From differential forms to Galois representations (and back again): a survey of Serre's conjecture

Bryden Cais

Sumner Myers Colloquium, March 21, 2008

What Do Number Theorists Do?

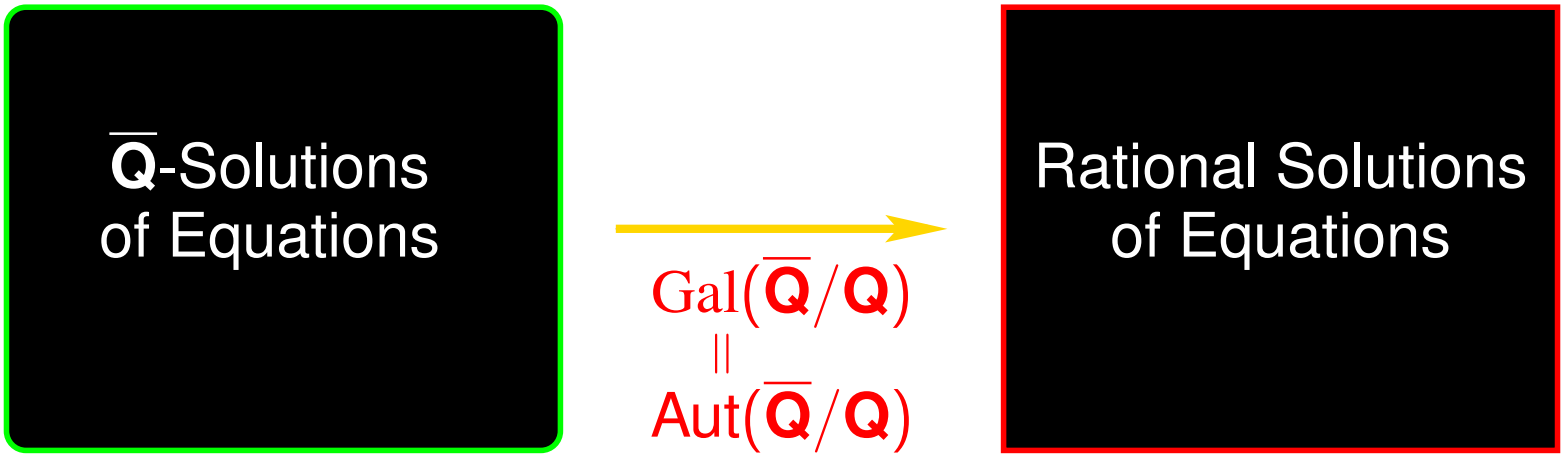
- Study rational solutions of equations:
  - Pythagorean Triples: $x^2 + y^2 = z^2$
    Solutions: $(x, y, z) = (3, 4, 5),\ (5, 12, 13),\ (7, 24, 25), \ldots$
  - Pell's equation: $x^2 - 3y^2 = 1$
    Solutions: $(x, y) = (2, 1),\ (7, 4),\ (26, 15), \ldots$
  - Congruent Number Problem: $x^2 + y^2 = z^2$ and $\frac{1}{2}xy = 157$
    Simplest Solution: $x = \frac{411340519227716149383203}{21666555693714761309610}$
- Can be extremely hard to understand rational solutions!
  - FLT: $x^n + y^n = z^n$, $xyz \neq 0$
  - BSD Conjecture: $y^2 = x^3 + ax + b$

From rational solutions to the Galois group

- Instead of studying solutions to particular equations... study solutions to all equations at once!
- Easy to understand solutions in $\overline{\mathbf{Q}}$
  - Ex: $2^5 + 3^5 = (\sqrt[5]{2^5 + 3^5})^5$

EASY PROBLEM

HARD PROBLEM



- The absolute Galois group measures the difference between the problem we can solve and the problem we want to solve.

