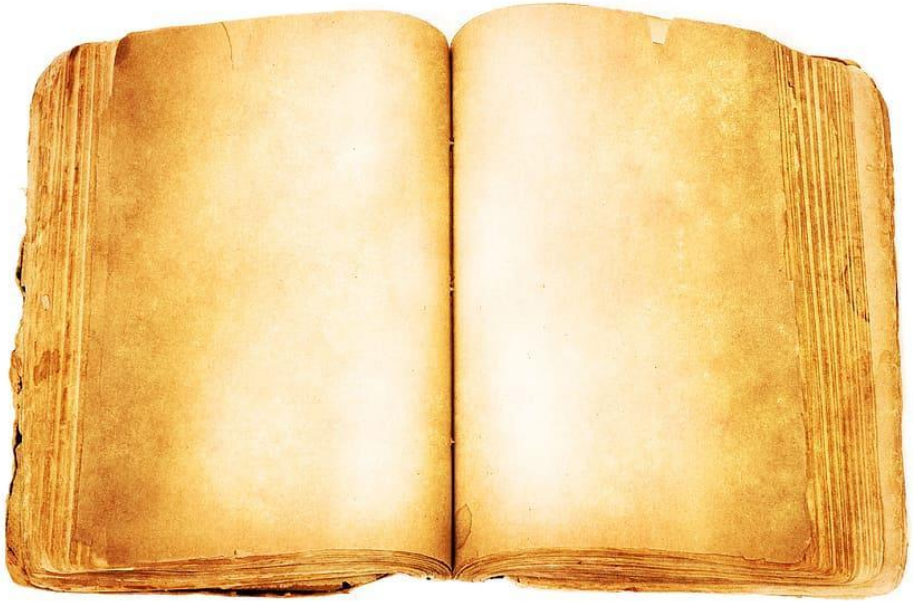
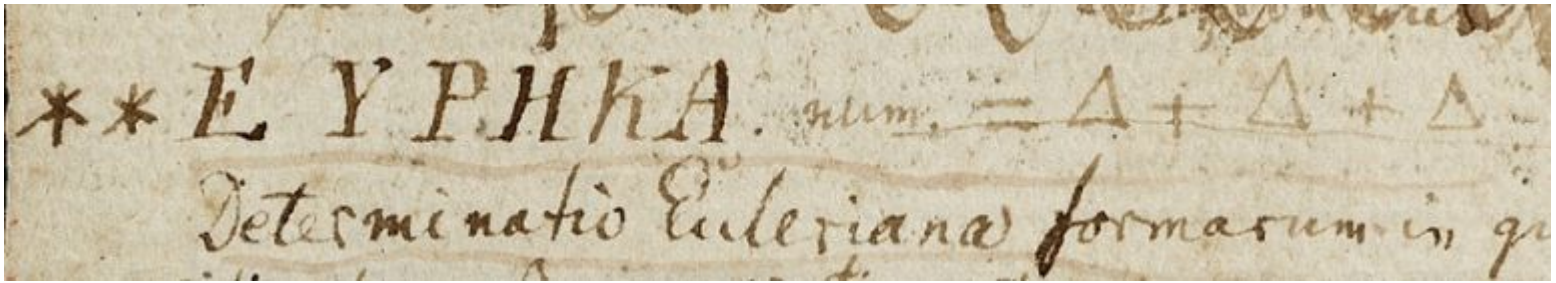
1796



Notizenjournal
146 notas
19 páginas


** EYPHKA.
Determinatio Eulerian formarum

Carl Friedrich Gauß

1777-1855

GN4480100S8

Deutsche Bundesbank

Frankfurt am Main
1. September 1999

Princeps Mathematicorum

01 Formalidad y rigor

02 Reservado

“Hace mucho tiempo que tengo mis resultados, pero no sé aún cómo llegar a ellos”.

