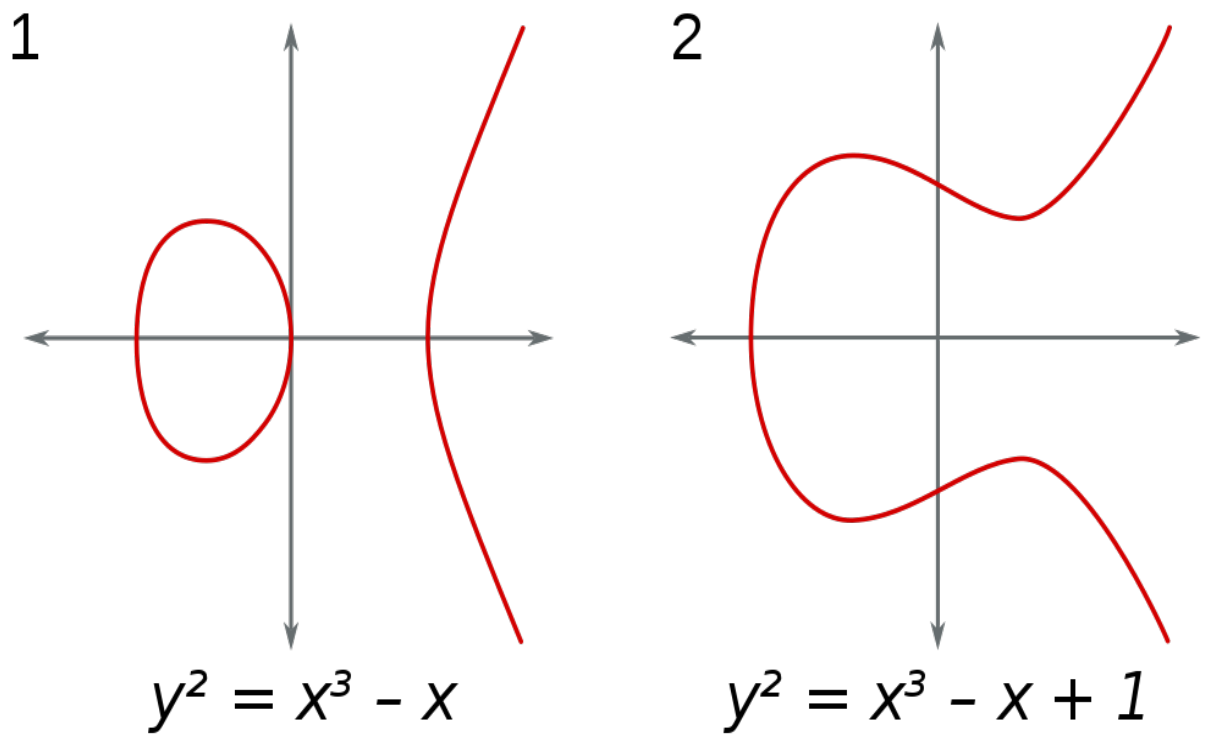
Un viaje por las curvas elípticas y el Último Teorema de Fermat

Marta Sánchez Pavón

Facultad de Matemáticas US

17 de marzo de 2021

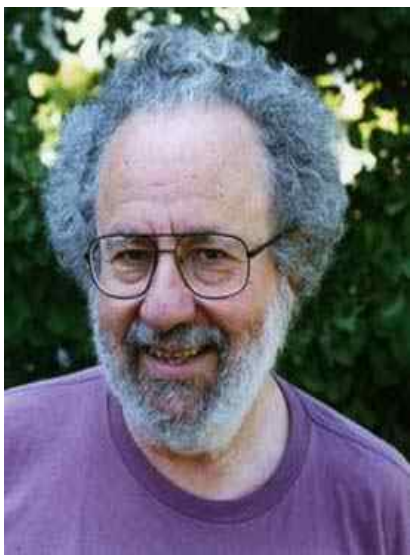
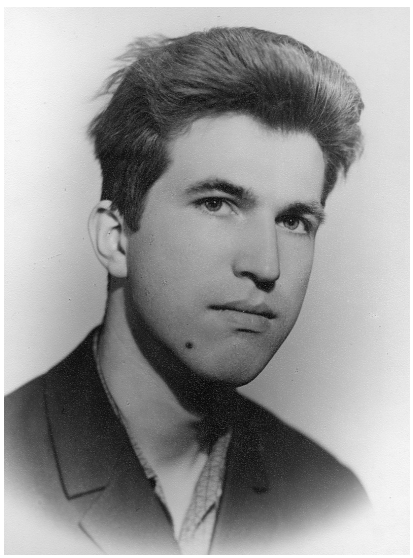
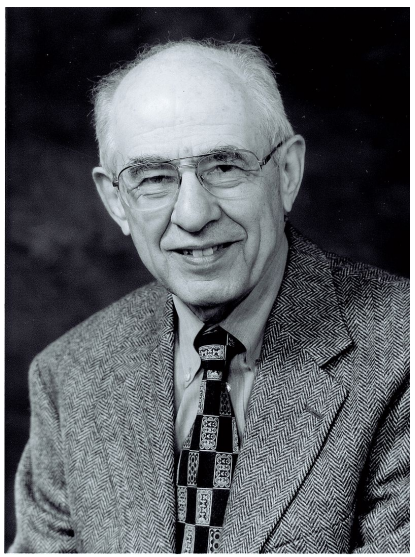
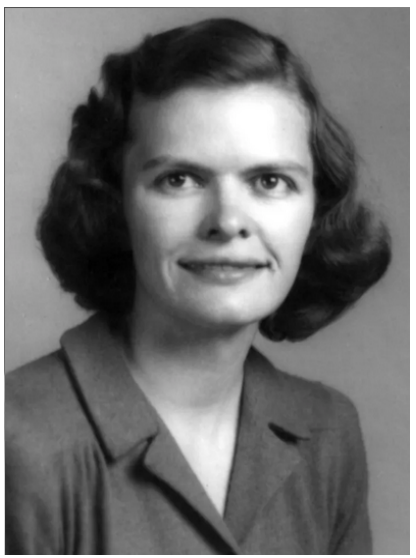
Curvas elípticas



Décimo problema de Hilbert, 1900

Sea $f(x_1, \ldots, x_n) = 0$ una ecuación polinómica con coeficientes en $\mathbb{Z}$. ¿Existe un algoritmo que determine si la ecuación tiene soluciones enteras?

Martin Davis, Yuri Matiyasevich, Hilary Putnam and Julia Robinson demostraron que NO. (1970)

