Reciprocity laws and torsion classes

Ana Caraiani

Imperial College London

January 2022

Motivation

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.

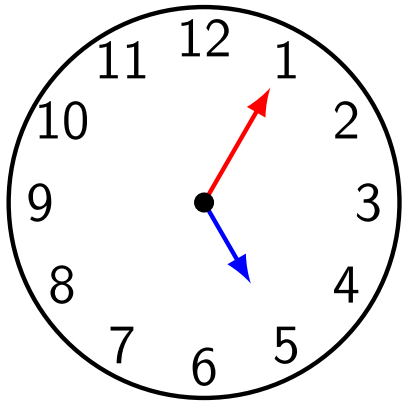
$$\left(\frac{p}{\ell}\right) \cdot \left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{\ell-1}{2}}$$

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".



Higher-dimensional reciprocity laws

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 laws

- 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 laws

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

Modular forms and elliptic curves

- 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 $\mathbb{Q}$.

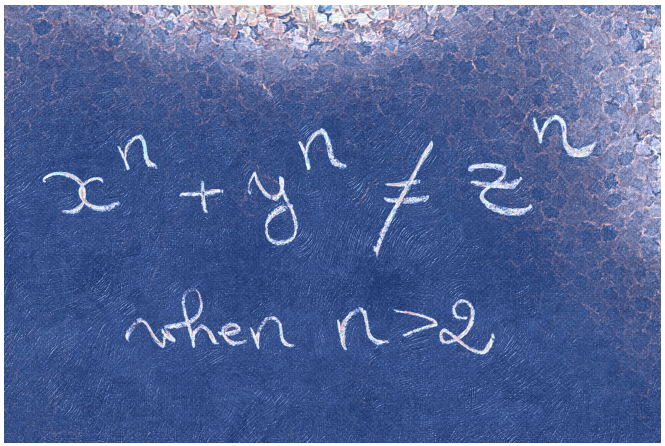
Modular forms and elliptic curves

- 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 $\mathbb{Q}$.



What is the Langlands correspondence?

The global Langlands correspondence matches:

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

with

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

To describe such a correspondence, we first need to choose:

- a global field F, such as $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(i)$;
- a connected reductive group G, such as GL_n, or SL_n, or Sp_{2n}.

The Galois side

Given a number field F, we are interested in its absolute Galois group

$$\Gamma_F = \varprojlim_{F'} \mathrm{Gal}(F'/F),$$

where F' runs over all finite Galois extensions of F.

The Galois side

Given a number field F, we are interested in its absolute Galois group

$$\Gamma_F = \varprojlim_{F'} \mathrm{Gal}(F'/F),$$

where F' runs over all finite Galois extensions of F.

For example, if $E/\mathbb{Q}$ is an elliptic curve, we have an action of $\Gamma_{\mathbb{Q}}$ on the torsion points

$$E[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2.$$

As n varies, these give rise to a Galois representation

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

More generally, the étale cohomology of algebraic varieties defined over number fields is a source of Galois representations.

The automorphic side

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

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

that satisfies many symmetries and a growth condition.

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

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

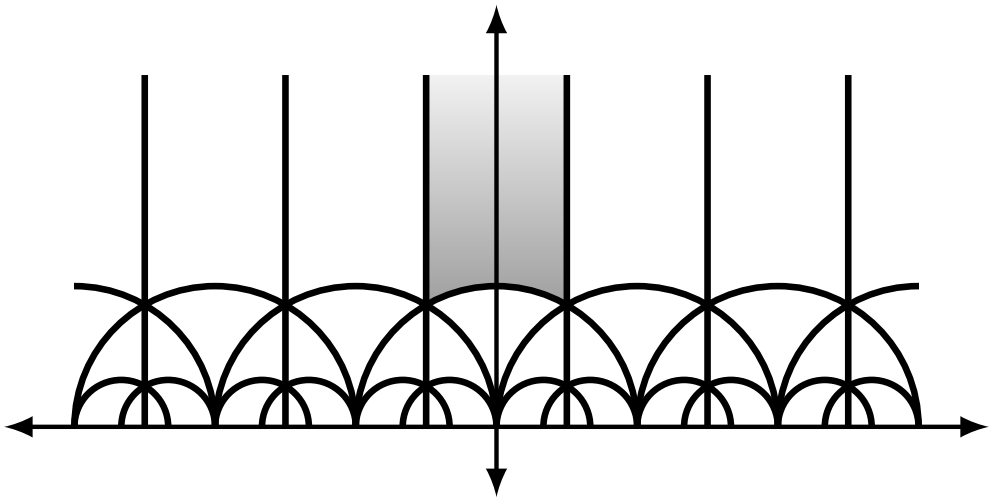
This gives the identification of $\mathbb{H}$ with the symmetric space

