n} \end{aligned}\right\} \Rightarrow x\left(1-\frac{1}{2}\right) = \sum_{2\nmid n}\frac{1}{n}$$

Los albores de los métodos analíticos

Diversas observaciones sobre series infinitas 1744

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\dots\cdot\frac{p}{p-1}\cdot\ldots = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots$$

$$\prod(1-p^{-1})^{-1} = \sum\frac{1}{n} = x$$

$$\left.\begin{aligned} x(1-\frac{1}{2}) &= \sum_{2\nmid n}\frac{1}{n} \\ \frac{1}{3}x(1-\frac{1}{2}) &= \sum_{2\nmid n}\frac{1}{3n} \end{aligned}\right\} \Rightarrow x(1-\frac{1}{2})(1-\frac{1}{3}) = \sum_{\substack{2\nmid n\\ 3\nmid n}}\frac{1}{n},\ldots \quad \text{etc.}$$

Los albores de los métodos analíticos

Diversas observaciones sobre series infinitas 1744

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\cdots\cdot\frac{p}{p-1}\cdot\ldots = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots$$

$$\prod(1-p^{-1})^{-1} = \sum\frac{1}{n} = x$$

El producto de Euler

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}, \qquad \zeta(s)=\prod_p(1-p^{-s})^{-1}.$$

La distribución de los primos

¿Para qué otra demostración de la infinitud de los primos?

La distribución de los primos

Corolario 1 $\prod(1-p^{-s})^{-1}=\sum n^{-s},\ s=1$

Se cumple $\prod(1-p^{-1})^{-1}=\log\infty$.

"$\log\infty$ es el mínimo entre todas las potencias de infinito".

La distribución de los primos

Corolario 1 $\prod(1-p^{-s})^{-1} = \sum n^{-s},\ s=1$

Se cumple $\prod(1-p^{-1})^{-1} = \log\infty$.

Corolario 2 $\prod(1-n^{-2})^{-1} = 2$

Los primos son infinitamente más numerosos que los cuadrados.

La distribución de los primos

Corolario 1 $\prod(1-p^{-s})^{-1} = \sum n^{-s},\ s=1$

Se cumple $\prod(1-p^{-1})^{-1} = \log\infty$.

Corolario 2 $\prod(1-n^{-2})^{-1} = 2$

Los primos son infinitamente más numerosos que los cuadrados.

Corolario 3 $\prod(1-n^{-1})^{-1} = \infty, \quad \log\infty < \infty$

Los primos son infinitamente menos numerosos que los naturales.

La distribución de los primos

Corolario 1 $\prod(1-p^{-s})^{-1} = \sum n^{-s}$, $s=1$

Se cumple $\prod(1-p^{-1})^{-1} = \log\infty$.

Corolario 2 $\prod(1-n^{-2})^{-1} = 2$

Los primos son infinitamente más numerosos que los cuadrados.

Corolario 3 $\prod(1-n^{-1})^{-1} = \infty, \quad \log\infty < \infty$

Los primos son infinitamente menos numerosos que los naturales.

Corolario 4 $\log\prod(1-p^{-1})^{-1} \sim p^{-1}$

La suma de los inversos de los primos diverge: $\sum p^{-1} = \log\log\infty$.

Después de Euler

Mertens (1897):

$$\prod_{p<x}(1-p^{-1})^{-1} \sim C\log x \qquad \text{y} \qquad \sum_{p<x}\frac{1}{p} \sim \log\log x$$

dando sentido explícito a los infinitos de Euler.

Después de Euler

Mertens (1897):

$$\prod_{p<x}(1-p^{-1})^{-1} \sim C\log x \qquad \text{y} \qquad \sum_{p<x}\frac{1}{p} \sim \log\log x$$

dando sentido explícito a los infinitos de Euler.

La definición de $\zeta(s)$ puede extenderse dando lugar a una función meromorfa en $\mathbb{C}$ (¿Euler? Riemann).

Después de Euler

Mertens (1897):

$$\prod_{p<x}(1-p^{-1})^{-1} \sim C\log x \qquad \text{y} \qquad \sum_{p<x}\frac{1}{p} \sim \log\log x$$

dando sentido explícito a los infinitos de Euler.

La definición de $\zeta(s)$ puede extenderse dando lugar a una función meromorfa en $\mathbb{C}$ (¿Euler? Riemann).

Hipótesis de Riemann 1859

Todos los zeros complejos de la función ζ tienen parte real $1/2$.

$$\#\{p<x\} = \int_2^x \frac{dt}{\log t} + O(\sqrt{x}\log x) \qquad \Leftrightarrow \qquad \text{HR es cierta}$$

Referencias

Referencias electrónicas

THE EULER ARCHIVE

- http://www.math.dartmouth.edu/~euler/

ED SANDIFER'S 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`