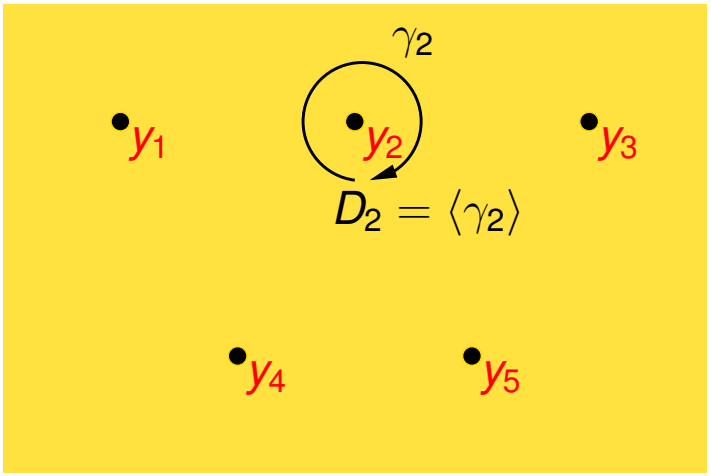
$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is very complicated

- Every symmetric group S_n is a quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (Hilbert)
- Every finite solvable group is a quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (Shafarevich)
- The Monster is a quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$
- If you believe the truth of the inverse Galois problem, then every finite group is a quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$!

How to visualize $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$

- For each prime number ℓ, there is a distinguished subgroup $D_\ell \subseteq \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$
- The subgroups D_ℓ generate $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$
- Analogy:

$$Y = \mathbf{C} - \{y_1, \ldots, y_5\}$$



$\pi_1(Y, y)$ is generated by the groups $D_i \simeq \mathbf{Z}$

To understand $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, study its representations!

- General mathematical principle: to understand a complicated group, study how it acts on various structures:
- Study representations, i.e. homomorphisms

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(V),$$

  where $V =$ some mathematical object.
- Natural choices for V are vector spaces over a field F:
  - The groups $\mathrm{Aut}(F^n) = \mathrm{GL}_n(F)$ are well-understood.
  - Allows us to "break up" the study of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ by dimension.
- N.B. If instead we considered certain types of graphs for V, we would get Grothendieck's theory of dessins d'enfants.

Representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$

- We will concentrate on (continuous) linear representations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(F)$
  - Natural choices for F are: $\mathbf{C}$, $\overline{\mathbf{F}}_p$, $\overline{\mathbf{Q}}_p \ldots$
- Major question: How to classify such representations?
- When $n = 1$, the crown jewel of 19th century algebraic number theory, Class Field Theory, provides a complete description of (continuous) homomorphisms:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) & \longrightarrow & \mathrm{GL}_1(F) = F^\times \\ \downarrow & \nearrow & \\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})^{\mathrm{ab}} & & \end{array}$$

- Topological analogy: 1-dimensional representations of $\pi_1(Y, y)$ yield information about $\pi_1(Y, y)^{\mathrm{ab}} = H_1(Y, \mathbf{Z})$
- For all $n > 0$: Langlands Program (many conjectures).

Representations coming from Geometry I

We can rephrase our study of rational solutions of equations:

- If $X =$ algebraic variety defined by equations over $\mathbf{Q}$, then $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts naturally on

$$X(\overline{\mathbf{Q}}) = \text{set of } \overline{\mathbf{Q}}\text{-solutions to those equations}$$

number theory

$\cap$

geometry

$$X(\mathbf{C}) = \text{complex variety (like a manifold)}$$

- We'll focus on the simplest case: $X =$ a curve

Representations coming from Geometry II

Question: How to make a vector space out of $X(\overline{\mathbf{Q}})$?

- Problem: In general no way to add elements of $X(\overline{\mathbf{Q}})$
- However, there is a smallest commutative algebraic group variety containing X: the Jacobian $\mathrm{Jac}(X)$

$$\text{Can't add} \longrightarrow X(\overline{\mathbf{Q}}) \subseteq \mathrm{Jac}(X)(\overline{\mathbf{Q}}) \longleftarrow \text{Can add!}$$

- We get a $\mathbf{Q}$-vector space by killing torsion:

$$V^{\mathrm{bad}} = \mathrm{Jac}(X)(\overline{\mathbf{Q}}) \otimes_{\mathbf{Z}} \mathbf{Q}$$

- V^{bad} gives a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, but it is almost never finite dimensional!

