A trip through elliptic curves and Fermat's Last Theorem

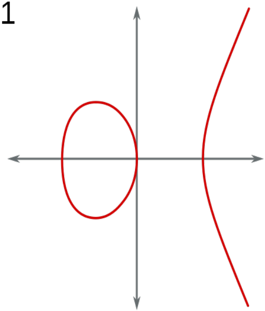
Marta Sánchez Pavón

Facultad de Matemáticas US

17th March 2021

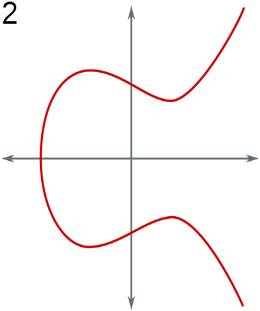
Elliptic curves

1



$y^2 = x^3 - x$

2

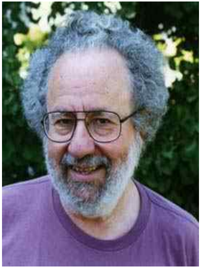
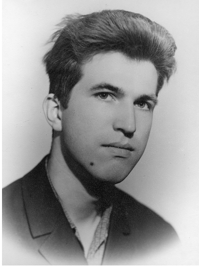
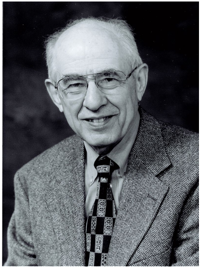
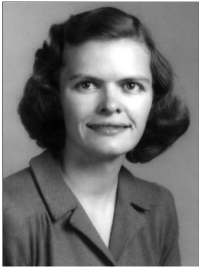


$y^2 = x^3 - x + 1$

Hilbert's tenth problem, 1900

Let $f(x_1, \ldots, x_n) = 0$ be a polynomial equation with coefficients in $\mathbb{Z}$. Can we find an algorithm that determines if this equation has integer solutions?

Martin Davis, Yuri Matiyasevich, Hilary Putnam and Julia Robinson proved that such an algorithm does not exist. (1970)

Plimpton 332

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

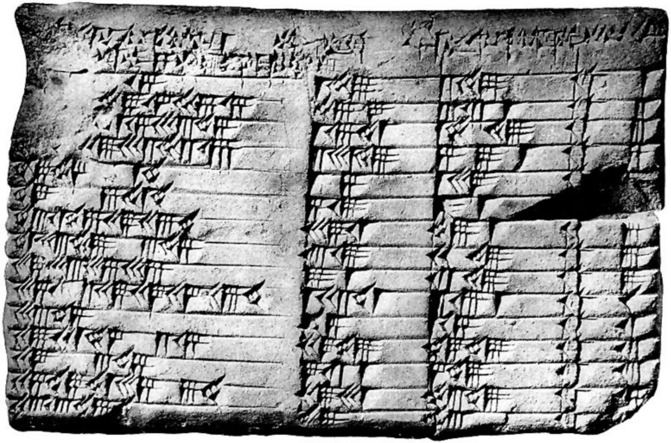


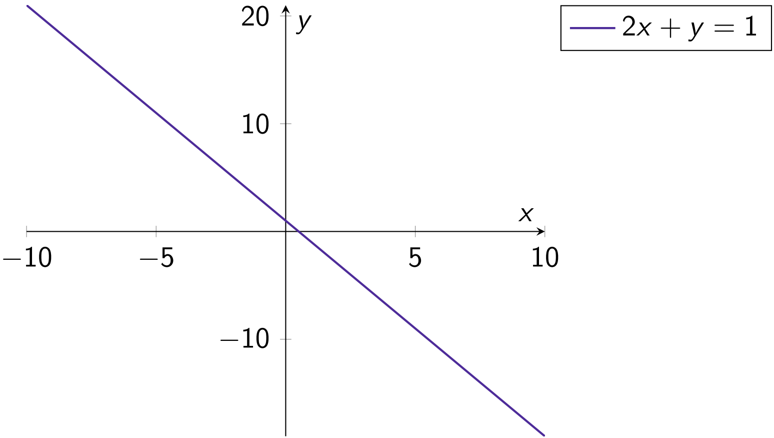
Figure 1: Plimpton 332

Degree 1

$$ax + by = c$$

The equation has integer solutions if and only if the greatest common divisor of a and b, $\gcd(a, b)$, divides the integer c.

