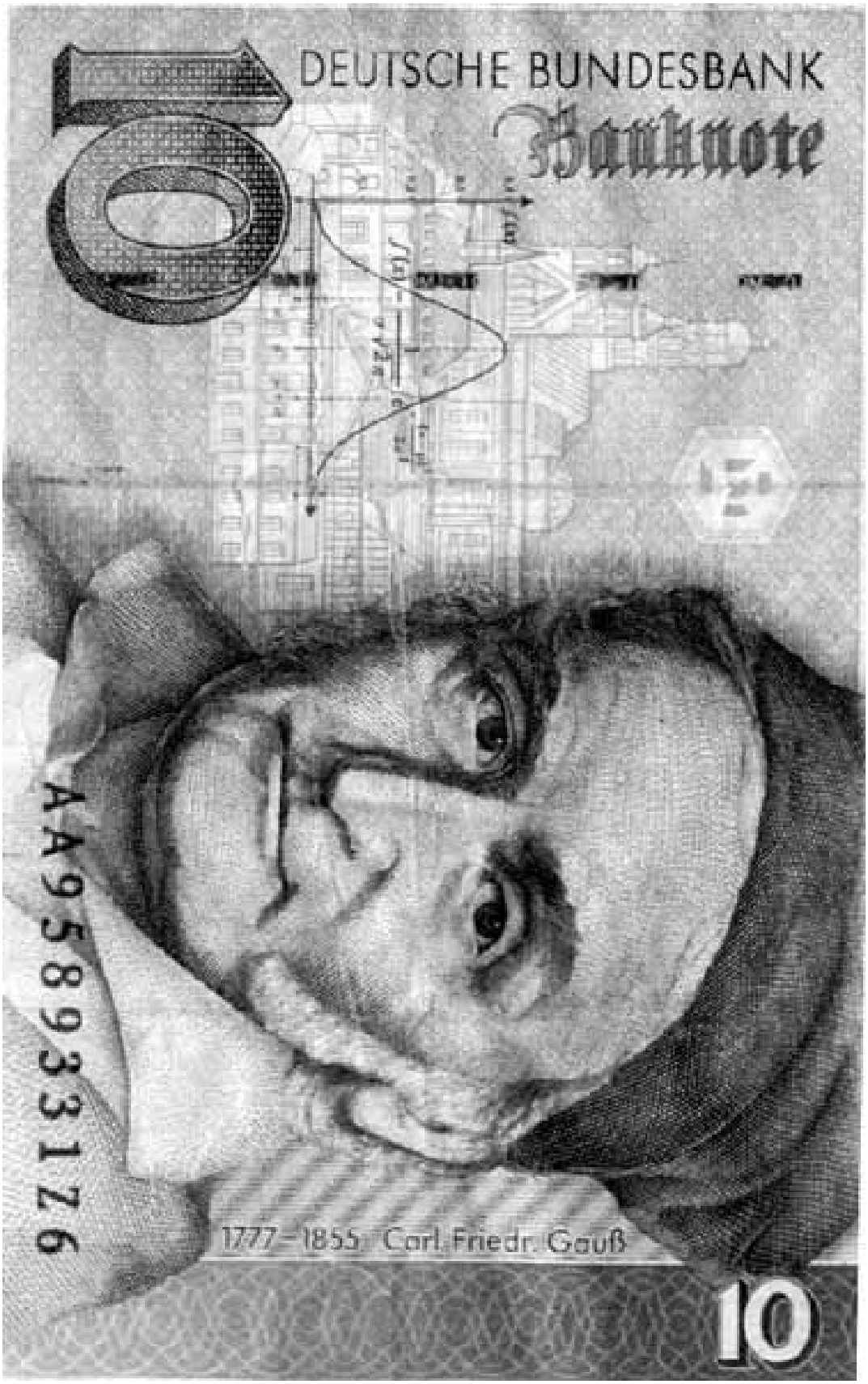
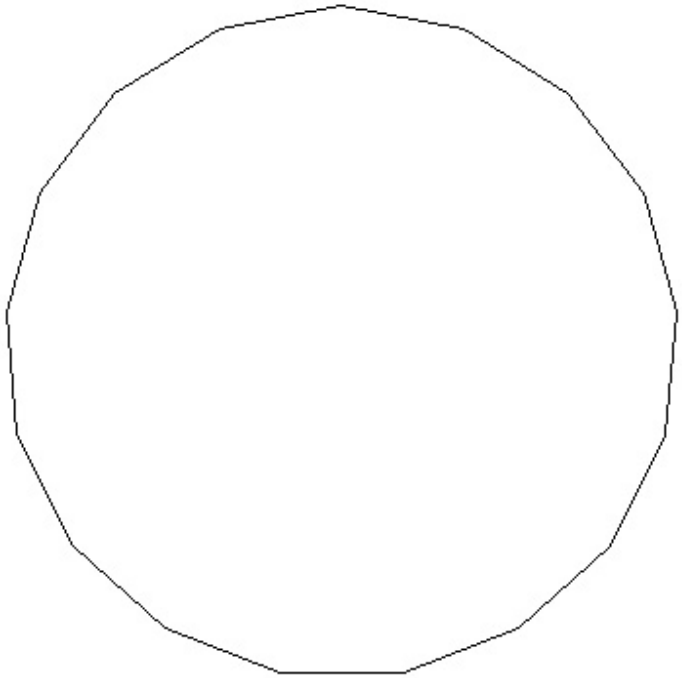
L'Última Anotació de Gauss.