Plimpton 332

$$119^2 + 120^2 = 169^2$$

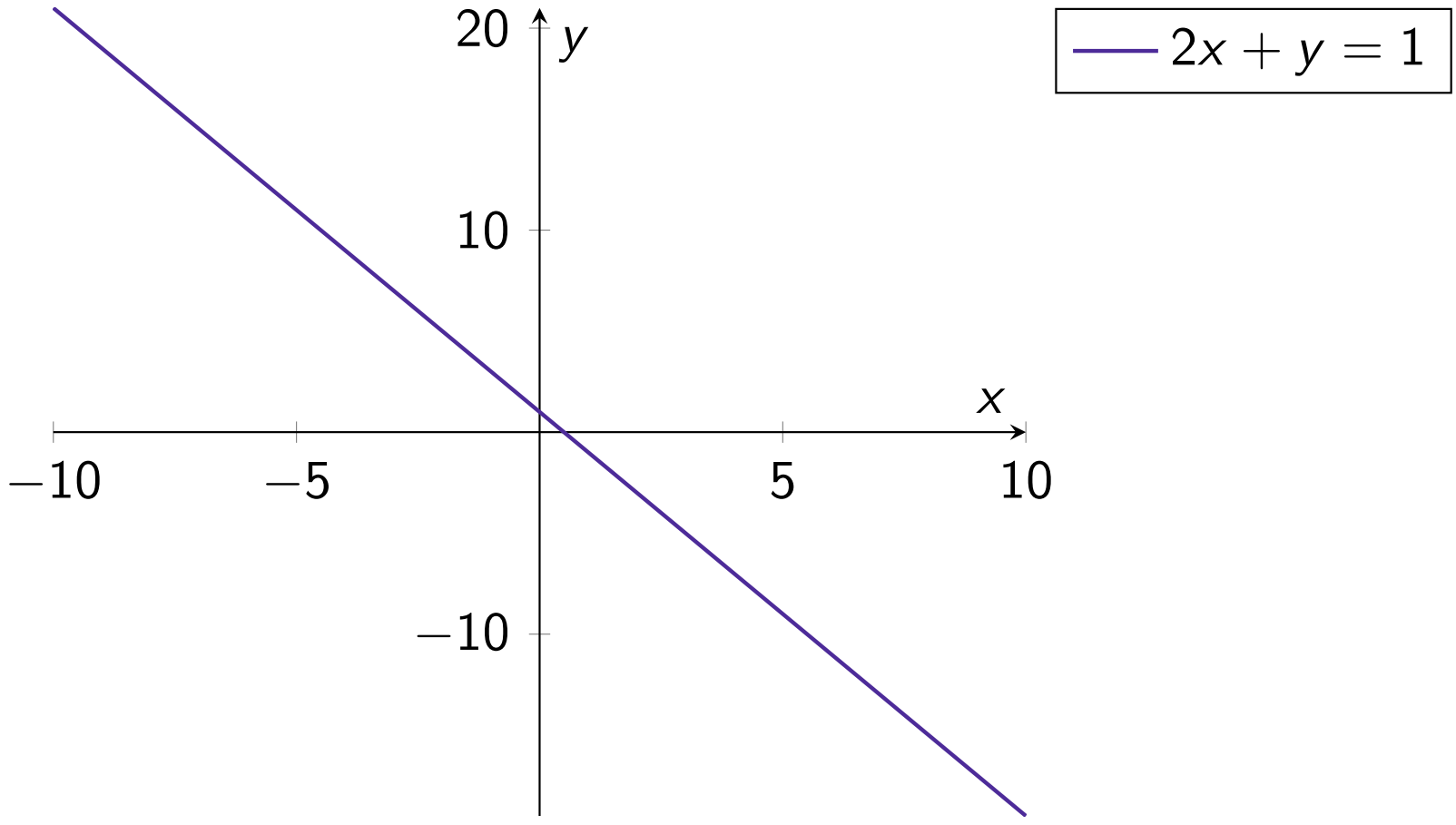
Figura 1: Plimpton 332

Grado 1

$$ax + by = c$$

La ecuación tiene soluciones enteras si y sólo si el máximo común divisor de a y b, $\text{mcd}(a, b)$, divide al entero c.

Ejemplo: $2x + y = 1$. Como $\text{mcd}(2, 1) = 1$ y divide a 1, tiene infinitas soluciones: $x = \lambda$, $y = 1 - 2\lambda$.


20
y
10
x
−10
−5
5
10
−10
2x + y = 1

Grado 2

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

Teorema de Hasse-Minkowski

Una forma cuadrática tiene solución en $\mathbb{Q}$ si y sólo si tiene solución en $\mathbb{R}$ y en $\mathbb{Q}_p$ para todo primo p.

Por ejemplo, las curvas C de género 0 tienen infinitos puntos racionales ó ninguno.

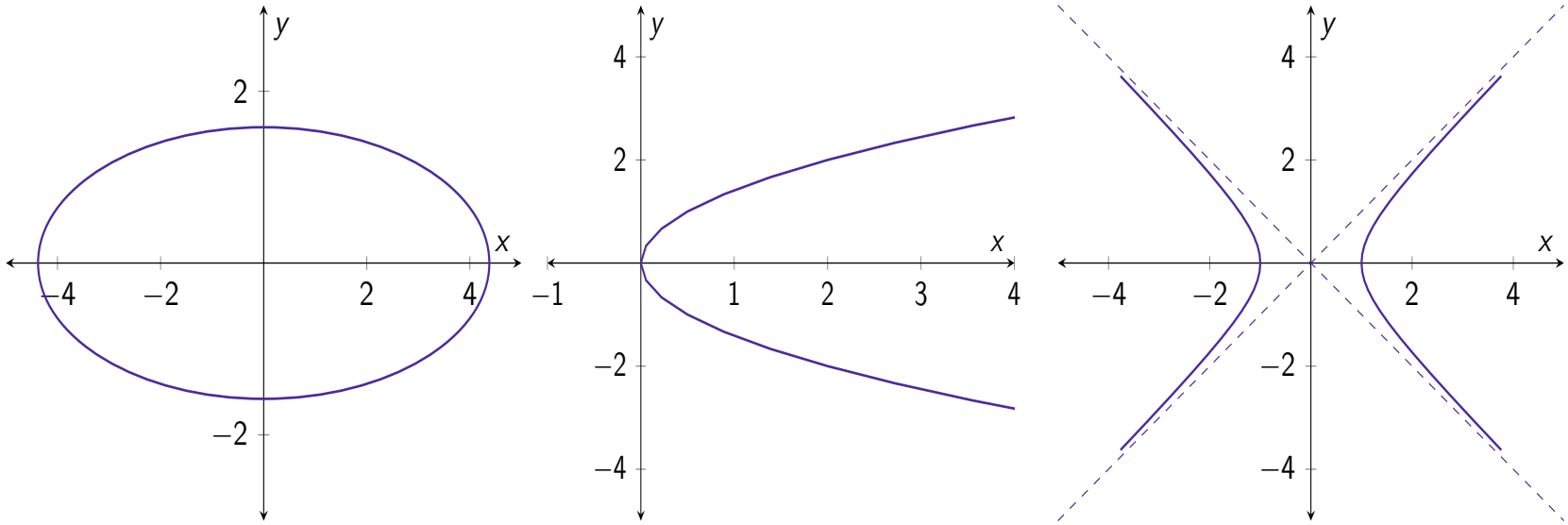


Figura 2: Elipse, parábola, hipérbola

Grado 3

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

¡¡Contraejemplos!!

- $2y^2 = x^4 - 17$ (Carl-Erik Lind, 1940)
- $3x^3 + 4y^3 + 5z^3 = 0$ (Ernst S. Selmer, 1951)

Por ejemplo, las curvas C de género 1 tienen infinitos puntos racionales, ó un número finito de ellos, ó ninguno.

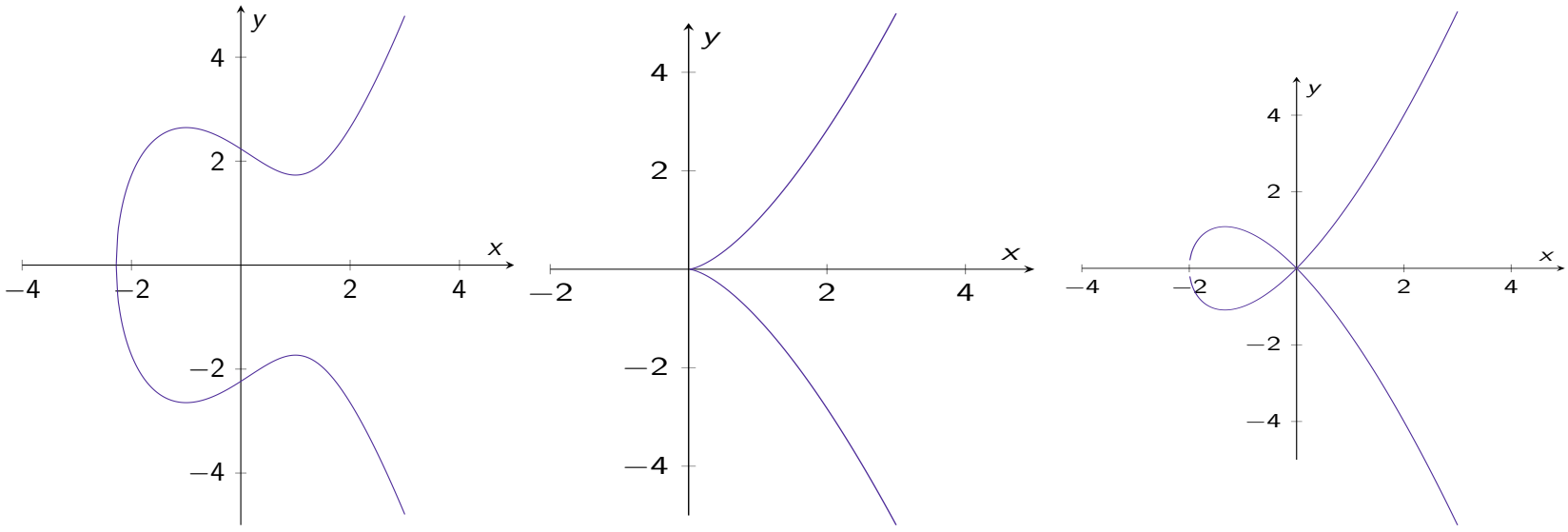


Figura 3: Curva suave, cúspide, nodo

Grado $n > 3$

Teorema de Faltings, 1983

Sea C una curva de género $n > 1$. Entonces el conjunto de los puntos racionales de C es finito.

En resumen, dependiendo del género, el conjunto de puntos racionales es un conjunto...

