Elliptic curves and modularity

Ana Caraiani

University of Bonn / Imperial College London

April 2023

Perfect squares and quadratic residues

Question

What are the last digits of perfect squares?

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225...

Perfect squares and quadratic residues

Question

What are the last digits of perfect squares?

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225...

Harder question

Let $\ell \geq 5$ be a prime number. Can 3 be the last digit of a perfect square in base ℓ? When does the polynomial

$$x^2 - 3$$

split into two distinct linear factors modulo ℓ?

The law of quadratic reciprocity

Let p and ℓ be distinct odd primes. The law of quadratic reciprocity relates whether

- p is a quadratic residue modulo ℓ

to whether

- ℓ is a quadratic residue modulo p.

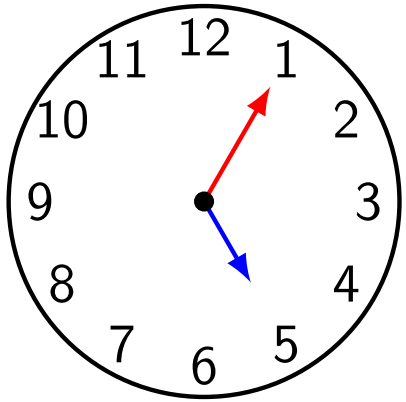
$$\left(\frac{p}{\ell}\right) \cdot \left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{\ell-1}{2}}$$

It was conjectured by Euler and Legendre and first proved by Gauss in 1796.

The law of quadratic reciprocity

Consequence: whether 3 can be the last digit of a perfect square in base ℓ only depends on ℓ modulo $3 \cdot 4 = 12$.

- For ℓ equal to 13, 37, 61 and 1093, the answer is "Yes".
- For ℓ equal to 17, 29, 41 and 1637, the answer is "No".



What is the most general reciprocity law?

Higher-dimensional reciprocity

The infinite product

$$f(q) := q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2$$

$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + \dots$$

and the Diophantine equation

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

seem to know about each other in a mysterious way.

Higher-dimensional reciprocity

- The coefficient a_ℓ of q^ℓ in the expansion of $f(q)$ takes the values:

ℓ	2	3	5	7	13	17	19	23	29
a_ℓ	-2	-1	1	-2	4	-2	0	-1	0

- The number N_ℓ of solutions to $y^2 + y \equiv x^3 - x^2 \pmod{\ell}$ takes the values:

ℓ	2	3	5	7	13	17	19	23	29
N_ℓ	4	4	4	9	9	19	19	24	29

Higher-dimensional reciprocity

- The coefficient a_ℓ of q^ℓ in the expansion of $f(q)$ takes the values:

ℓ	2	3	5	7	13	17	19	23	29
a_ℓ	-2	-1	1	-2	4	-2	0	-1	0

- The number N_ℓ of solutions to $y^2 + y \equiv x^3 - x^2 \pmod{\ell}$ takes the values:

ℓ	2	3	5	7	13	17	19	23	29
N_ℓ	4	4	4	9	9	19	19	24	29

- We always seem to have $a_\ell = \ell - N_\ell$.

Higher-dimensional reciprocity laws

- The power series $f(q)$ is the Fourier expansion of a modular form.
- The Diophantine equation E represents an elliptic curve over $\mathbb{Q}$.

The reciprocity law

$$a_\ell = \ell - N_\ell$$

is a consequence of the *modularity of elliptic curves* over $\mathbb{Q}$.

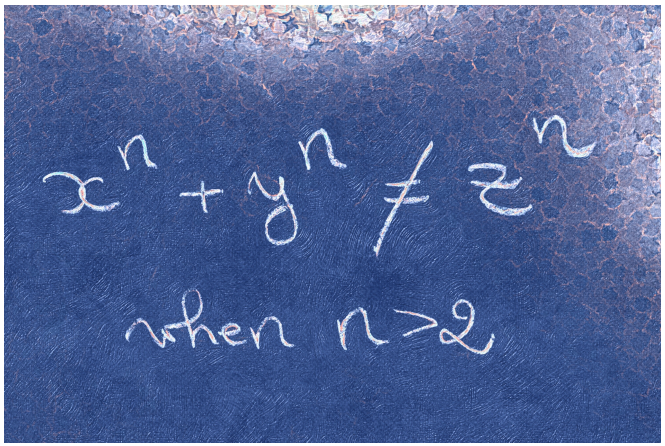
Higher-dimensional reciprocity laws

- The power series $f(q)$ is the Fourier expansion of a modular form.
- The Diophantine equation E represents an elliptic curve over $\mathbb{Q}$.