Example: $2x + y = 1$. Since $\gcd(2, 1) = 1$ divides 1, the equation has infinite solutions: $x = \lambda$, $y = 1 - 2\lambda$.


20
10
−10
y
x
−10
−5
5
10
2x + y = 1

Degree 2

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

Hasse-Minkowski theorem

A quadratic form has a solution in $\mathbb{Q}$ if and only if it has a solution over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p.

For example, genus 0 curves C have either infinite rational points or none.

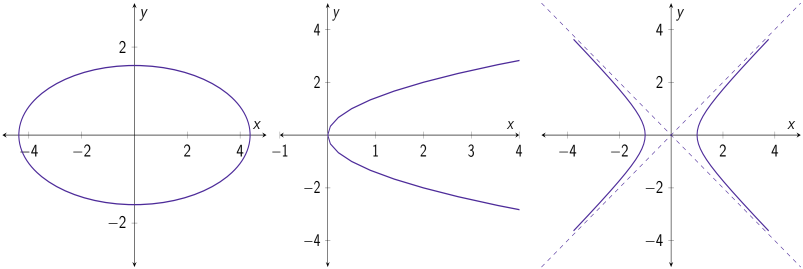


Figure 2: Ellipse, parabola, hyperbola

Degree 3

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

Counterexamples!!

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

For example, genus 1 curves C have either infinitely-many rational points, or finitely-many, or none.

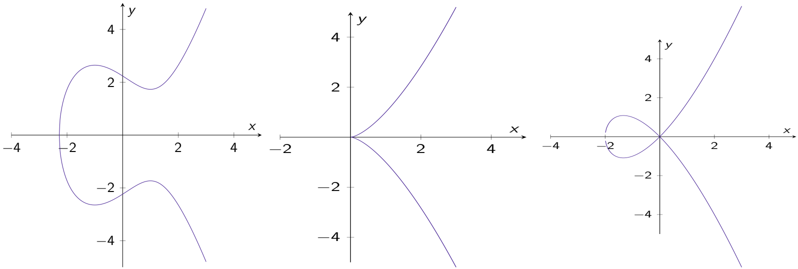


Figure 3: Smooth curve, cusp, node

Degree $n > 3$

Faltings' theorem, 1983

Let C be a curve of genus $n > 1$. Then the set of rational points $C(\mathbb{Q})$ is finite.

Summarizing, depending on the genus, the set of rational points can be...

Genus 0	Genus 1	Genus >1
$\emptyset$	$\emptyset$	$\emptyset$
-	Finite	Finite
Infinite	Infinite	-

Elliptic curve

An elliptic curve E defined over a field K is an algebraic curve such that:

- it is smooth,
- it is projective,
- it has genus 1,
- there is a marked point on E, denoted $\mathcal{O}$.

We can write them in Weierstrass form:

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

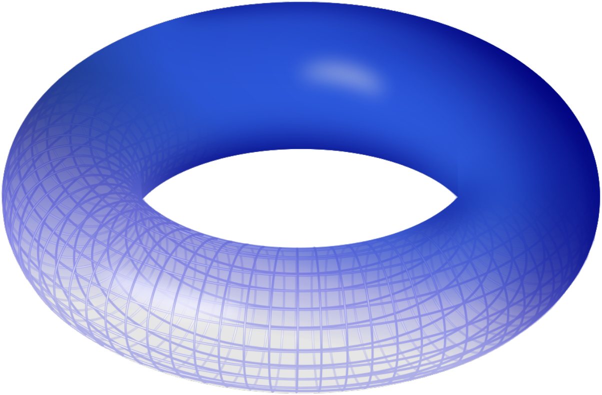


Figure 4: Complex torus... and elliptic curve!

If E is defined over a field K of characteristic different from 2 and 3, we can write E in short Weierstrass form:

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

Goal: understanding rational points on elliptic curves!