$$\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$$

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

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

The correspondence

Recall the example

$$E : y^2 + y = x^3 - x^2, \text{ and}$$

$$f(z) := q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2, q = e^{2\pi i z}.$$

The correspondence

Recall the example

$$E : y^2 + y = x^3 - x^2, \text{ and}$$

$$f(z) := q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2, q = e^{2\pi i z}.$$

When we say that E and f are matched under the global Langlands correspondence, we mean that there is an isomorphism

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

The correspondence

Recall the example

$$E : y^2 + y = x^3 - x^2, \text{ and}$$

$$f(z) := q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2, q = e^{2\pi i z}.$$

When we say that E and f are matched under the global Langlands correspondence, we mean that there is an isomorphism

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

This implies the explicit reciprocity law

$$a_\ell = \ell - N_\ell \text{ for all primes } \ell \neq 11,$$

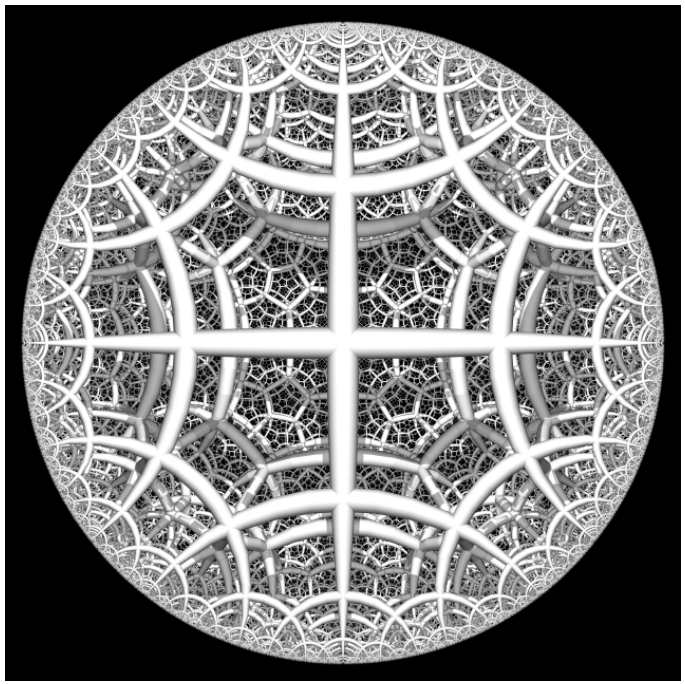
by taking traces at distinguished conjugacy classes $\{\mathrm{Frob}_\ell\} \in \Gamma_{\mathbb{Q}}$.

New frontiers

Arithmetic hyperbolic 3-manifolds

Let F be an imaginary quadratic field. The symmetric space for SL_2/F is hyperbolic 3-space $\mathrm{SL}_2(\mathbb{C})/\mathrm{SU}_2(\mathbb{R}) \simeq \mathbb{H}^3$.

If $\Gamma \subset \mathrm{SL}_2(\mathcal{O}_F)$ 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!



Torsion cohomology

- Let F be a CM field and X_Γ be a locally symmetric space for GL_n/F.

Theorem 1 (Scholze, 2013)

Any system of Hecke eigenvalues occurring in $H^*(X_\Gamma, \mathbb{F}_\ell)$ has an associated Galois representation $\rho : \Gamma_F \to \mathrm{GL}_n(\mathbb{F}_\ell)$.

- This strengthens previous work of Harris–Lan–Taylor–Thorne for $H^*(X_\Gamma, \mathbb{Q}_\ell)$ (automorphic forms).
- The need to consider torsion classes comes from the Calegari–Geraghty extension of the Taylor–Wiles method.