Representations coming from Geometry III

- Salvage: Instead of killing torsion, use it! For each prime p,

$$V_p := \mathrm{Jac}(X)(\overline{\mathbf{Q}})_p := \left\{ \alpha \in \mathrm{Jac}(X)(\overline{\mathbf{Q}}) \ : \ p \cdot \alpha = 0 \right\}$$

  is a vector space over the finite field $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$
- $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on V_p, so get a Galois representation!

Question: What is the dimension of V_p?

- $\mathrm{Jac}(X)$ has dimension $g =$ genus of X
- The complex Lie group $\mathrm{Jac}(X)(\mathbf{C})$ is a complex torus:

$$\mathrm{Jac}(X)(\mathbf{C}) \simeq \mathbf{C}^g/\Lambda \qquad (\text{For some lattice } \Lambda \subseteq \mathbf{C}^g)$$

- Follows that $V_p \simeq \frac{1}{p}\Lambda/\Lambda \simeq \Lambda \otimes_{\mathbf{Z}} \mathbf{F}_p$, so dim $V_p = 2g$.

Subrepresentations of V_p

- Problem: In general, dim $V_p = 2g$ is too big!
- Q: How to decompose V_p into smaller representations?
- A: Use endomorphisms!

Endomorphism $T : V_p \to V_p$ $\longrightarrow$ Eigenspace decomposition

$\lambda =$ eigenvalue of T $\longrightarrow$ $V_p^\lambda =$ eigenspace

Any algebra $\mathbf{H} \subseteq \mathrm{End}(V_p)$ $\longrightarrow$ Similar decomposition with smaller pieces

$\lambda : \mathbf{H} \to \overline{\mathbf{F}}_p$ $\longrightarrow$ $V_p^\lambda = \{v \ : \ Tv = \lambda(T)v\}$

Goals:

- Find suitable $\mathbf{H} \subseteq \mathrm{End}(V_p)$
- Find suitable $\lambda \in \mathrm{Hom}(\mathbf{H}, \overline{\mathbf{F}}_p)$

How do we find a suitable **H**?

- To get smaller representations from V_p, we need $\mathbf{H} \subseteq \mathrm{End}(V_p)$ that commute with $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-action

$$\mathrm{End}(\mathrm{Jac}(X)) \subseteq \left\{ \begin{array}{l} \text{End's commuting} \\ \text{with Galois} \end{array} \right\} \subseteq \mathrm{End}(V_p)$$

- To exploit the geometry of our situation, we'll choose

$$\mathbf{H} \subseteq \mathrm{End}(\mathrm{Jac}(X)) \subseteq \mathrm{End}(V_p)$$

- Big algebras $\mathbf{H} \leftrightarrow$ small subrepresentations V_p^λ

How to find suitable λ: From differentials to rep's

For any smooth curve X of genus g, we have a map

$$\mathbf{Z}^{2g} \simeq H_1(X, \mathbf{Z}) \longrightarrow H^0(X, \Omega_X)^\vee \simeq \mathbf{C}^g$$

by integrating differential forms along homology cycles.

Abel-Jacobi: As complex tori, $\mathrm{Jac}(X)(\mathbf{C}) \simeq \dfrac{H^0(X, \Omega_X)^\vee}{H_1(X, \mathbf{Z})}$

- Any $\mathbf{H} \subseteq \mathrm{End}(\mathrm{Jac}(X))$ acts on $\mathrm{Cot}_0(\mathrm{Jac}(X)) = H^0(X, \Omega_X)$
- Suppose $\omega \in H^0(X, \Omega_X)$ is an eigenvector for all $T \in \mathbf{H}$:

$$T\omega = \lambda(T)\omega, \qquad \lambda(T) \in \mathbf{C}$$

- Then $\lambda \in \mathrm{Hom}(\mathbf{H}, \mathbf{C})$ and we can reduce to get