Género 0	Género 1	Género >1
$\emptyset$	$\emptyset$	$\emptyset$
-	Finito	Finito
Infinito	Infinito	-

Curva elíptica

Una curva elíptica E definida sobre un cuerpo K es una curva tal que:

- es suave,
- es proyectiva,
- tiene género 1,
- existe un punto marcado en E, que denotaremos por $\mathcal{O}$.

Podemos escribirlas en forma de Weierstrass:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

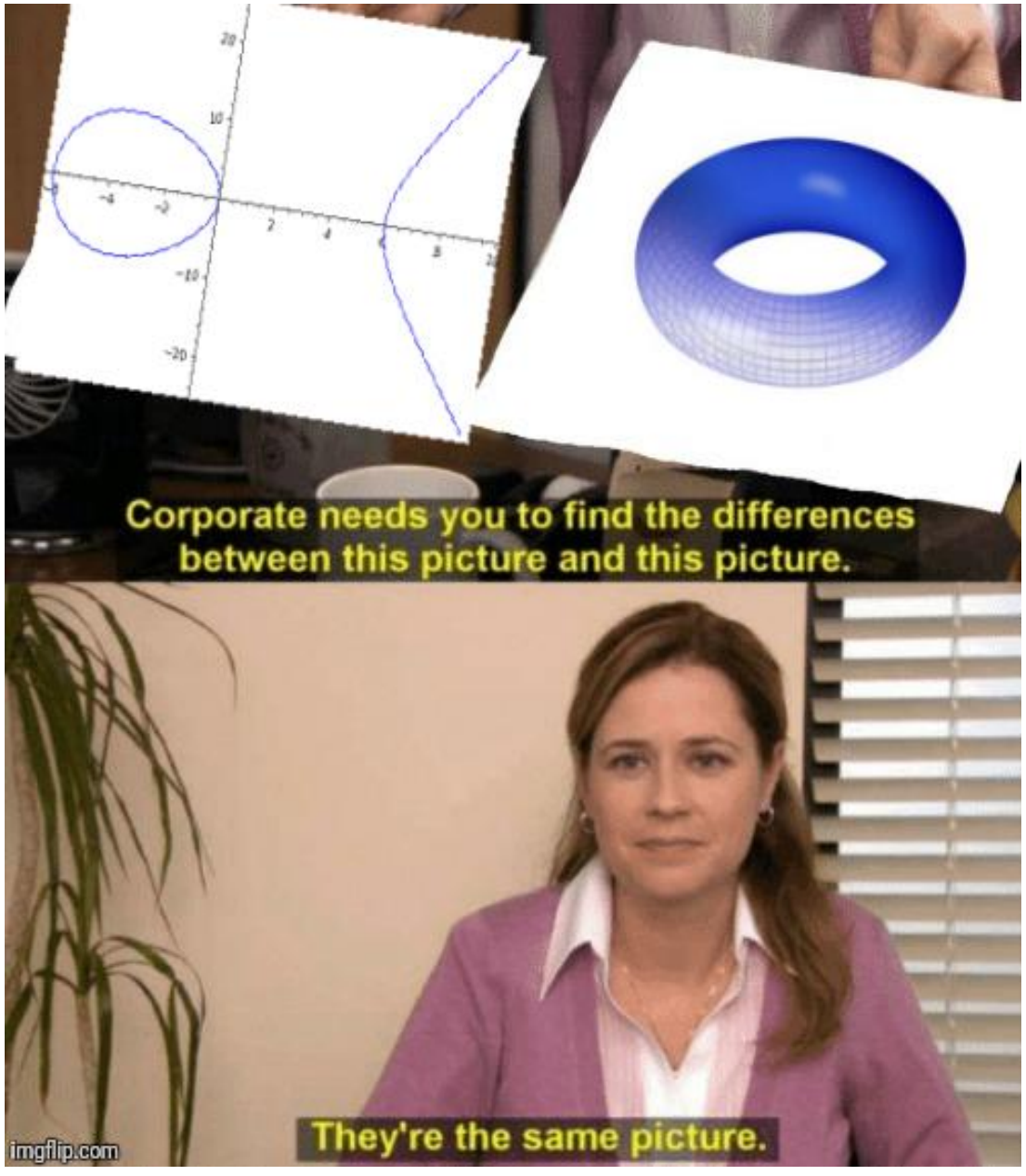


Figura 4: ...son curvas elípticas sobre $\mathbb{C}$!

Si E está definida sobre un cuerpo K de característica distinta de 2 ó 3, entonces podemos escribir E en forma corta de Weierstrass:

$$E : y^2 = x^3 + Ax + B$$

Objetivo: entender los puntos racionales de las curvas elípticas.

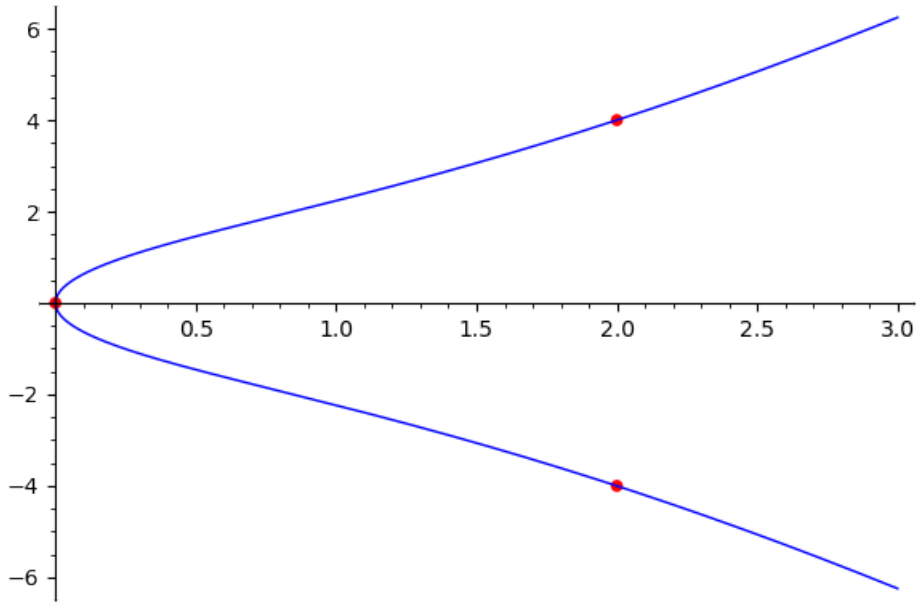
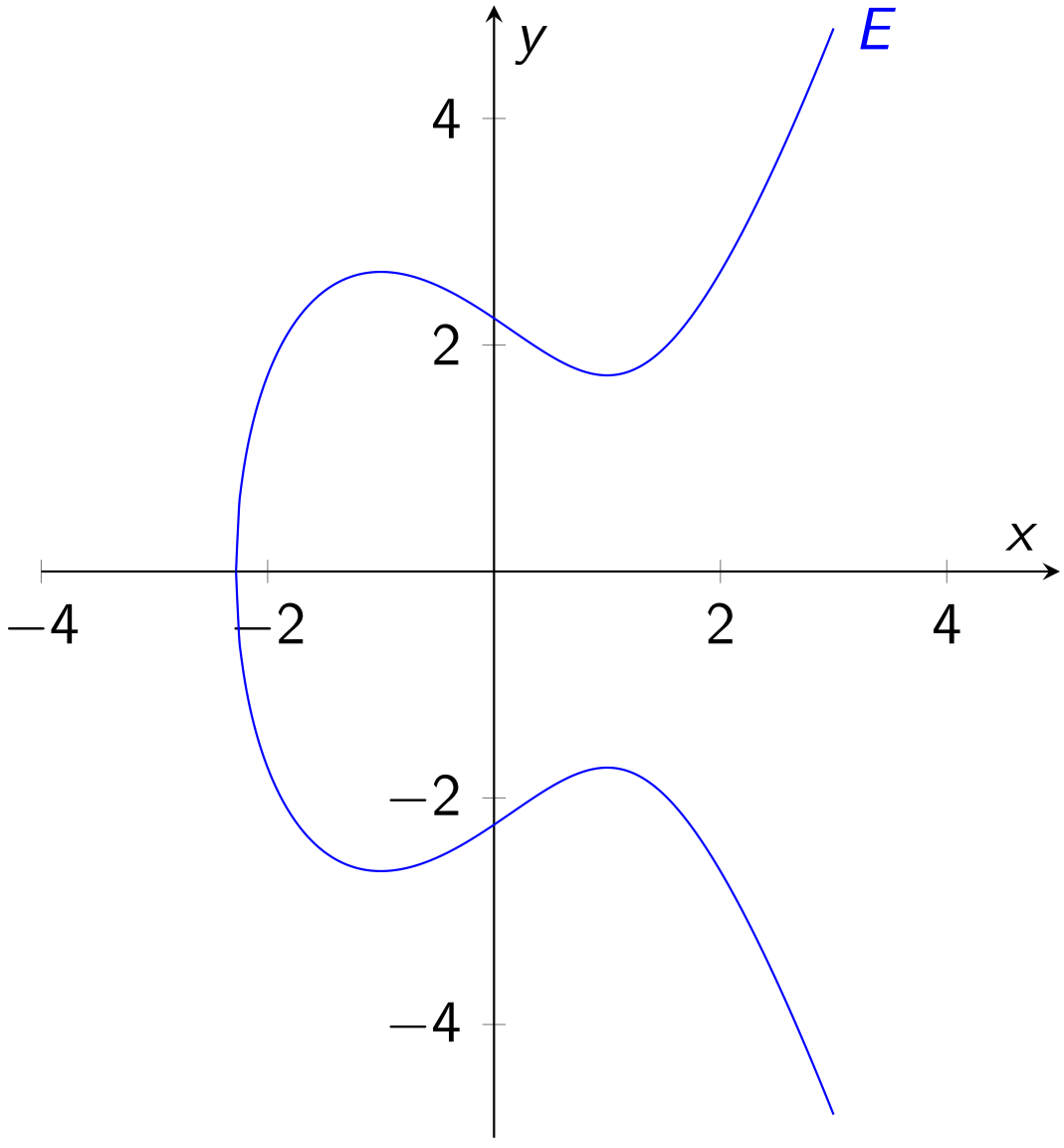