The Sato–Tate conjecture

Recall the elliptic curve

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

By Hasse, the normalised error terms $\frac{\ell - N_\ell}{2\sqrt{\ell}}$ are in $[-1, 1]$. The Sato–Tate conjecture predicts they are equidistributed with respect to the semicircle probability measure $\frac{2}{\pi}\sqrt{1-x^2}dx$.

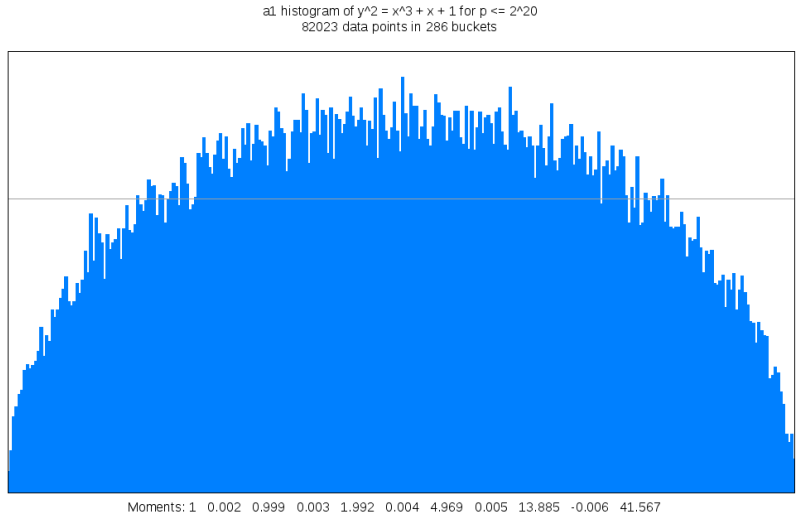


Image credit: A. Sutherland, "Sato–Tate Distributions"

The Sato–Tate conjecture

- For (most) elliptic curves over $\mathbb{Q}$, the Sato–Tate conjecture was proved by Clozel, Harris, Shepherd-Barron, and Taylor in 2008.

Theorem 2 (Allen, Calegari, C., Gee, Helm, Le Hung, Newton, Scholze, Taylor, Thorne, 2018)

Let F be a CM field and let E/F be an elliptic curve without complex multiplication. Then E is potentially automorphic and satisfies the Sato–Tate conjecture.

The Ramanujan conjecture

- The Ramanujan conjecture bounds the absolute value of Fourier coefficients of modular eigenforms.
- Its generalisation predicts that the local components of cuspidal automorphic representations of GL_n are tempered.

Theorem 3 (Allen, Calegari, C., Gee, Helm, Le Hung, Newton, Scholze, Taylor, Thorne, 2018)

Let F be a CM field and π be a cuspidal automorphic representation of GL_2/F of parallel weight 2. Then π satisfies the generalised Ramanujan–Petersson conjecture.

Shimura varieties

- Theorems 2 and 3 rely on the following result about Shimura varieties.

Theorem 4 (C., Scholze, 2015, 2019, Koshikawa 2021)

Let X_K be a unitary Shimura variety and $\mathfrak{m}$ be a system of Hecke eigenvalues occurring in $H^i_{(c)}(X_K, \mathbb{F}_p)$. Under mild technical assumptions on X_K, if $\mathfrak{m}$ is sufficiently generic, then

$$H^i_c(X_K, \mathbb{F}_p)_{\mathfrak{m}} = 0 \text{ for } i \geq \dim X_K.$$

- The proof relies on the geometry of the Hodge–Tate period morphism, which gives a new way to access the cohomology of Shimura varieties.

Local-global compatibility

Theorem 5 (C., Newton, in preparation)

Assume F is a CM field with $F^+ \neq \mathbb{Q}$. Under mild technical assumptions, the Galois representations constructed in Theorem 1 satisfy local-global compatibility at $\ell = p$ in the crystalline case.

- This goes significantly beyond the state of the art: p can be small, highly ramified in F, and the Hodge–Tate weights of the Galois representation can be arbitrarily high.

Thank you!