$$\overline{\lambda} \in \mathrm{Hom}(\mathbf{H}, \overline{\mathbf{F}}_p)$$

- This gives the desired λ, hence a subrepresentation

$$V_p^\omega := V_p^{\overline{\lambda}}$$

Summary

X curve of genus g

p a prime

$$V_p = \left\{ \alpha \in \mathrm{Jac}(X)(\overline{\mathbf{Q}}) \ : \ p \cdot \alpha = 0 \right\}$$

a $2g$-dimensional $\mathbf{F}_p$-representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$

subalgebra $H \subseteq \mathrm{End}(\mathrm{Jac}(X))$

eigenvector for all $T \in H$ $\omega \in H^0(X, \Omega_X)$

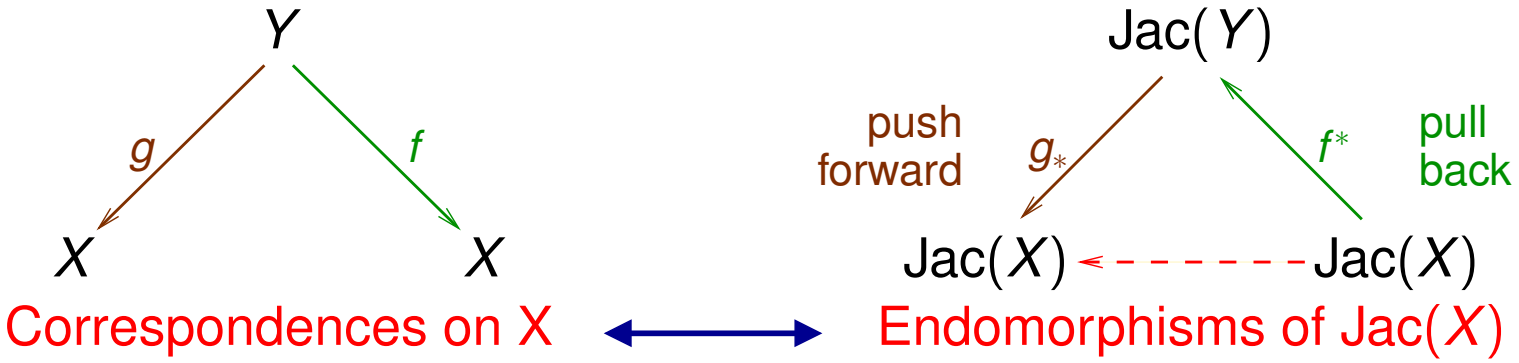
V_p^ω the subrepresentation of V_p attached to ω

Endomorphisms of Jac(X)

- If X is a generic curve of genus g then

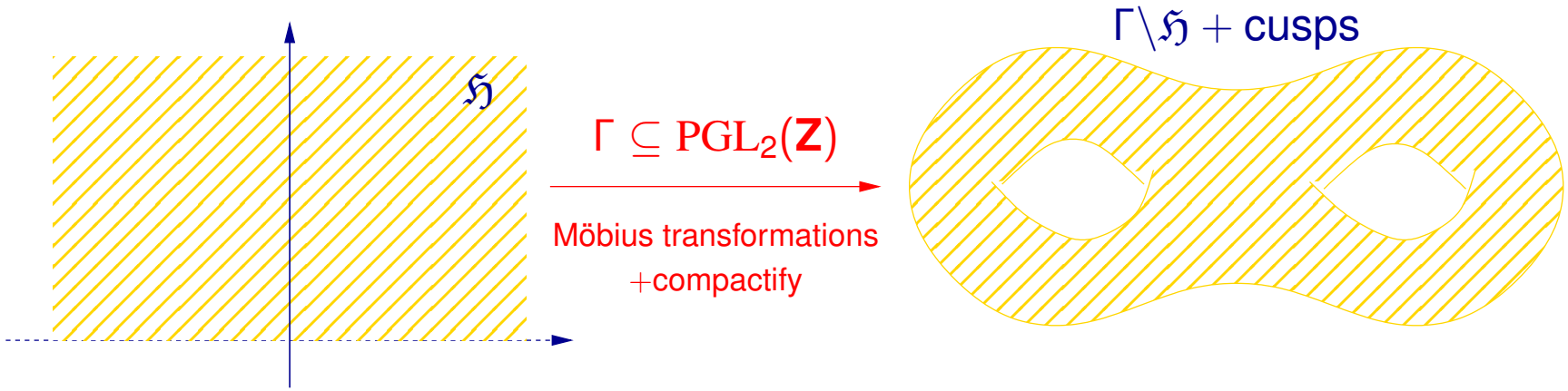
$$\mathrm{End}(\mathrm{Jac}(X)) \simeq \mathbf{Z}.$$