Xavier Xarles

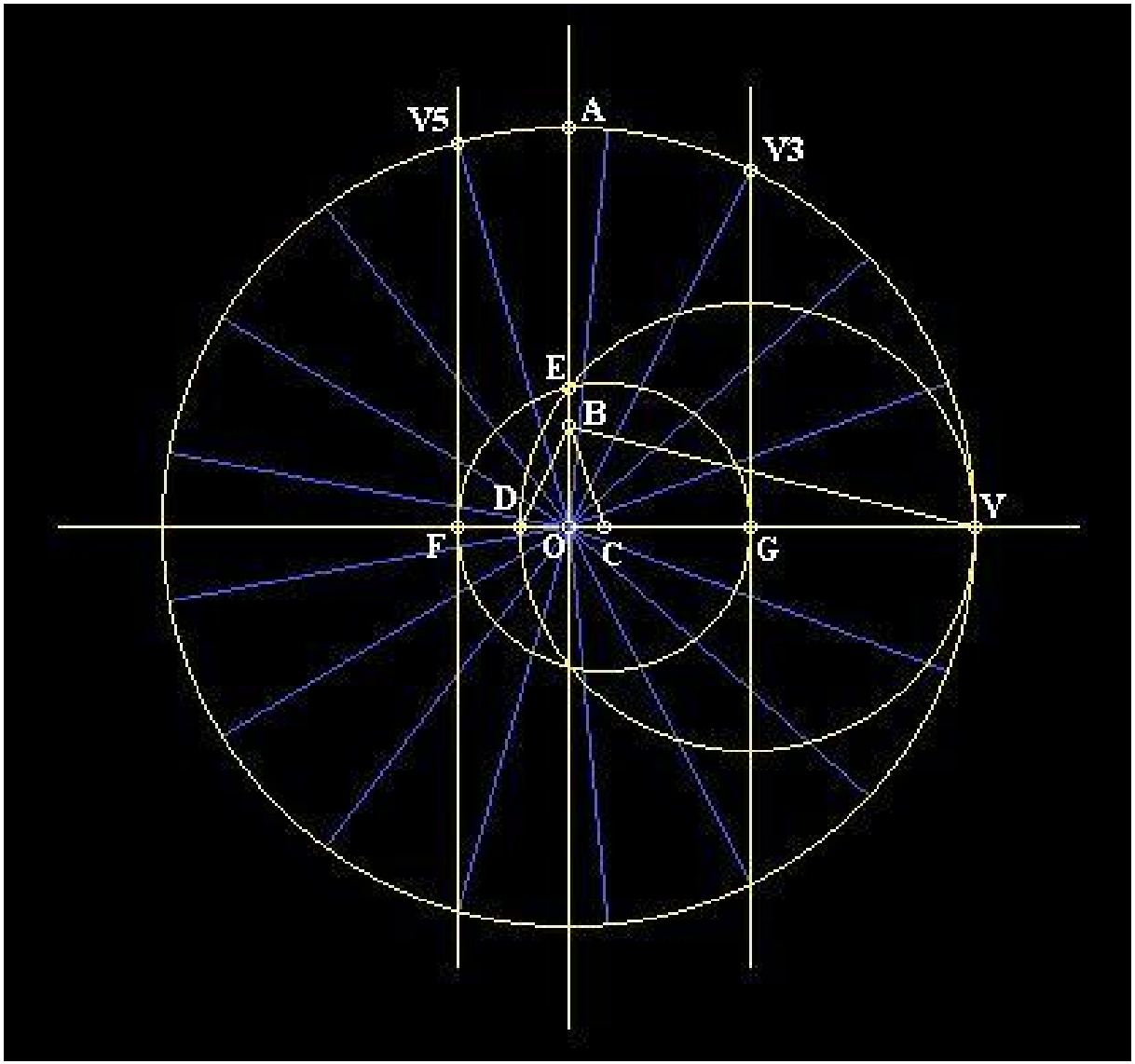

DEUTSCHE BUNDESBANK
Banknote
AA9589331 Z 6
1777 – 1855 Carl Friedr. Gauß
10

Polígon regular de 17 costats



$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+ 2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\right)$$

Gauss als 26 anys.


V5
A
V3
E
B
D
V
F
O
C
G

Gauss als 51 anys.

9 de Juliol, 1814. (37 anys).

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a + bi$ *est numerus primus,* $a - 1 + bi$ *per* $2 + 2i$ *divisibilis, multitudo omnium solutionum congrentiae*

$$1 \equiv xx + yy + xxyy \pmod{a + bi}$$

inclusis $x = \infty$, $y = \pm i$; $x = \pm i$, $y = \infty$ *fit* $= (a-1)^2 + b^2$.

9 de Juliol, 1814. (37 anys).

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ *est numerus primus,* $a-1+bi$ *per* $2+2i$ *divisibilis, multitudo omnium solutionum congrentiae*

$$1 \equiv xx + yy + xxyy \pmod{a+bi}$$

inclusis $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ *fit* $=(a-1)^2+b^2$.