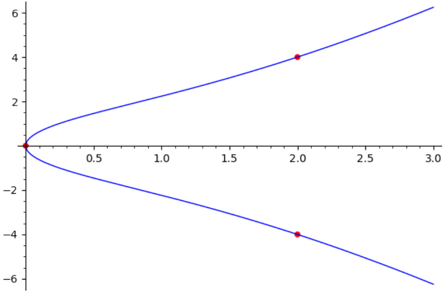
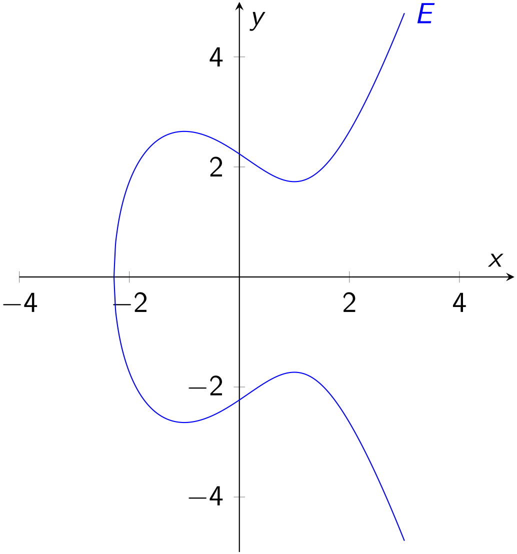


Figure 5: $y^2 = x^3 + 4x$. Rational points: $(0, 0), (2, 4), (2, -4)$.

Group structure



Mordell-Weil theorem, 1922

The group of rational points $E(\mathbb{Q})$ of an elliptic curve E defined over $\mathbb{Q}$ is a finitely generated abelian group and we can write it as follows:

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

Theorem. Mazur, 1977

The torsion group $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of the following 15 groups:

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

Moreover, all these possibilities happen!

Conjecture

There exists elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.

Elliptic curve of rank, at least, 28 (Elkies, 2006):

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

$$-20067762415575526585033208209338542750930230312178956502x$$

$$+34481611795030556467032985690390720374855944359319180361266008296291939448732243429$$

Congruent number problem

We say that an integer $n > 0$ is a congruent number if it is the area of a right triangle whose sides are rational numbers.

Can we find an algorithm that determines if a number is congruent or not?

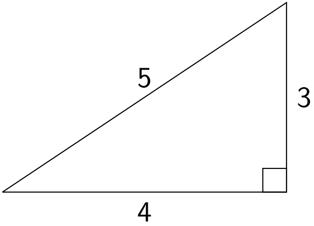


Figure 6: 6 is congruent

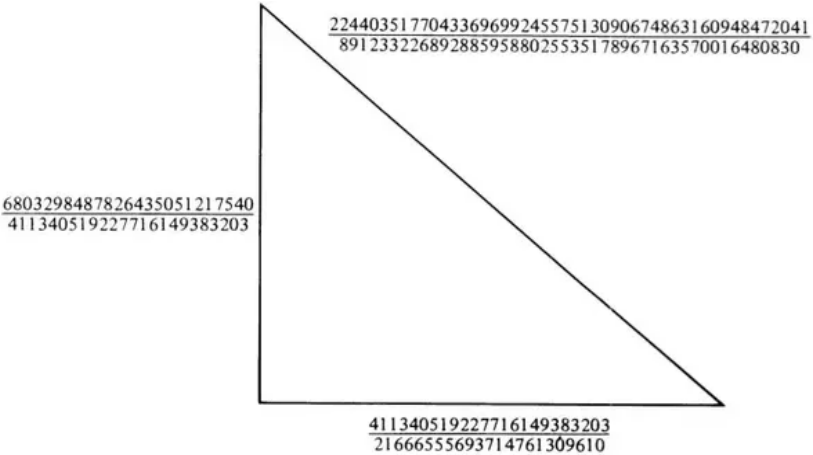

$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$
$\frac{6803298487826435051217540}{411340519227716149383203}$
$\frac{411340519227716149383203}{21666555693714761309610}$

Figure 7: 157 is congruent!

We start from:

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

Set the following change of variables:

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

and we obtain this equation:

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

Conversely, we can set:

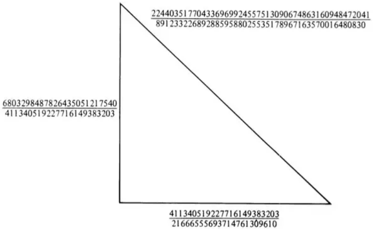
$$a = \frac{x^2 - n^2}{y}, \quad b = \frac{2nx}{y}, \quad c = \frac{x^2 + n^2}{y}$$

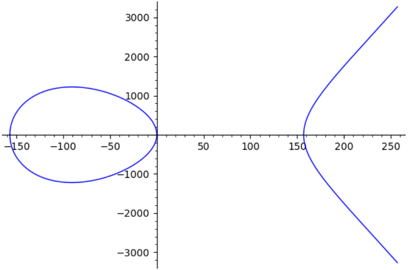
and we can check these a, b, c verify the conditions.