- So every $\omega \in H^0(X, \Omega_X)$ is an eigenvector; $V_p^\omega = V_p$
- How to find special curves X for which End(Jac(X)) is big?



- Q: How to find curves with lots of correspondences?

Correspondences and Belyi's Theorem



$\Gamma \subseteq \mathrm{PGL}_2(\mathbf{Z})$ $\longrightarrow$ $\Gamma\backslash\mathfrak{H}$ + cusps $\longrightarrow$ X_Γ

finite index

compact Riemann surface

algebraic curve

Belyi's Theorem: Every smooth curve (defined over a finite extension of $\mathbf{Q}$) is equal to X_Γ for some $\Gamma \subseteq \mathrm{PGL}_2(\mathbf{Z})$.

- Q: When does X_Γ have lots of correspondences?
- A: When Γ has good group-theoretic properties!
- (good = Γ is of infinite index in its commeasurator)

Modular curves

It turns out that good choices for Γ are congruence subgroups:

$$\Gamma_N = 2 \times 2 \text{ integer matrices} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N$$

Definition

The *modular curve of level N* is $X_N := X_{\Gamma_N} = \Gamma_N \backslash \mathfrak{H} + \text{cusps}$

- X_N is defined over $\mathbf{Q}$ and has many correspondences
- $\mathrm{End}(\mathrm{Jac}(X_N))$ contains a commutative subalgebra

$$\mathbf{H}_N \subseteq \mathrm{End}(\mathrm{Jac}(X_N))$$

  of rank $\mathrm{genus}(X_N)$ over $\mathbf{Z}$
- $H^0(X_N, \Omega_{X_N})$ has many eigenvectors for H_N
- For most $\mathbf{H}_N$-eigenvectors ω,

$$\dim V_p^\omega = 2$$

Serre's conjecture I

$N \in \mathbf{Z}$

$\omega \in H^0(X_N, \Omega_{X_N})$

eigenvector for $\mathbf{H}_N$

$\rho_{N,\omega} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}(V_p^\omega)$

Galois representation (continuous)

Facts:

- For most ω, we have $\dim V_p^\omega = 2$
- $\rho_{N,\omega}$ is *odd*, that is $\det \rho_{N,\omega}(\text{cplx. conj.}) = -1$

Get lots of odd, 2-dimensional, mod p Galois representations.

Conjecture (Serre)

Every odd and irreducible continuous representation

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

is isomorphic to $\rho_{N,\omega}$ for some N, ω.