He observat per inducció el fet més important que relaciona la teoria de residus biquadràtics amb les funcions lemniscàtiques. Suposeu que $a+bi$ és un nombre primer, $a-1+bi$ divisible per $2+2i$, aleshores el nombre de totes les solucions de la congruència:

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a+bi}$$

incloent $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ és $=(a-1)^2+b^2$.

9 de Juliol, 1814. (37 anys).

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ *est numerus primus,* $a-1+bi$ *per* $2+2i$ *divisibilis, multitudo omnium solutionum congrentiae*

$$1 \equiv xx + yy + xxyy \pmod{a+bi}$$

inclusis $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ *fit* $=(a-1)^2+b^2$.

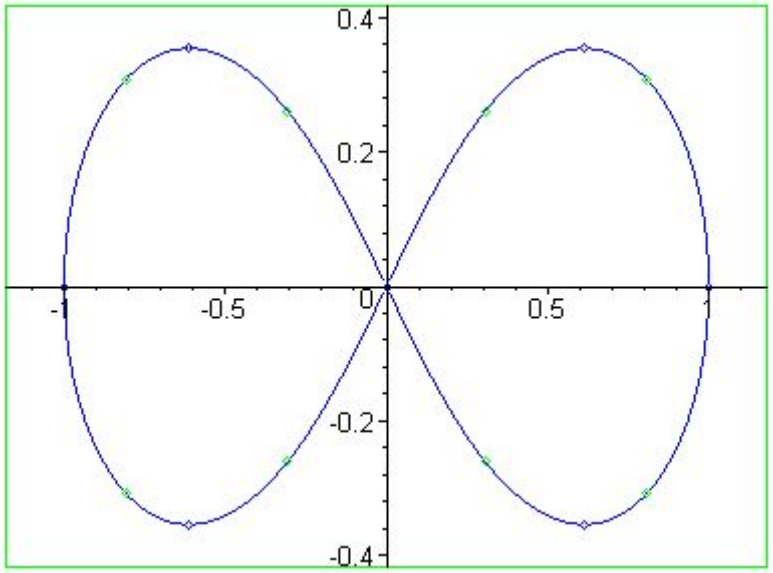
He observat per inducció el fet més important que relaciona la teoria de residus biquadràtics amb les funcions lemniscàtiques. Suposeu que $a+bi$ és un nombre primer, $a-1+bi$ divisible per $2+2i$, aleshores el nombre de totes les solucions de la congruència:

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a+bi}$$

incloent $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ és $=(a-1)^2+b^2$.