Figura 5: $y^2 = x^3 + 4x$. Puntos racionales: $(0, 0), (2, 4), (2, -4)$.

Estructura de grupo



Teorema de Mordell-Weil, 1922

El grupo de puntos racionales de una curva elíptica E definida sobre $\mathbb{Q}$ está finitamente generado y podemos escribirlo así:

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$$

Teorema. Mazur, 1977

El grupo de torsión $E(\mathbb{Q})_{\text{tors}}$ es isomorfo a uno de los siguiente 15 grupos:

- $\mathbb{Z}/N\mathbb{Z}$, para $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$, ó
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$, para $N = 2, 4, 6, 8$.

Además, todas estas posibilidades ocurren!

Conjetura

Existen curvas elípticas definidas sobre $\mathbb{Q}$ con rango arbitrariamente grande.

Curva elíptica de rango, al menos, 28 (Elkies, 2006):

$$y^2 + xy + y = x^3 - x^2$$

$$-20067762415575526585033208209338542750930230312178956502x$$

$$+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Problema de los números congruentes

Decimos que un número entero $n > 0$ es un número congruente si es el área de un triángulo rectángulo de lados racionales.
¿Podemos encontrar un algoritmo que determine si un número es congruente o no?

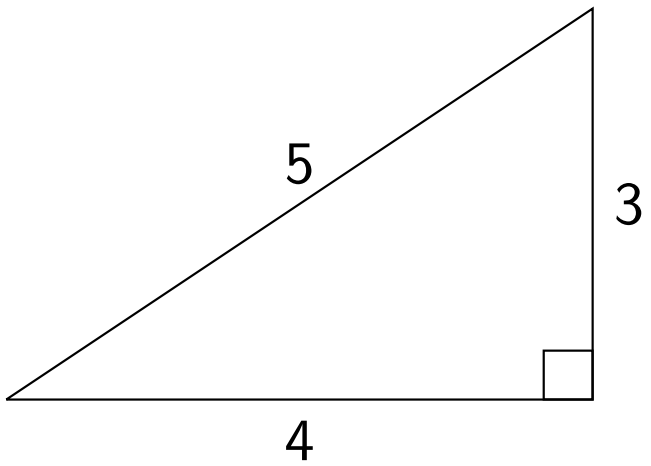


Figura 6: 6 es congruente

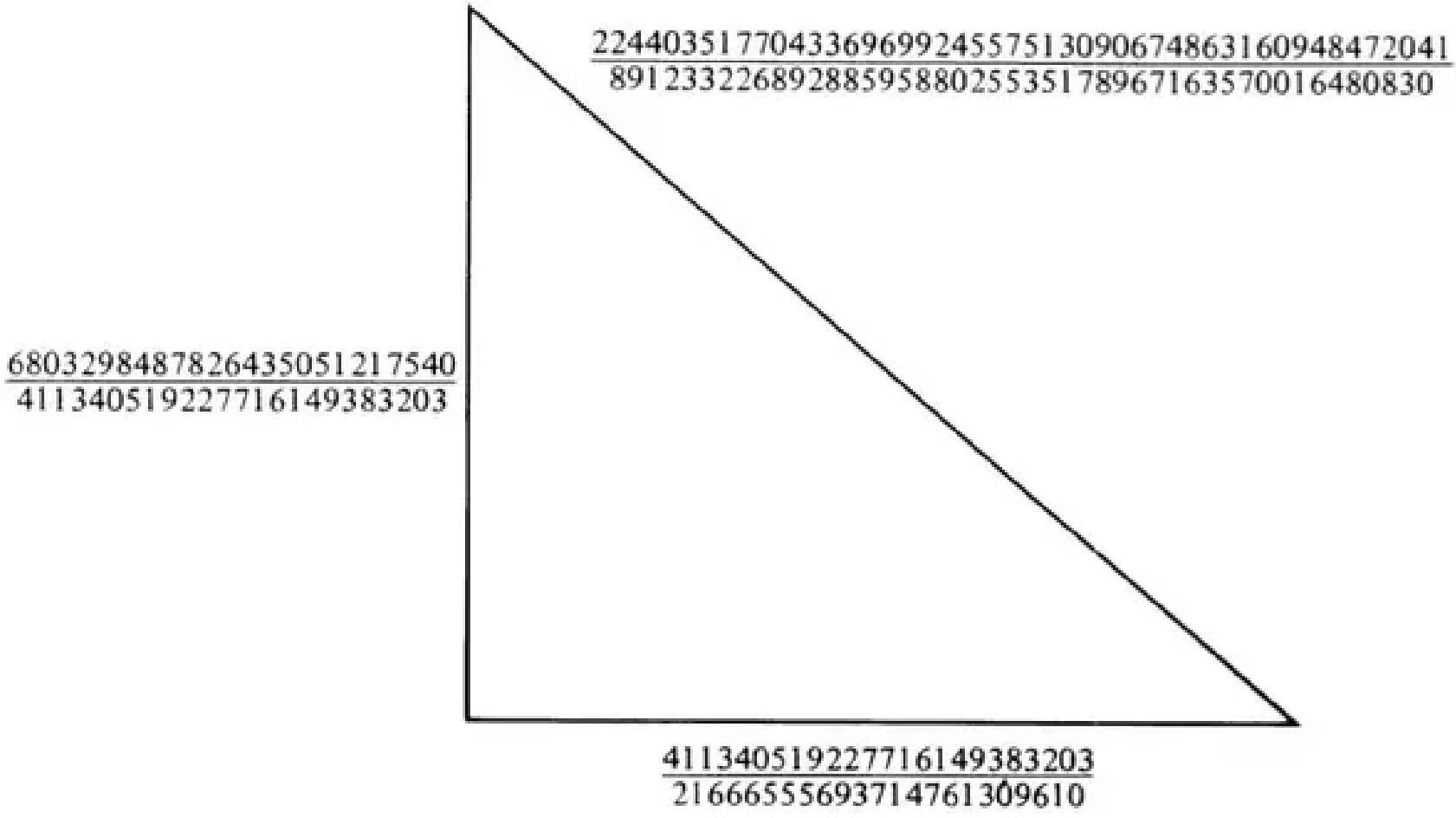


Figura 7: 157 es congruente!