The reciprocity law

$$a_\ell = \ell - N_\ell$$

is a consequence of the *modularity of elliptic curves* over $\mathbb{Q}$.



Elliptic curves

An elliptic curve $E/\mathbb{Q}$ is a smooth projective curve of genus 1 together with a specified rational point.

Its torsion points $E[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$ have an action of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

As n varies, these assemble into a Galois representation

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_p).$$

More generally, the étale cohomology of algebraic varieties defined over $\mathbb{Q}$ is a source of representations of $G_{\mathbb{Q}}$.

Modular forms

A modular form is a holomorphic function on the upper-half plane

$$\mathbb{H}^2 = \{z \in \mathbb{C} \mid \mathrm{Im}\ z > 0\}$$

that satisfies many symmetries and a growth condition.

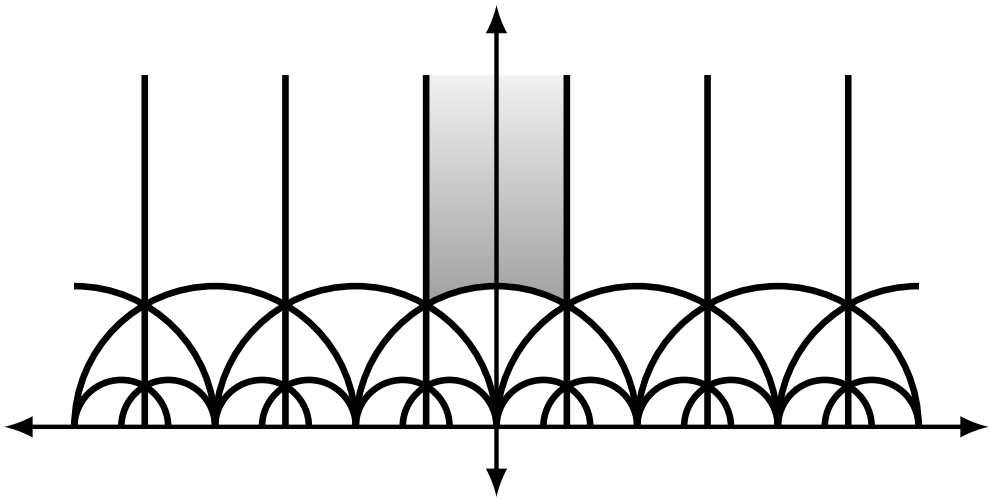
There is a transitive action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}^2$:

$$z \mapsto \frac{az+b}{cz+d} \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

This gives the identification of $\mathbb{H}^2$ with the symmetric space for the group SL_2.

Modular curves

Modular curves are quotients $\Gamma\backslash\mathbb{H}^2$, where $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup.



The quotients $\Gamma\backslash\mathbb{H}^2$ arise from algebraic curves defined over number fields. Their étale cohomology is a source of Galois representations

$$f \mapsto \rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_p).$$

Modularity

We say that an elliptic curve $E/\mathbb{Q}$ is *modular* if there exists a modular form f together with an isomorphism of Galois representations

$$\rho_f \simeq \rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_p)$$

This implies the explicit reciprocity law $a_\ell = \ell - N_\ell$ by taking traces at distinguished conjugacy classes $\{\mathrm{Frob}_\ell\} \in G_{\mathbb{Q}}$.

Theorem 1 (Wiles, Taylor–Wiles 1995, Breuil–Conrad–Diamond–Taylor 2001)

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

Modularity

Theorem 2 (Freitas–Le Hung–Siksek 2013)

Let F be a real quadratic field. Every elliptic curve E/F is modular.