Funcions lemniscàtiques

La lemniscata:



Equació:

$$(x^2 + y^2)^2 = (x^2 - y^2)$$

En polars:

$$r^2 = \cos(2\theta)$$

Parametrització:

$$2x^2 = r^2 + r^4 \qquad 2y^2 = r^2 - r^4$$

És el conjunt de punts P tals que

$$d(P,(0.5,0))d(P,(-0.5,0))) = \frac{1}{4}$$

Funcions lemniscàtiques

Cercle:

Llargada del arc (en el primer quadrant)

$$z = \int_0^w \frac{dt}{\sqrt{1-t^2}}$$

Surt de

$$(x'(r))^2 + (y'(r))^2 = (1-r^2)^{-1}$$

La funció inversa que a cada z associa w és

$$w = \sin(z).$$

Lemniscata:

Llargada del arc (en el primer quadrant)

$$z = \int_0^w \frac{dt}{\sqrt{1-t^4}}$$

Surt de

$$(x'(r))^2 + (y'(r))^2 = (1-r^4)^{-1}$$

La funció inversa que a cada z associa w és

$$w = \sin \text{ lemn } (z) =: \mathrm{sl}(z)$$

Funcions lemniscàtiques

Cercle:

La longitud del mig cercle és

$$\pi = 2\int_0^1 \frac{dt}{\sqrt{1-t^2}} = 3.141592...$$

Exemple: $\sin(\pi/4) = \sqrt{2}/2$

Definim

$$\cos(z) := \sin(z + \frac{\pi}{2})$$

Es compleix

$$\sin^2(z) + \cos^2(z) = 1$$

Lemniscata:

La longitud de mitja corba és

$$\omega = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 2.62205...$$

Exemple: $\mathrm{sl}(\omega/4) = \sqrt{\sqrt{2}-1}$

Definim

$$\mathrm{cl}(z) := \mathrm{sl}(z + \frac{\omega}{2})$$

Es compleix

$$\mathrm{sl}^2(z) + \mathrm{cl}^2(z) + \mathrm{sl}^2(z)\mathrm{cl}^2(z) = 1$$

9 de Juliol, 1814. (37 anys).

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ *est numerus primus,* $a-1+bi$ *per* $2+2i$ *divisibilis, multitudo omnium solutionum congrentiae*

$$1 \equiv xx + yy + xxyy \pmod{a+bi}$$

inclusis $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ *fit* $=(a-1)^2+b^2$.

He observat per inducció el fet més important que relaciona la teoria de residus biquadràtics amb les funcions lemniscàtiques. Suposeu que $a+bi$ és un nombre primer, $a-1+bi$ divisible per $2+2i$, aleshores el nombre de totes les solucions de la congruència:

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a+bi}$$

incloent $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ és $=(a-1)^2+b^2$.

L'equació

Volem contar quantes solucions N té l'equació:

$$x^2 + y^2 + x^2y^2 = 1 (\text{mod } p).$$

Si l'escrivim com

$$y^2(x^2 + 1) = 1 - x^2$$

multiplicant per $(1 + x^2)$ als dos costats tenim

$$\Big((1 + x^2)y\Big)^2 = 1 - x^4$$

Substituint $w = (1 + x^2)y$ obtenim l'equació

$$w^2 = 1 - x^4.$$

L'equació

Observem que l'aplicació

$$\{(x,y) \mid x^2+y^2+x^2y^2=1\} \longrightarrow \{(x,w) \mid w^2=1-x^4\}$$

$$(x,y) \rightarrowtail (x,(1+x^2)y)$$

té inversa

$$(x,\frac{w}{(1+x^2)}) \leftarrowtail (x,w)$$

ven definida sempre que $x^2 \neq -1$.