Gauss

Princeps Mathematicorum

01 Formalidad y rigor

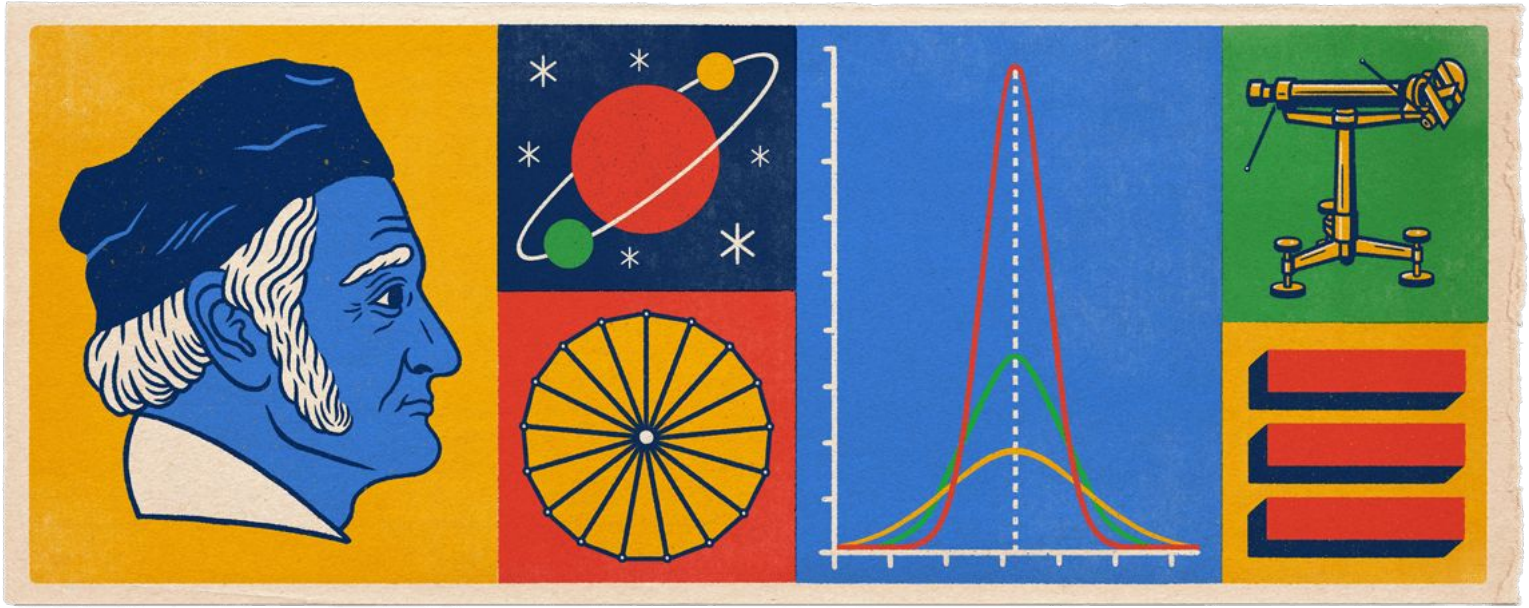
02 Reservado

03 Transdisciplinario

04 Precoz

Doodle-Gauss

30 de abril de 2018



Disquisitiones a

DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

CAR

DELLA SCOPERTA

DEL NUOVO PIANETA

CERERE FERDINANDEA

OTTAVO TRA I PRIMARJ DEL NOSTRO SISTEMA SOLARE.

PALERMO

1802

NELLA STAMPERIA REALE.

Disquisitiones arithmeticae

Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum vbi opus erit in clausulis adiungentes, $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$ *).

¿En qué casos la suma de dos cuadrados resulta congruente con 3 módulo 4.

Módulo 4

$2n + 1$

Primos

$4k + 1$

$4k + 3$

2 y todos los primos de la forma 4k+1 se pueden escribir como suma de dos cuadrados.

Los primos de la forma 4k+3 no se pueden escribir como suma de dos cuadrados.

¿En qué casos la suma de dos cuadrados resulta congruente con 3 módulo 4.

Módulo 4

n^2

$0^2=0\equiv 0$
$1^2=1\equiv 1$
$2^2=4\equiv 0$
$3^2=9\equiv 1$

n^2+m^2

$0+0\equiv 0$
$0+1\equiv 1$
$1+1\equiv 2$

LRC

$$x^2 \equiv p \pmod{q}$$
$$y^2 \equiv q \pmod{p}$$

Teorema áureo

Si ninguno de los primos p o q pertenece a la sucesión 4k+1 entonces una de las congruencias tiene solución si y sólo si la otra no tiene solución.