Partimos de:

$$a^2 + b^2 = c^2, \quad \frac{ab}{2} = n$$

Haciendo el cambio de variable:

$$x = \frac{nb}{c-a}, \quad y = \frac{2n^2}{c-a}$$

obtenemos la siguiente ecuación:

$$y^2 = x^3 - n^2 x, \quad y \neq 0$$

Recíprocamente, podemos escribir:

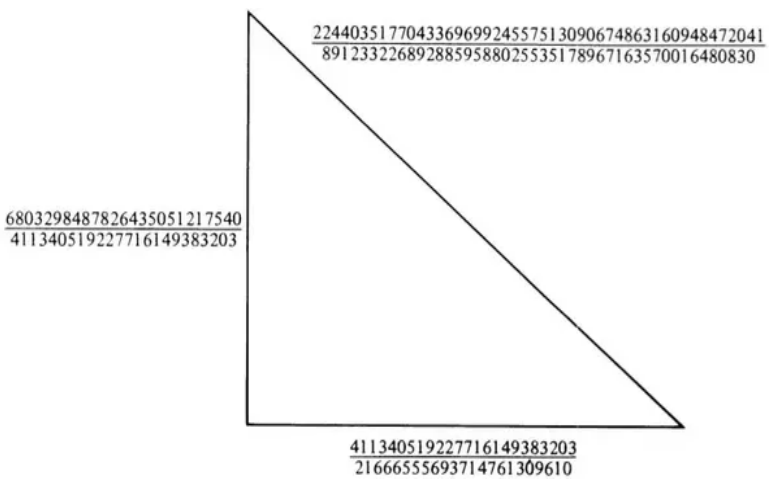
$$a = \frac{x^2 - n^2}{y}, \quad b = \frac{2nx}{y}, \quad c = \frac{x^2 + n^2}{y}$$

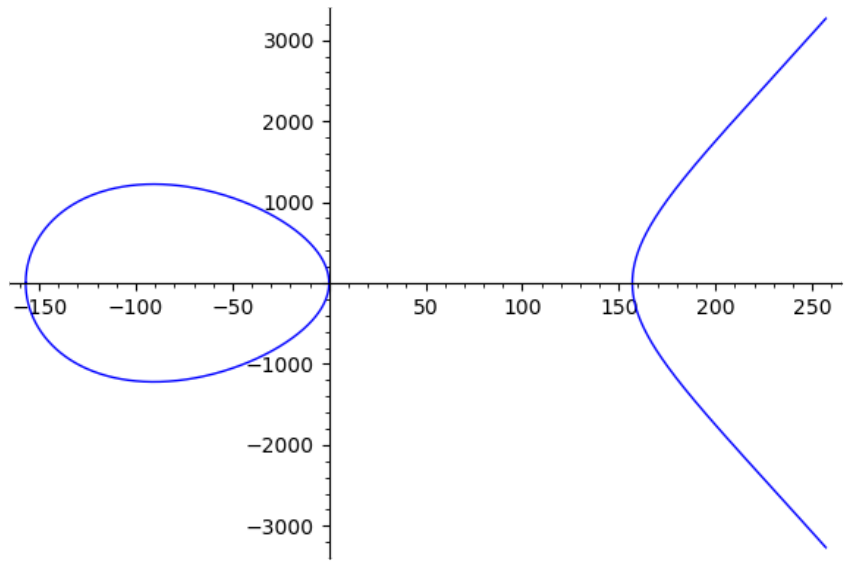
y podemos ver que a, b, c verifican las condiciones.

$$\{(a,b,c) : a^2 + b^2 = c^2, \frac{ab}{2} = n\} \leftrightarrow \{(x,y) : y^2 = x^3 - n^2 x, y \neq 0\}$$

$$(a,b,c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$$

$$\left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right) \mapsto (x,y)$$





Teorema de Tunnell, 1983

Sea $n > 0$ un entero libre de cuadrados. Definimos las siguentes cantidades:

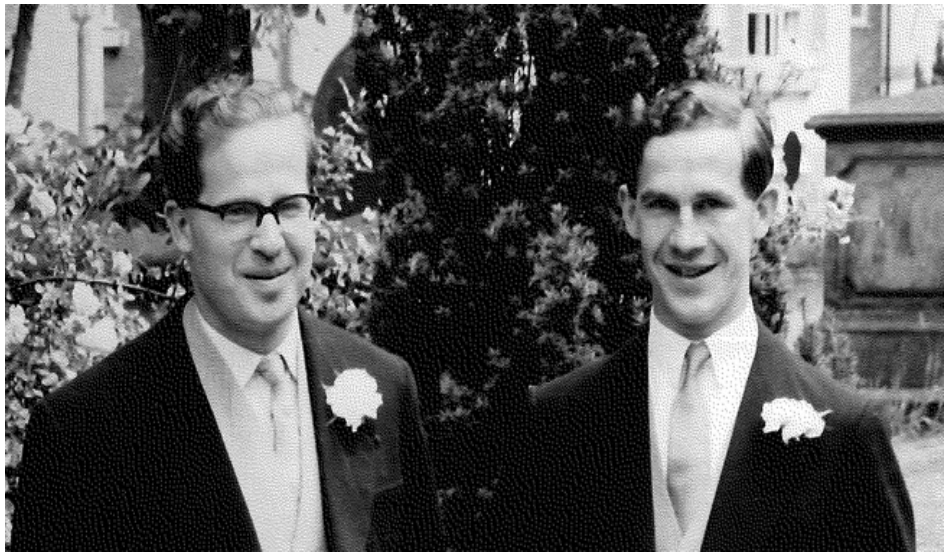
$$A_n = \#\{(x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\}$$
$$B_n = \#\{(x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\}$$
$$C_n = \#\{(x, y, z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 64z^2\}$$
$$D_n = \#\{(x, y, z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 16z^2\}$$

Supongamos que n es un número congruente. Entonces

- Si n es impar, $2A_n = B_n$.
- Si n es par, $2C_n = D_n$.

Recíprocamente, si la conjetura BSD es cierta para las curvas elípticas de la forma $y^2 = x^3 - n^2x$ entonces estas igualdades implican que n es congruente.

Conjetura de Birch y Swinnerton-Dyer



Sea E una curva elíptica definida sobre $\mathbb{Q}$ y sea $L(E,s)$ su función L. Entonces,

- $L(E,s)$ se anula en $s=1$, y el orden de anulación coincide con el rango (algebraico) R_E de la curva elíptica.
- El residuo de $L(E,s)$ en $s=1$ viene dado por:

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{R_E}} = \frac{|Ш|\cdot\Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E_{\mathrm{tors}}(\mathbb{Q})|^2}$$

Curvas elípticas en $\mathbb{F}_p$

Por ejemplo, sea la curva elíptica E definida sobre $\mathbb{Q}$:

$$E : y^2 = x^3 + x^2 - 2x + 9$$

¿Qué pasa si queremos considerarla sobre cuerpos finitos? En $\mathbb{F}_p$ para $p = 2, 3, 31$ deja de ser una curva elíptica!

- En $p = 2$ tiene mala reducción aditiva.
- En $p = 3, 31$ tiene mala reducción multiplicativa, y distinguimos dos casos:
  - Split en $p = 3$.
  - Non-split en $p = 31$.
- En el resto de primos p, tiene buena reducción.