L'equació

Com que -1 és un quadrat mod $p \Leftrightarrow p \equiv 1(\text{mod } 4)$, tenim que:

- Si $p \equiv 3(\text{mod } 4)$, aleshores hi ha tantes solucions de l'equació: $x^2 + y^2 + x^2y^2 \equiv 1(\text{mod } p)$ com de l'equació $w^2 \equiv 1 - x^4(\text{mod } p)$.

- Si $p \equiv 1(\text{mod } 4)$, aleshores hi ha dues solucions menys de l'equació: $x^2 + y^2 + x^2y^2 \equiv 1(\text{mod } p)$ que de l'equació $w^2 \equiv 1 - x^4(\text{mod } p)$.

9 de Juliol, 1814. (37 anys).

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ *est numerus primus,* $a-1+bi$ *per* $2+2i$ *divisibilis, multitudo omnium solutionum congrentiae*

$$1 \equiv xx + yy + xxyy \pmod{a+bi}$$

inclusis $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ *fit* $=(a-1)^2+b^2$.

He observat per inducció el fet més important que relaciona la teoria de residus biquadràtics amb les funcions lemniscàtiques. Suposeu que $a+bi$ és un nombre primer, $a-1+bi$ divisible per $2+2i$, aleshores el nombre de totes les solucions de la congruència:

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a+bi}$$

incloent $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ és $=(a-1)^2+b^2$.

Residus quadràtics

El problema:

¿Quins nombres enters són un quadrat mòdul un nombre primer p?

Denotem per

$$\left(\frac{n}{p} \right) = 1$$

si $n \not\equiv 0 \pmod{p}$ i n és un quadrat mòdul p, i per

$$\left(\frac{n}{p} \right) = -1$$

si $n \not\equiv 0 \pmod{p}$ i n **no** és un quadrat mòdul p.

Exercici

$$\left(\begin{array}{c} n \\ p \end{array} \right) \equiv n^{\frac{p-1}{2}} (\text{mod } p)$$

$$\left(\begin{array}{c} -1 \\ p \end{array} \right) \equiv 1 (\text{mod } p) \Leftrightarrow p \equiv 1 (\text{mod } 4)$$

$$\left(\begin{array}{c} 2 \\ p \end{array} \right) \equiv 1 (\text{mod } p) \Leftrightarrow p \equiv 3, 5 (\text{mod } 8)$$

Interpretació moderna

$$
\begin{array}{ccccc}
 & & n & \mapsto & n^{\frac{p-1}{2}} \pmod p \\
\text{Quadrats mod } p & \to & \mathbb{F}_p^* & \to & \{\pm 1\} \\
\updownarrow & & \updownarrow & & \updownarrow \\
\mathbb{Z}/(\frac{p-1}{2})\mathbb{Z} & \to & \mathbb{Z}/(p-1)\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z}
\end{array}
$$

Llei de reciprocitat quadràtica

Si p i q són dos nombres primers senars, aleshores

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

Per exemple, si $p \equiv 1 (\text{mod } 4)$, aleshores

$$\left(\begin{array}{c} q \\ p \end{array}\right) = \left(\begin{array}{c} p \\ q \end{array}\right)$$

Residus biquadràtics (o quàrtics)

És l'equivalent però per a detectar nombres que són potencies quartes.

Idea important: És imprescindible, a l'hora de definir un símbol quàrtic, treballar amb nombres de $\mathbb{Z}[i]$.

Què passa quan $p \equiv 3$(**mod** 4)**.**

Si $p \equiv 3(\text{mod } 4)$, aleshores un nombre és un biquadrat si i només si és un quadrat.

Per què? Doncs perquè $\frac{p-1}{2}$ no és divisible per 2.

O sigui, perquè 2 és invertible mòdul $\frac{p-1}{2}$.

Idea: llegiu-ho al diagrama

$$
\begin{array}{ccccc}
 & & n & \mapsto & n^{\frac{p-1}{2}} \pmod p \\
\text{Quadrats mod } p & \to & \mathbb{F}_p^* & \to & \{\pm 1\} \\
\updownarrow & & \updownarrow & & \updownarrow \\
\mathbb{Z}/(\frac{p-1}{2})\mathbb{Z} & \to & \mathbb{Z}/(p-1)\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z}
\end{array}
$$

Aplicació: Solucions a $p \equiv 3(\textbf{mod } 4)$.