Si alguno de los primos pertenece a la sucesión 4k+1 entonces o bien ambas congruencias tienen solución o bien ninguna de las dos tiene solución.

LRC

Versión de Legendre.

Sean p y q primos impares. Entonces.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Versión de Euler.

Si p y q son primos impares distintos, entonces $\left(\frac{p}{q}\right) = 1$ si y sólo si $p \equiv \pm b^2 \bmod 4q$ para algún entero impar b.

LRC

Versión de Gauss.

Sean p y q primos impares. Entonces

- Si p es de la forma 4n + 1, entonces q es un residuo cuadrático módulo p si y sólo si p es un residuo cuadrático módulo q.

- Si p es de la forma 4n + 3, entonces q es un residuo cuadrático módulo p si y sólo si −p es un residuo cuadrático módulo q.

Residuos cuadráticos

Definición. Sea p un primo impar. Un entero ***a***, coprimo con ***p***, es un residuo cuadrático módulo ***p***, si existe un x tal que $x^2 \equiv a \pmod{p}$

En caso contrario ***a*** es un no-residuo cuadrático módulo ***p***.

LRC

Definición. Sea p un primo impar. Un entero ***a***, coprimo con ***p***, es un residuo cuadrático módulo ***p***, si existe un x tal que $x^2 \equiv a \pmod{p}$

En caso contrario ***a*** es un no-residuo cuadrático módulo ***p***.

Sean p y q primos impares. Entonces

- Si p es de la forma 4n + 1, entonces q es un residuo cuadrático módulo p si y sólo si p es un residuo cuadrático módulo q.
- Si p es de la forma 4n + 3, entonces q es un residuo cuadrático módulo p si y sólo si –p es un residuo cuadrático módulo q.

$$x^2 \equiv p \pmod{q}$$
$$y^2 \equiv q \pmod{p}$$

17

Primo

$17 \equiv 1$ módulo 4

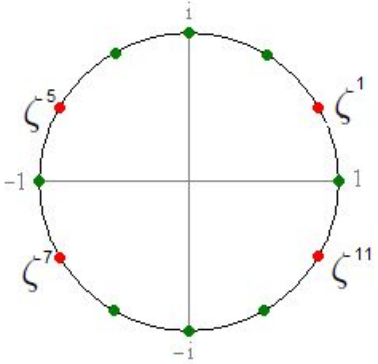
Ciclotómicos

Polinomios ciclotómicos

De orden n
Φ_n

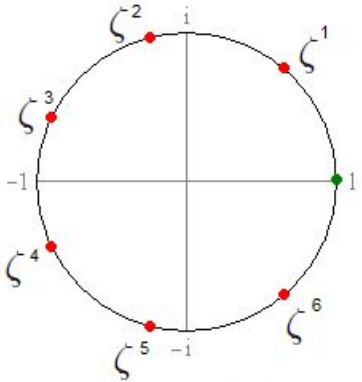
Polinomio unitario
cuyas raíces son todas las raíces primitivas de orden n de la unidad.

$z^n = 1$.
Donde z es un número complejo.



con $\zeta = e^{\frac{2i\pi}{12}} = e^{\frac{i\pi}{6}}$

$$\Phi_{12} = (X-\zeta)(X-\zeta^5)(X-\zeta^7)(X-\zeta^{11}) = X^4 - X^2 + 1$$



con $\zeta = e^{\frac{2i\pi}{7}}$

$$\Phi_7 = (X-\zeta)(X-\zeta^2)(X-\zeta^3)(X-\zeta^4)(X-\zeta^5)(X-\zeta^6) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

Φ_{17}

$$\Phi_{17} = \frac{X^{17} - 1}{\Phi_1}$$

$$= \frac{X^{17} - 1}{X - 1}$$

$$= X^{16} + X^{15} + X^{14} + X^{13} + X^{12} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$