Serre's conjecture II

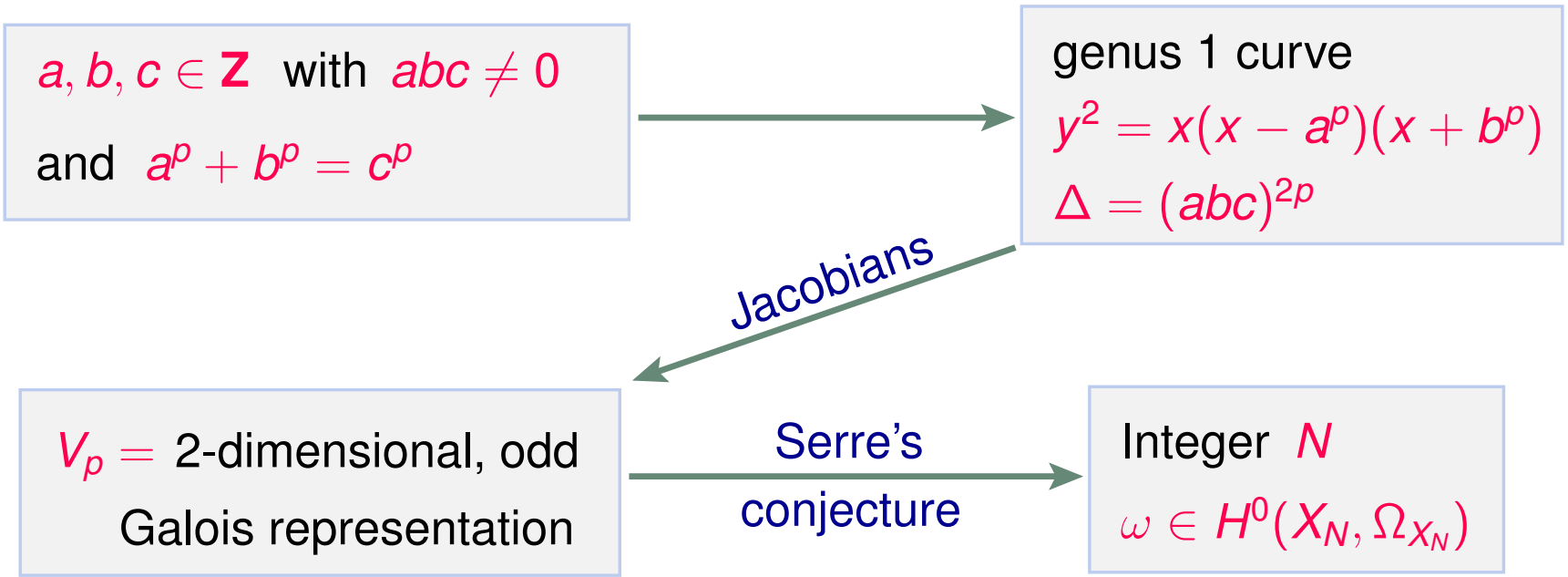
Given a Galois representation ρ as in his conjecture, Serre further conjectured a precise recipe for computing an appropriate N so that $\rho = \rho_{N,\omega}$

Building on work of many mathematicians:

Theorem (Khare-Wintenberger, 2006)

Serre's conjecture (*with his predictions for N*) *is true.*

Application: Fermat's Last Theorem



- By construction, V_p is nontrivial and odd
- $\Delta = p^{\text{th}}$-power $\implies$ can take $N = 2$
- But X_2 has genus zero, so $H^0(X_2, \Omega_{X_2}) = 0$
- $\implies$ V_p is trivial, a contradiction

Fourier expansions I

Differential forms on

$X_N := \Gamma_N \backslash \mathfrak{H} + \text{cusps}$

$\longleftrightarrow$

Γ_N-invariant differential forms on $\mathfrak{H}$ that are holomorphic at cusps

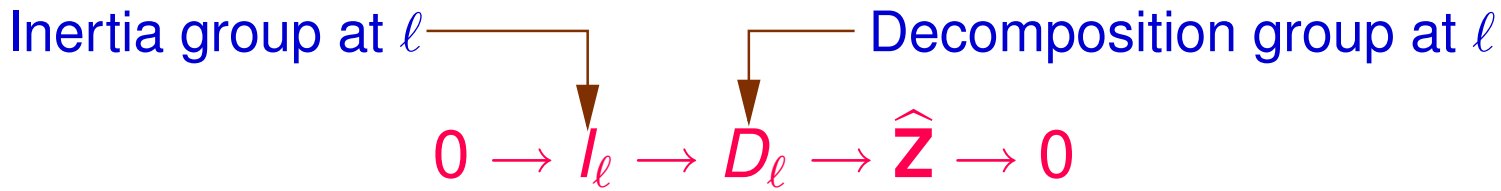
- By definition of Γ_N, every Γ_N-invariant differential form on $\mathfrak{H}$ is periodic
- $\Longrightarrow$ Every Γ_N-invariant differential form on $\mathfrak{H}$ has a Fourier expansion in powers of $q := e^{2\pi i z}$

$$\omega = \left(\sum_{n \geq 1} a_n q^n \right) \frac{dq}{q}$$

- The a_n encode deep information about $\rho_{N,\omega}$

Fourier expansions II

Recall: $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is (topologically) generated by subgroups D_ℓ