Si $p \equiv 3(\text{mod } 4)$, els següents conjunts tenen el mateix nombre d'elements:

- Solucions de l'equació $x^2 + y^2 + x^2y^2 \equiv 1(\text{mod } p)$.
- Solucions de l'equació $w^2 \equiv 1 - x^4(\text{mod } p)$.
- Solucions de l'equació $w^2 \equiv 1 - z^2(\text{mod } p)$.

L'últim conjunt té $p + 1$ elements.

Que passa quan $p \equiv 1$(mod 4).

$$p \equiv 1(\text{mod } 4) \Leftrightarrow -1 \text{ és un quadrat (mod } p)$$

Tenim per tant un element i a $\mathbb{F}_p$ tal que $i^2 \equiv -1(\text{mod } p)$.

Altre interpretació:

p és producte de dos elements primers a $\mathbb{Z}[i]$,

$$p = (a + bi)(a - bi) \Leftrightarrow p = a^2 + b^2$$

9 de Juliol, 1814. (37 anys).

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ *est numerus primus,* $a-1+bi$ *per* $2+2i$ *divisibilis, multitudo omnium solutionum congrentiae*

$$1 \equiv xx + yy + xxyy \pmod{a+bi}$$

inclusis $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ *fit* $=(a-1)^2+b^2$.

He observat per inducció el fet més important que relaciona la teoria de residus biquadràtics amb les funcions lemniscàtiques. Suposeu que $a+bi$ és un nombre primer, $a-1+bi$ divisible per $2+2i$, aleshores el nombre de totes les solucions de la congruència:

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a+bi}$$

incloent $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ és $=(a-1)^2+b^2$.

Residus biquadràtics (si $p \equiv 1 (\mathbf{mod}\ 4)$)

Si α i β són primers de $\mathbb{Z}[i]$ que no divideixen a 2, el residu biquadràtic de α mòdul β és

$$\left[\begin{array}{c} \alpha \\ \beta \end{array} \right] = \alpha^{\frac{N\beta-1}{4}} (\text{mod } \beta) \in \{\pm 1, \pm i\} \subseteq \mathbb{F}_p^*$$

on $N\beta$ és el nombre d'elements de $\mathbb{Z}[i]/\beta$, o, equivalentment, igual a $\beta\overline{\beta} = p$.

$$
\begin{array}{ccccc}
 & & \alpha & \mapsto & \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \\
\text{Biquadrats mod } p & \to & \mathbb{F}_p^* & \to & \{\pm 1, \pm i\} \\
\updownarrow & & \updownarrow & & \updownarrow \\
\mathbb{Z}/(\frac{p-1}{4})\mathbb{Z} & \to & \mathbb{Z}/(p-1)\mathbb{Z} & \to & \mathbb{Z}/4\mathbb{Z}
\end{array}
$$

Llei de reciprocitat biquadràtica

Si α i β són dos nombres primers de $\mathbb{Z}[i]$, tals que

$$\alpha \equiv \beta \equiv 1 (\text{mod } 2+2i),$$

aleshores

$$\left[\begin{array}{c} \alpha \\ \beta \end{array} \right] \left[\begin{array}{c} \beta \\ \alpha \end{array} \right] = (-1)^{\frac{N\alpha-1}{4}\frac{N\beta-1}{4}}$$

Observeu que α primer a $\mathbb{Z}[i]$ que no divideix 2 implica que

$$N\alpha \equiv 1 (\text{mod } 4).$$

Lleis de reciprocitat

- G.Eisenstein (1844): Case especial de una llei de reciprocitat per a ℓ-potencies, amb ℓ primer senar.

- E.Kummer(1849,1850,..): Llei de reciprocitat quíntica, i llei de reciprocitat ℓ-àdica per a primers regulars, nombres ideals.

- D.Hilbert(1897,1900): Llei de reciprocitat quadràtica sobre cossos de nombres, problema 9 de Hilbert.

- Ph.Furtwängler(1910): Cos de classes de Hilbert, llei de reciprocitat general.

- T.Takagi (1920): Teoria de cossos de classes.

- H.Hasse (1923): Llei de reciprocitat dèbil.