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

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

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


$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$
$\frac{6803298487826435051217540}{411340519227716149383203}$
$\frac{411340519227716149383203}{21666555693714761309610}$



Tunnell's theorem, 1983

Let $n > 0$ square-free integer. We define the following quantities:

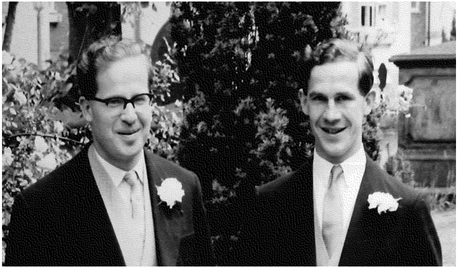
$$
\begin{aligned}
A_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\} \\
B_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\} \\
C_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 64z^2\} \\
D_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 16z^2\}
\end{aligned}
$$

Suppose n is congruent. Then

- If n is odd, $2A_n = B_n$.
- Si n is even, $2C_n = D_n$.

Conversely, if the BSD conjecture is true for elliptic curves of the form $y^2 = x^3 - n^2x$ then this quantities would imply that n is congruent.

Birch and Swinnerton-Dyer conjecture



Let E be an elliptic curve defined over $\mathbb{Q}$, let $L(E, s)$ be its L-function. Then,

- $L(E, s)$ has a zero at $s = 1$, and the order of vanishing is the (algebraic) rank R_E of E.
- The residue of $L(E, s)$ at $s = 1$ is given by:

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

Elliptic curves over $\mathbb{F}_p$

For example, let $E/\mathbb{Q}$ be the elliptic curve:

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

What happens if we want to consider it over finite fields $\mathbb{F}_p$? For $p = 2, 3, 31$ it is no longer an elliptic curve!

- In $p = 2$ it has bad additive reduction.
- In $p = 3, 31$ it has bad multiplicative reduction, and we distinguish two cases:
  - Split in $p = 3$.
  - Non-split in $p = 31$.
- In the rest of primes p, it has good reduction.