This relies on improvements to the Taylor–Wiles method, particularly due to Kisin, and on a sophisticated analysis of quadratic points on modular curves.

Modularity

Theorem 2 (Freitas–Le Hung–Siksek 2013)

Let F be a real quadratic field. Every elliptic curve E/F is modular.

This relies on improvements to the Taylor–Wiles method, particularly due to Kisin, and on a sophisticated analysis of quadratic points on modular curves.

Theorem 3 (C–Newton 2023)

Every elliptic curve $E/\mathbb{Q}(i)$ is modular.

This relies on work of Calegari–Geraghty, Scholze, Allen–Khare–Thorne and many others.

Arithmetic hyperbolic 3-manifolds

The symmetric space for $\mathrm{SL}_2/\mathbb{Q}(i)$ is hyperbolic 3-space.

If $\Gamma \subset \mathrm{SL}_2(\mathbb{Z}[i])$ is a sufficiently small congruence subrgroup, the $\Gamma\backslash\mathbb{H}^3$ are arithmetic hyperbolic 3-manifolds. They do not have the structure of algebraic varieties!

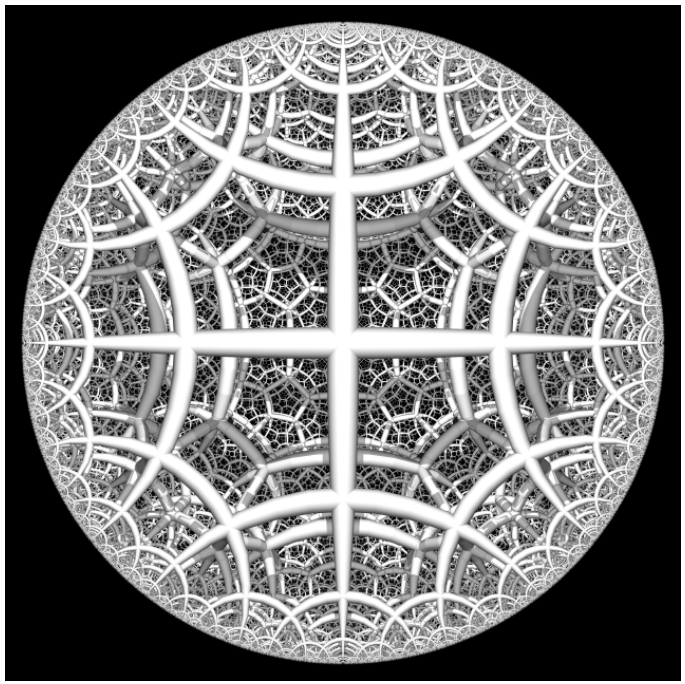


Image credit: http://kim.oyhus.no/icosians.html

The Langlands program

The modularity of elliptic curves is an instance of the global Langlands correspondence. This matches:

$$\{\text{spectral data}\} \text{ – seen on the automorphic side}$$

with

$$\{\text{arithmetic data}\} \text{ – seen on the Galois side.}$$

There are many instances of Langlands correspondences, including some with a more geometric flavour. It is an exciting and rapidly evolving field!

Thank you!

Career path and recognition

- PhD Harvard University (2007–2012).
- Postdocs: University of Chicago (2012–2013), Princeton / IAS (2013–2016), University of Bonn (2016–2017).
- Permanent positions: Imperial (2017–), University of Bonn (2022–).
- Professional recognition: LMS Whitehead Prize (2018), ERC Starting Grant (2019), EMS Prize (2020), New Horizons Prize (2023).

Things people have said to / about me

- That sounds complicated! You should leave it to the experts. (Professor during my PhD)
- Most of her papers are collaborative. The only single-author papers are from her PhD and they demonstrate technical strength but are not very creative. I am skeptical that she will become a leader in the field. (ERC reviewer)
- I guess, for now, you are a better mathematician than me. (Postdoc hired on my ERC grant)

Some advice

- Be aware of your strengths and weaknesses.
- Think about the long-term and aim for a growth mindset.
- Find (or build!) your community.