- E.Artin (1927): Llei de reciprocitat general sobre cossos de nombres (teoria de cossos de classes, isomorfisme amb ideles).

- J.Tate (1965): Formulació de la llei d'Artin amb cohomologia.

- R.Langlands(1967): Teoria de cossos de classes no abeliana (Programa de Langlands)

- V.Drinfeld(1980): Cas de dimensió 2 del programa de Langlands sobre cossos de funcions.

- A.Wiles, ... (1994,2002): Cas especial del programa de Langlands (Conjectura modular de Shimura-Taniyama)

- L.Lafforgue (2000): Cas general del programa de Langlands sobre cossos de funcions.

9 de Juliol, 1814. (37 anys).

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ *est numerus primus,* $a-1+bi$ *per* $2+2i$ *divisibilis, multitudo omnium solutionum congrentiae*

$$1 \equiv xx + yy + xxyy \pmod{a+bi}$$

inclusis $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ *fit* $=(a-1)^2+b^2$.

He observat per inducció el fet més important que relaciona la teoria de residus biquadràtics amb les funcions lemniscàtiques. Suposeu que $a+bi$ és un nombre primer, $a-1+bi$ divisible per $2+2i$, aleshores el nombre de totes les solucions de la congruència:

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a+bi}$$

incloent $x=\infty$, $y=\pm i$; $x=\pm i$, $y=\infty$ és $=(a-1)^2+b^2$.

Reformulació del resultat

Sigui

$$p = a^2 + b^2 \equiv 1 (\text{mod } p)$$

un nombre primer, i suposem que

$$\pi := a + bi \equiv 1 (\text{mod } 2 + 2i).$$

Aleshores el nombre de solucions de $w^2 + x^4 \equiv (\text{mod } p)$, contant les dues a l'infinit, és $p + 1 - 2a$.

Observeu que: $2a = \pi + \overline{pi}$.

A més: Com que $|\pi| = \pi\overline{pi} = p$, aleshores $|\pi| = \sqrt{p}$.

Per tant $|a| \leq \sqrt{p}$.

Demostració:

Encara que molts matemàtics varen creure que Gauss no havia demostrat la seva ultima anotació, això no és cert. (Encara ara hi ha gent que treu preprints pretenent demostrar el resultat!).

De fet està demostrat un cas molt més general en la seva memoria sobre els residus biquadràtics.

La demostració de Gauss consisteix a comptar el nombres de residus quadràtics tals que als sumar 1 són residus biquadràtics, i això ho fa utilitzant el seu símbol biquadràtic.

Un altre resultat de Gauss

Sigui $p \equiv 1 (\text{mod } 3)$ un nombre primer, i sigui π un divisors primer de p a $\mathbb{Z}[\psi]$, on

$$\psi = \frac{-1+\sqrt{-3}}{2} \ , \ \psi^3 = 1.$$

Aleshores l'equació

$$x^3 + y^3 = 1 \ (\text{mod } p)$$

té exactament

$$N_p := p + 1 - \pi - \overline{\pi}$$

solucions, contant les tres solucions a l'infinit.

Observeu que

$$|N_p - (p+1)| = |\pi + \overline{\pi}| = 2|\pi| \leq 2\sqrt{p}.$$

Teorema de Hasse

Sigui $f(x)$ un polinomi de grau 3 a $\mathbb{F}_p[x]$, sense arrels repetides. Aleshores el nombre de solucions N_p de $y^2 = f(x)$ a $\mathbb{F}_p$, contant la solució a l'infinit, compleix que

$$|N_p - (p+1)| \leq 2\sqrt{p}.$$

Conjectures de Weil

Són una versió molt més sofisticada d'aquest resultat.

Weil les formula l'any 1949.

Weil demostrà el cas de corbes l'any 1940.

Grothendieck va demostrar totes les conjectures fora de la més important (anomenada la hipòtesis de Riemann).

Deligne (1974) va demostrar finalment la conjectura en general.

I finalment Wiles

De fet, però això ens portaria massa lluny, tenim que

L'Última anotació de Gauss és un cas particular del Teorema de Wiles.

O sigui, Gauss va demostrar que la corba el·líptica donada per

$$x^2 + y^2 + x^2y^2 = 1$$

és modular.