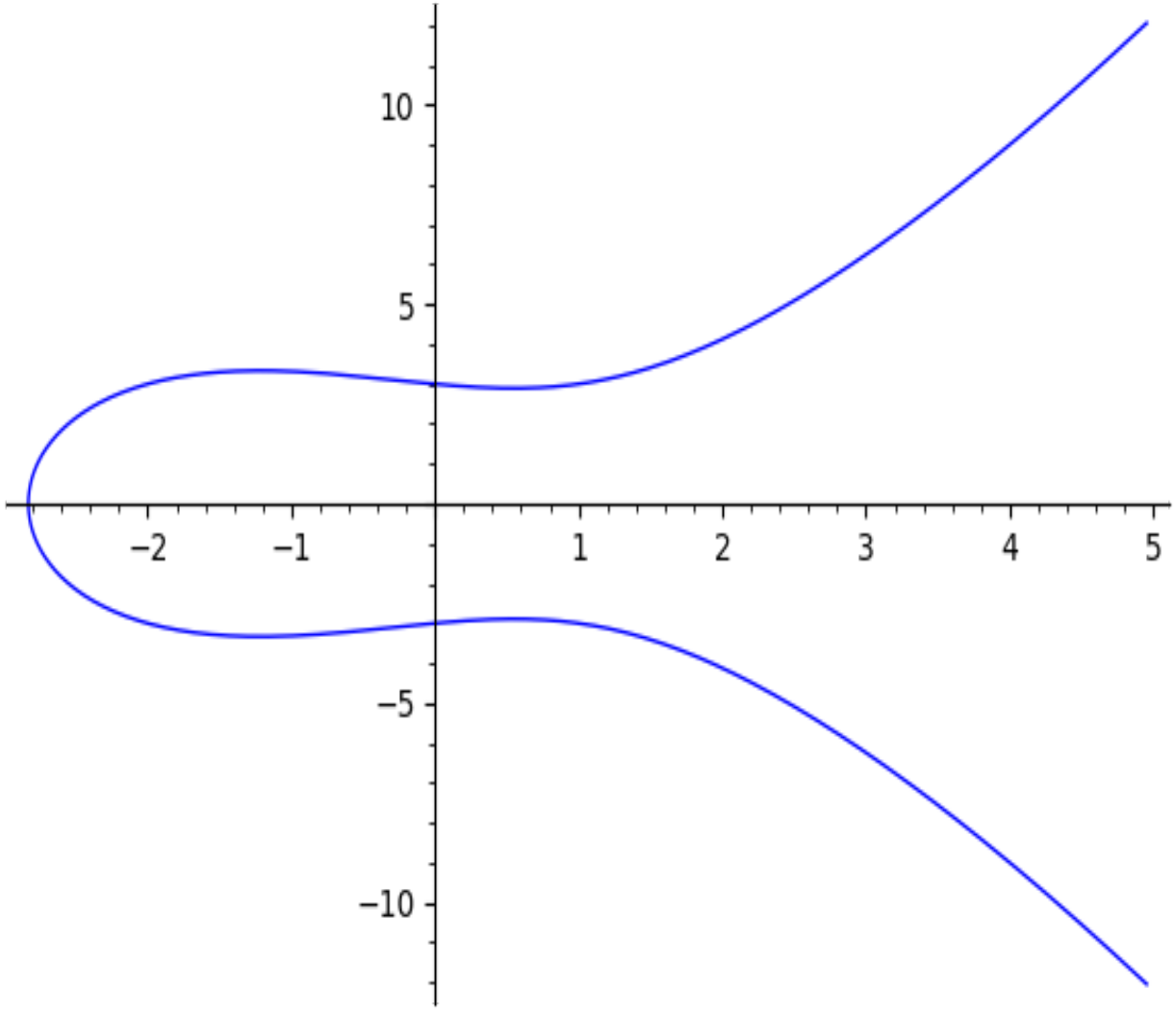


Figura 8: $y^2 = x^3 + x^2 - 2x + 9$ en $\mathbb{Q}$

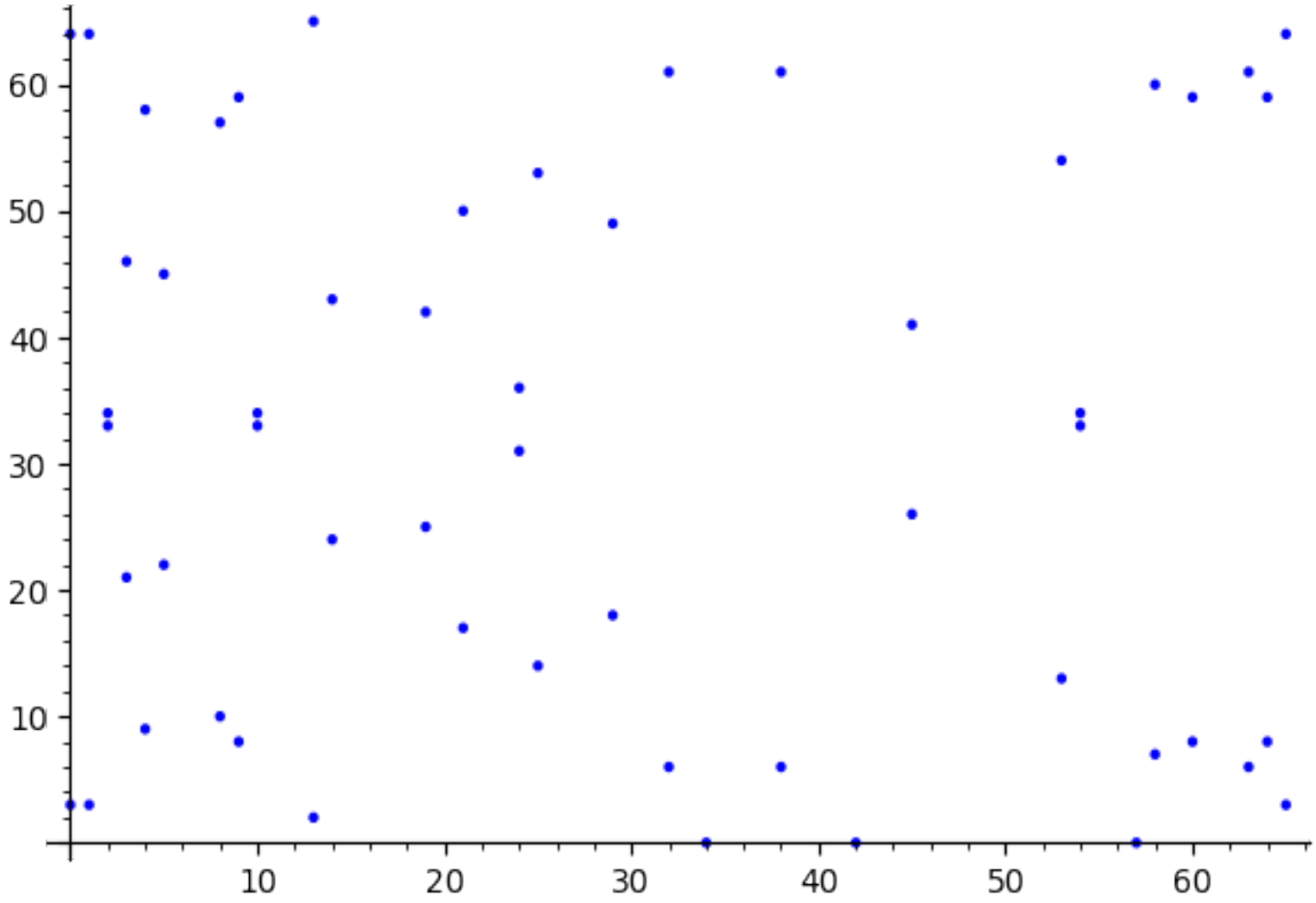


Figura 9: $y^2 = x^3 + x^2 - 2x + 9$ en $\mathbb{F}_{67}$

Funciones L

Función zeta de Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1 - p^{-s}}$$

Función L para una curva elíptica E sobre $\mathbb{Q}$:

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ primo}} \frac{1}{L_p(p^{-s})}$$

donde a_n son coeficientes de Fourier y $L_p(p^{-s})$ es un factor local que depende de la reducción de la curva elíptica módulo p. Ambas tienen continuación analítica a todo $\mathbb{C}$ y satisfacen una cierta ecuación funcional.

Último Teorema de Fermat

La ecuación $x^n + y^n = z^n$ no tiene solución entera con $xyz \neq 0$ para todo $n \geq 3$.

- Euler demostró el caso $n = 3$ en 1770.
- El propio Fermat demostró el caso $n = 4$.
- Dirichlet y Legendre demostraron el caso $n = 5$ de forma independiente, en 1825.
- Lamé demostró el caso $n = 7$ en 1839.

Por tanto, notemos que basta probarlo para todo $n = p$ primo mayor o igual que 11.

En 1984, Frey obtuvo una curva elíptica asumiendo que (a, b, c) era una solución, dada por

$$E : y^2 = x(x - a^p)(x + b^p)$$

y demostró ciertas propiedades de esta curva elíptica. En particular, demostró que es semiestable.

En 1986, Serre y Ribet demostraron que si esta curva existiera, no puede ser "modular".

Finalmente, en 1995, Wiles y Taylor demostraron:

"Toda curva elíptica semiestable definida sobre $\mathbb{Q}$ es modular."

Formas modulares

Sea $z \in \mathcal{H}$ donde $\mathcal{H}$ denota el plano superior complejo. Una forma modular f de peso k es una función compleja $f : \mathcal{H} \to \mathbb{C}$ verificando:

- f es una función holomorfa en $\mathcal{H}$,
- $|f(z)|$ permanece acotada cuando $\mathrm{im}(z) \to i\infty$.
- Condición de modularidad:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

para toda $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$.

Si además el límite es 0, decimos que f es una forma cúspide.