Def: A Galois representation ρ is unramified at ℓ if $\rho\big|_{I_\ell}$ is trivial

$\Longrightarrow$ $\rho\big|_{D_\ell}$ determined by $\rho(\sigma_\ell)$ for any $\sigma_\ell \in D_\ell$ mapping to $1 \in \widehat{\mathbf{Z}}$

Fix

$$\omega = \sum_{n \geq 1} a_n q^n \frac{dq}{q} \in H^0(X_N, \Omega_{X_N}),$$

an eigenvector for $\mathbf{H}_N$, normalized so $a_1 = 1$. For $\ell \nmid Np$:

- $\rho_{N,\omega}$ is unramified at ℓ
- $\mathrm{Trace}(\rho_{N,\omega}(\sigma_\ell)) \equiv a_\ell \cdot$ (known factor)

Refined questions

Question: How to understand $\rho_{N,\omega}\big|_{D_\ell}$ for $\ell | Np$, esp. $\ell = p$?

Theorem (Deligne, 1974)

If $a_p \not\equiv 0$, then the restriction of $\rho_{N,\omega}$ to D_p is upper-triangular

Theorem (Gross, 1989)

If $a_p \not\equiv 0$, then $\rho_{N,\omega}\big|_{D_p}$ is diagonal if and only if there exists an eigenvector for $\mathbf{H}_N$

$$\eta = \sum_{n \geq 1} b_n q^n \frac{dq}{q} \in H^0(X_N, \Omega_{X_N})$$

with $\eta \not\equiv \omega$, and an integer k such that

$$n^k b_n \equiv n a_n \qquad \text{for all } n$$

Thesis work I

Main tool in Gross' proof of his theorem: *p*-adic cohomology of modular curves and Jacobians:

- (*p*-adic) de Rham cohomology
- Crystalline cohomology and Dieudonné modules
- Monsky-Washnitzer cohomology

There are many comparison maps between these theories, which form the heart of Gross' argument

Gross' proof is incomplete, because he needed to assume:

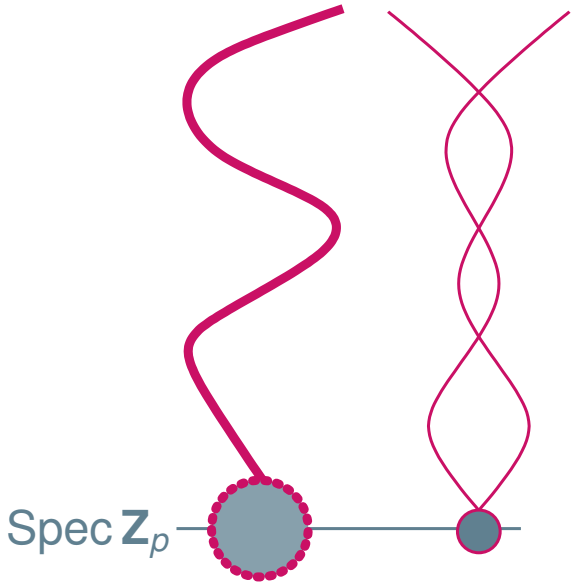
- Correspondences act on Monsky-Washnitzer cohomology
- Comparison maps are compatible with:
  - Endomorphisms, including Frobenius
  - Integral structures (i.e. certain $\mathbf{Z}_p$-lattices)

These things were not known at the time

Thesis work II

What was required to fill in these missing pieces?

- p-adic cohomology for families with a degenerate fiber



- Berthelot's rigid cohomology

$$H^1_{\text{cris}} \longleftrightarrow H^1_{\text{rig}} \longleftrightarrow H^1_{\text{MW}}$$

- Trace morphisms in rigid cohomology

$$f : X \to Y \longrightarrow f_* : H^1_{\text{rig}}(X) \to H^1_{\text{rig}}(Y)$$

Thank You