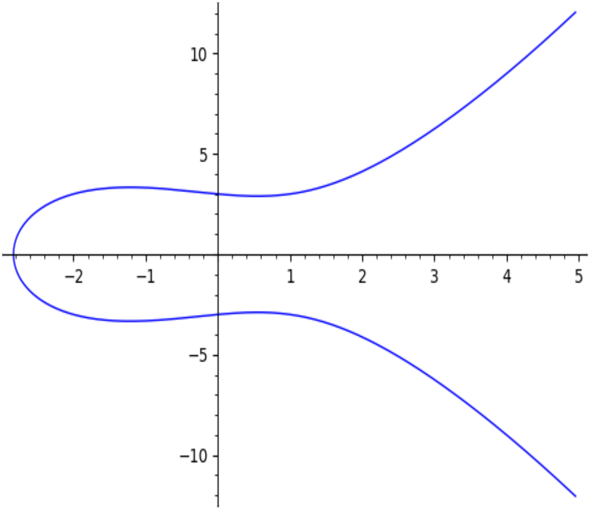


Figure 8: $y^2 = x^3 + x^2 - 2x + 9$ en $\mathbb{Q}$

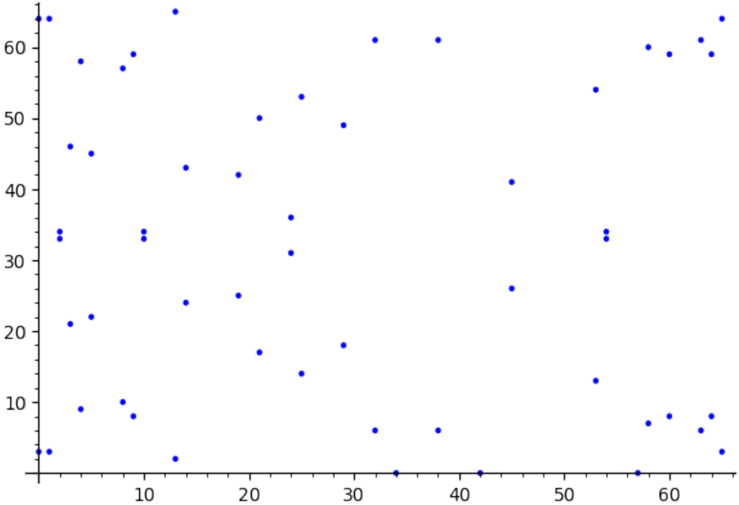


Figure 9: $y^2 = x^3 + x^2 - 2x + 9$ en $\mathbb{F}_{67}$

L-functions

Riemann zeta function:

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

L-function for an elliptic curve $E/\mathbb{Q}$:

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

where a_n are the Fourier coefficients and $L_p(p^{-s})$ is a local factor that depends on the kind of reduction of E modulo p. Both of these functions have analytic continuation to the whole complex plane and satisfy a certain functional equation.

Fermat's Last Theorem

The equation $x^n + y^n = z^n$ has no integer solutions with $xyz \neq 0$ for all $n \geq 3$.

- Euler proved the case $n = 3$ in 1770.
- Fermat himself proved the case $n = 4$.
- Independently, Dirichlet and Legendre proved the case $n = 5$, around 1825.
- Lamé proved the case $n = 7$ in 1839.

Therefore, note that it suffices to prove it for $n = p$ prime greater than 7.

In 1984, Frey obtained the following elliptic curve assuming that there exists a solution (a, b, c):

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

and he proved certain properties of this curve. In particular, he proved that it is semiestable.

In 1986, Serre y Ribet proved that if such curve exists, it can not be "modular".

Finally, in 1995, Wiles and Taylor proved:

"Every semiestable elliptic curve defined over $\mathbb{Q}$ is modular."

Modular forms

Let $z \in \mathcal{H}$ where $\mathcal{H}$ denotes the upper half plane. A modular form f of weight k is a complex function $f : \mathcal{H} \to \mathbb{C}$ satisfying:

- f is an holomorphic function on $\mathcal{H}$,
- $|f(z)|$ stays bounded as $\mathrm{im}(z) \to i\infty$.
- Modularity condition:

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

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

Further, if the limit is zero, we say that f is a cusp form.

In particular, the modularity condition is equivalent to:

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

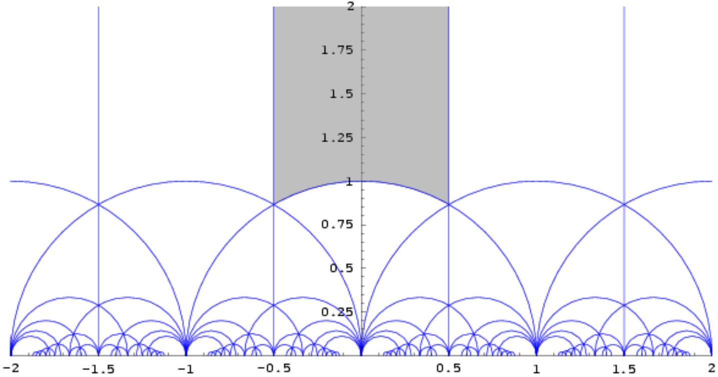


Figure 10: Fundamental domain

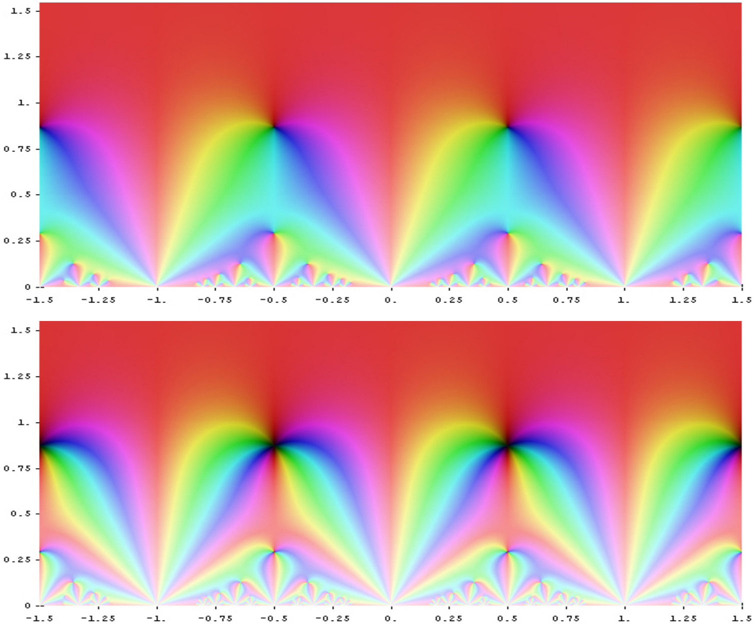


Figure 11: Eisenstein series of weight 4 and 8.

Let $q = e^{2\pi i z}$. We can write cusps form as Taylor expansions:

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

and we can also define its L-function:

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

Further, under certain conditions, we can have an Euler product, analytic continuation to the whole complex plane and functional equation for cusp forms of even weight!

Taniyama-Shimura-Weil conjecture

An elliptic curve E defined over $\mathbb{Q}$ is modular if $L(E,s) = L(f,s)$ where f is a modular form.

Modularity theorem, 2001

Every elliptic curve E defined over $\mathbb{Q}$ is modular.

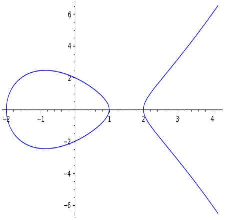
In fact, every elliptic curve E defined over $\mathbb{Q}$ corresponds to a cusp form of weight 2.

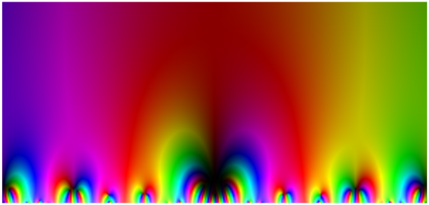
The elliptic curve E and the cusp form (of weight 2) $f(q)$

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

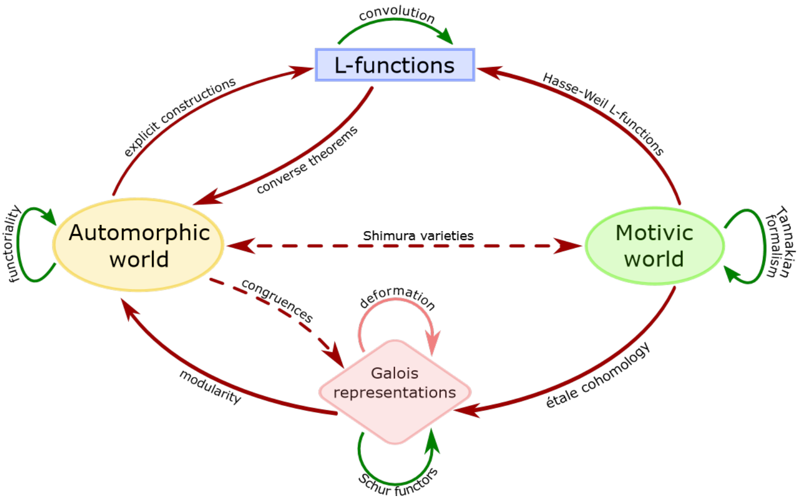
share the following L-function:

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





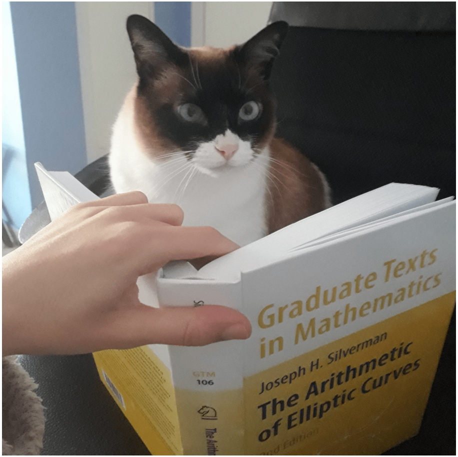
LMFDB universe



References

- 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

… and Salem!


Graduate Texts in Mathematics
Joseph H. Silverman
The Arithmetic of Elliptic Curves
2nd Edition
GTM 106

Thank you so much!