En particular, la condición de modularidad es equivalente a:

$$f(z+1) = f(z), \quad f(-1/z) = z^k f(z)$$

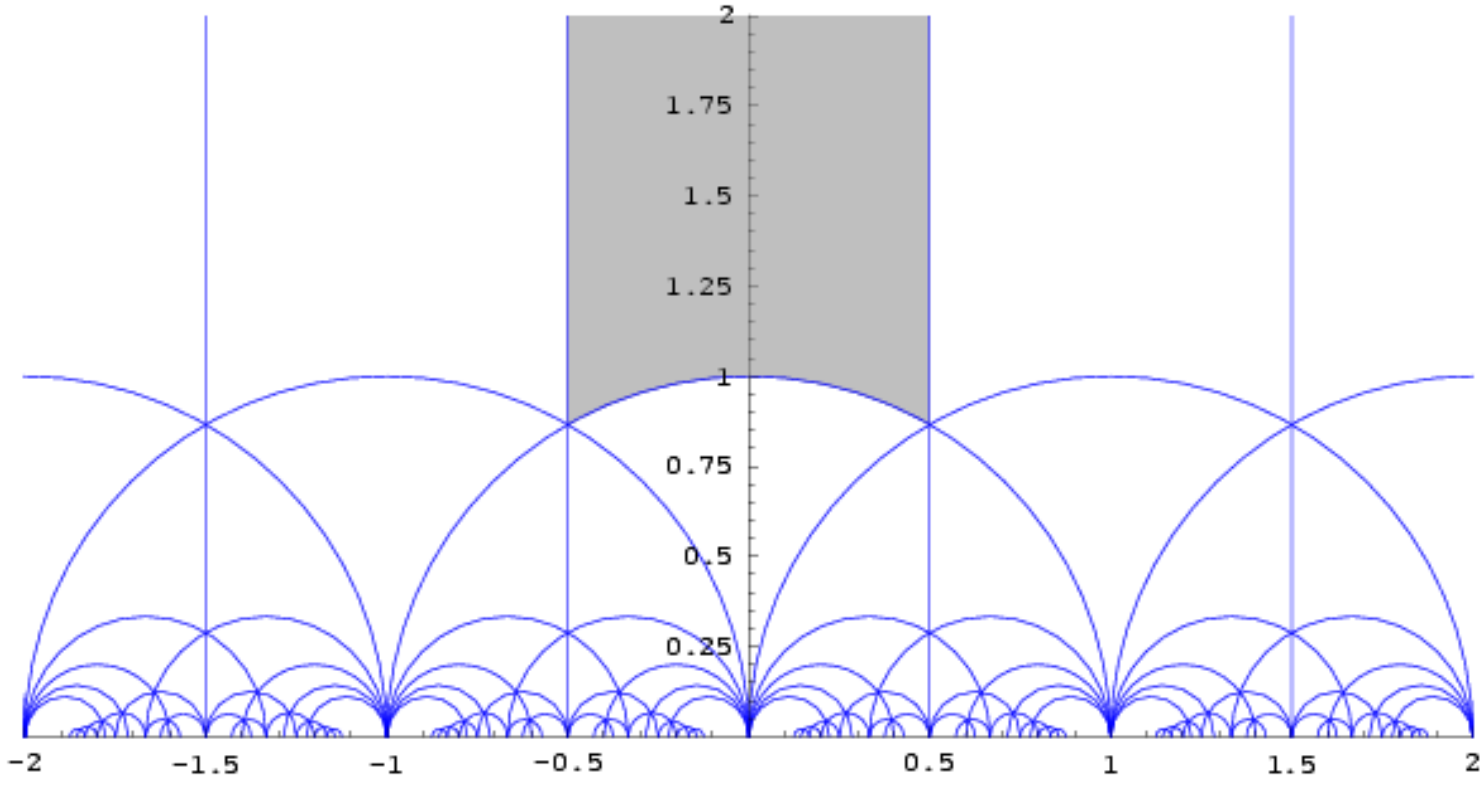


Figura 10: Dominio fundamental

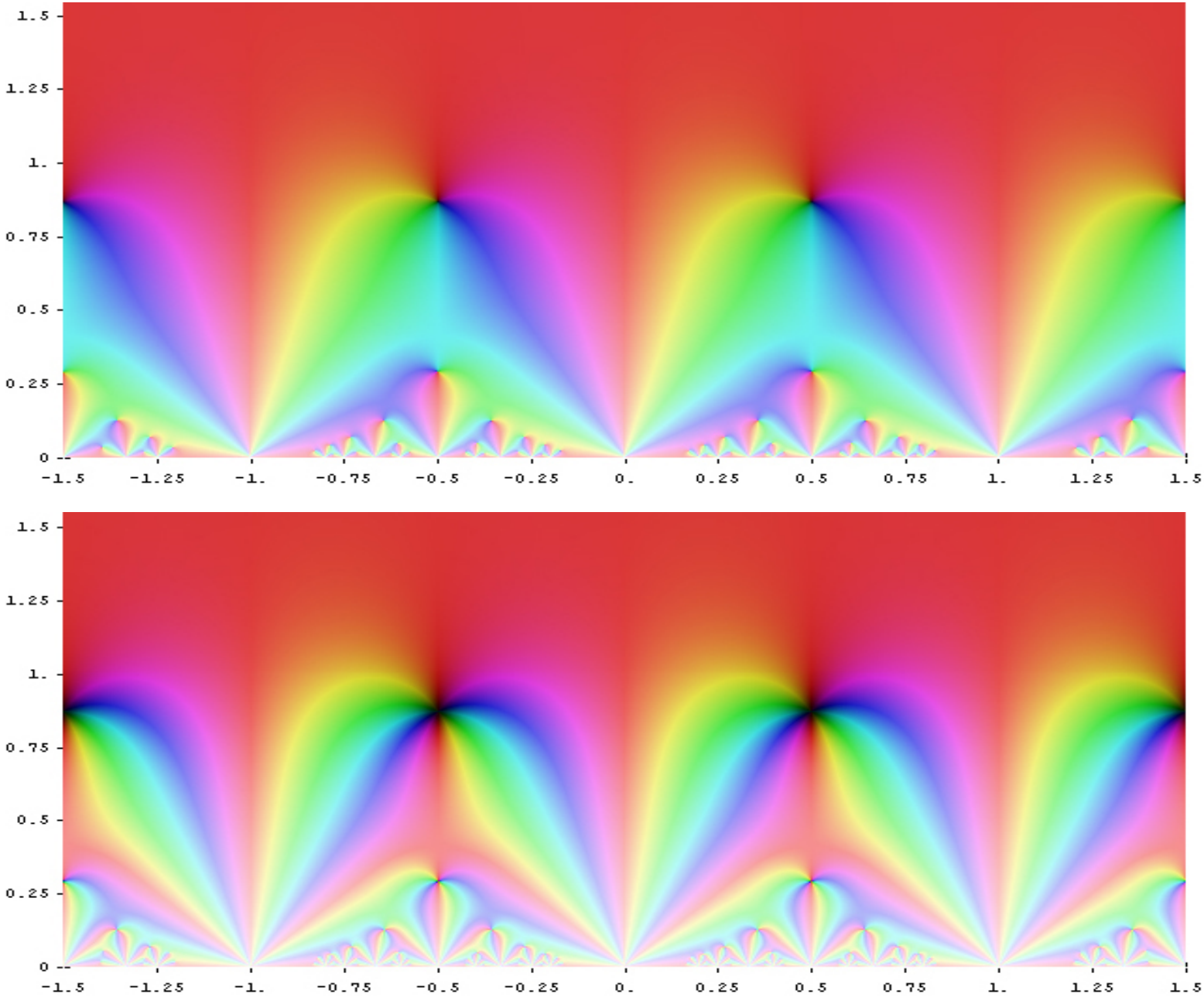


Figura 11: Series de Eisentein de peso 4 y 8

Sea $q = e^{2\pi iz}$. Podemos escribir las formas cúspides como expasión de Taylor:

$$f(z) = \sum_{n=1}^{\infty} a_n q^n = a_1 q + a_2 q^2 + \dots$$

y también podemos definir sus funciones L:

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Además, bajo ciertas condiciones, para formulas cúspide de peso k par también tenemos producto de Euler, continuación analítica a todo $\mathbb{C}$ y ecuación funcional!

Taniyama-Shimura-Weil

Una curva elíptica E definida sobre $\mathbb{Q}$ es modular si $L(E, s) = L(f, s)$ donde f es una forma modular.

Teorema de modularidad, 2001

Toda curva elíptica E definida sobre $\mathbb{Q}$ es modular.

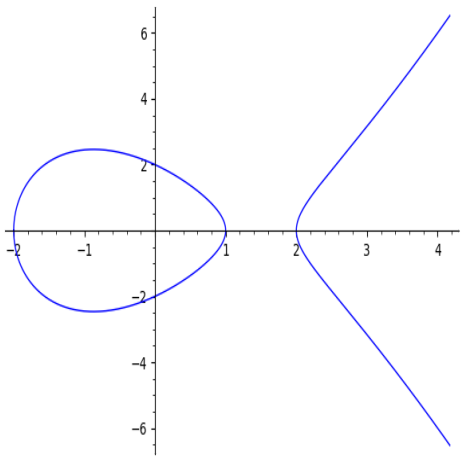
De hecho, toda curva elíptica E definida sobre $\mathbb{Q}$ se corresponde con una cierta forma cúspide de peso 2.

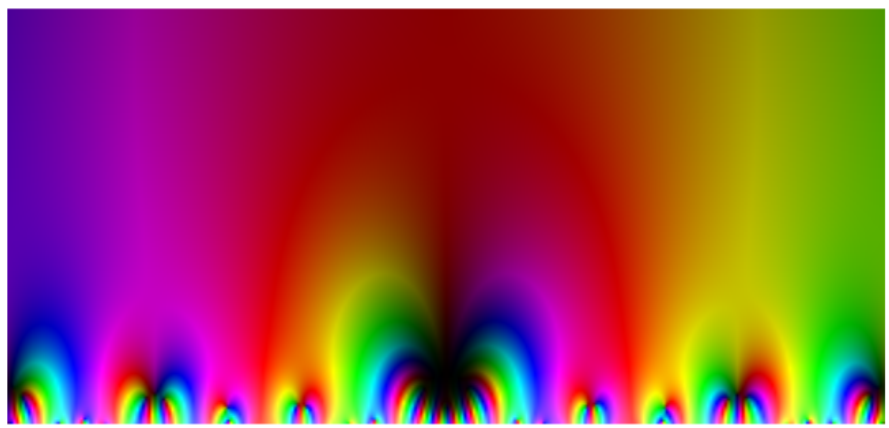
La curva elíptica E y la forma cúspide (de peso 2) $f(q)$

$$E : y^2 = x^3 - x^2 - 4x + 4, \quad f(q) = q - q^3 - 2q^5 + q^9 + O(q^{10})$$

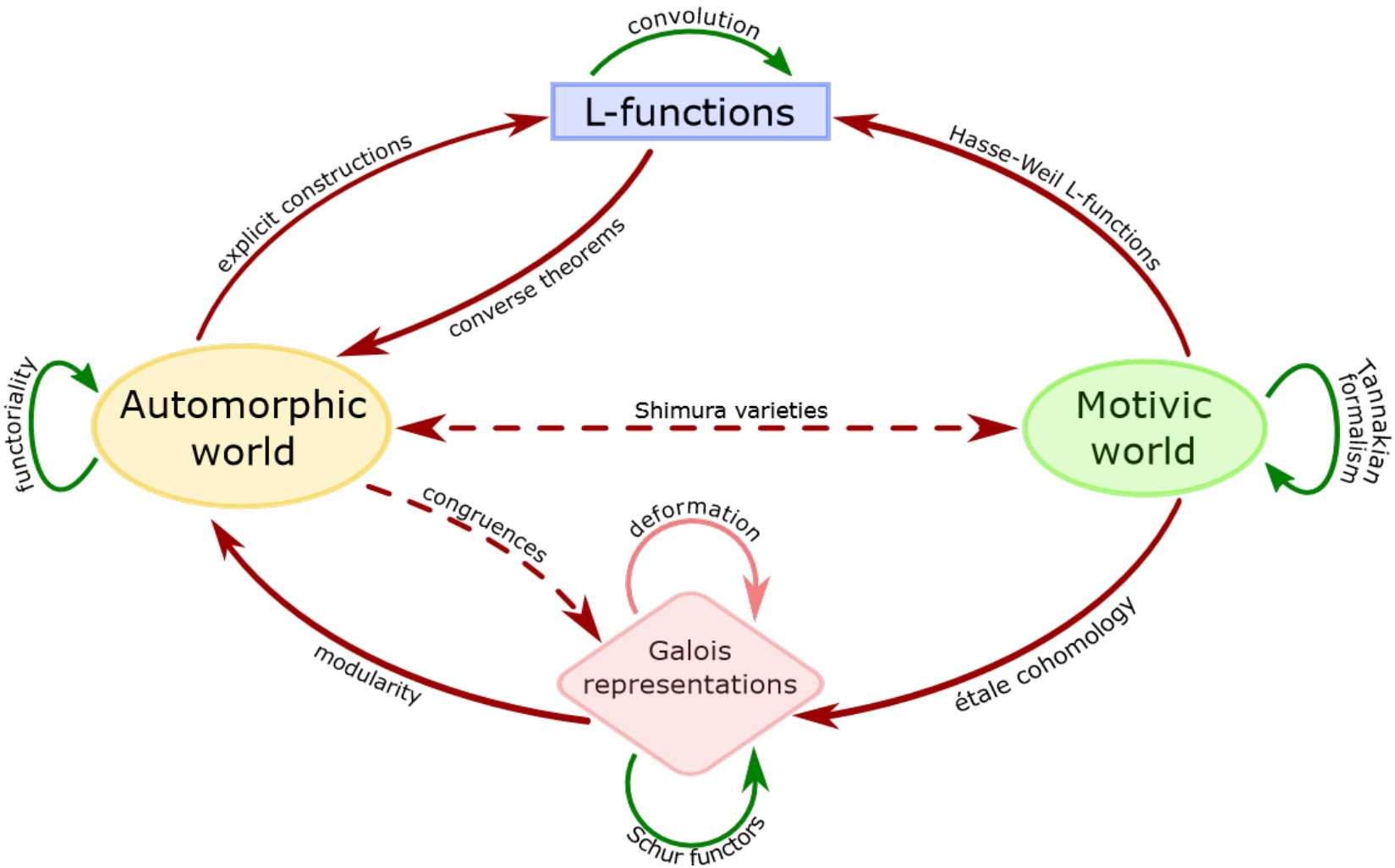
tienen la siguente función L:

$$L(E, s) = 1 - \frac{1}{3^s} - \frac{2}{5^s} + \frac{1}{9^s} + \frac{4}{11^s} - \frac{2}{13^s} + \dots$$





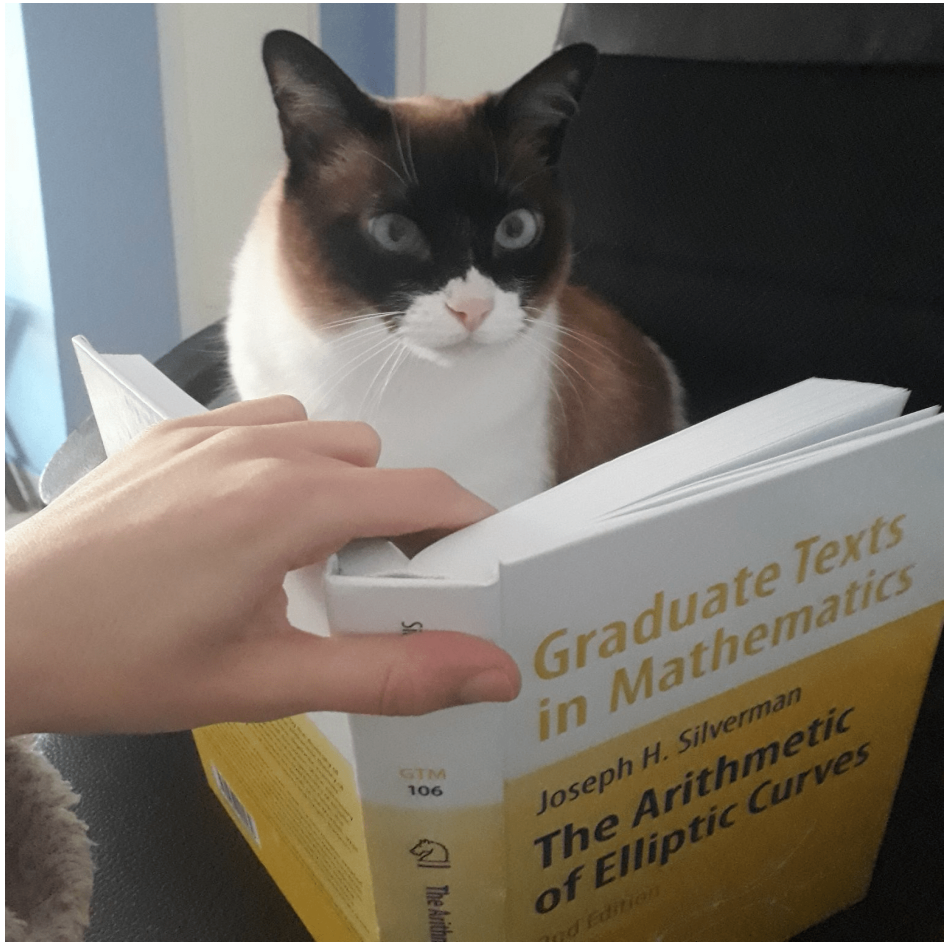
Universo de LMFDB



Referencias

- Elliptic Curves, Modular Forms and Their L-functions - Álvaro Lozano-Robledo
- Elliptic Tales - Avner Ash and Robert Gross
- Introduction to Elliptic Curves and Modular Forms - Neal Koblitz
- LMFDB - The L-functions and Modular Forms Database
- The Arithmetic of Elliptic Curves - Joseph H. Silverman

... y Salem!



¡Muchísimas gracias!