Explicit Modular Approaches to Generalized Fermat Equations

David Brown

University of Wisconsin-Madison
Slides available at `http://www.math.wisc.edu/~brownda/slides/`

Emory University Colloquium

February 14, 2011

Basic Problem (Solving Diophantine Equations)

Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$ be polynomials and let R be a ring (e.g., $R = \mathbb{Z}$, $\mathbb{Q}$).

Problem

Describe the set

$$\left\{(a_1, \ldots, a_n) \in R^n : \forall i, f_i(a_1, \ldots, a_n) = 0\right\}.$$

Basic Problem (Solving Diophantine Equations)

Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$ be polynomials and let R be a ring (e.g., $R = \mathbb{Z}$, $\mathbb{Q}$).

Problem

Describe the set

$$\left\{(a_1, \ldots, a_n) \in R^n : \forall i, f_i(a_1, \ldots, a_n) = 0\right\}.$$

Fact

Solving diophantine equations is hard.

Fermat's Last Theorem

Theorem (Wiles; Taylor-Wiles 1995)

The only integer solutions to the equation

$$x^n + y^n = z^n, n \geq 3$$

satisfy $xyz = 0$.

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)} \colon y^2 = x(x - a^p)(x + b^p)$$

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$
\begin{aligned}
E_{(a,b,c)} \colon y^2 &= x(x - a^p)(x + b^p) \\
j &= \frac{2^8 \left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}} \\
\Delta &= 2^{-8}(abc)^{2p}.
\end{aligned}
$$

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)} \colon y^2 = x(x - a^p)(x + b^p)$$
$$j = \frac{2^8 \left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}}$$
$$\Delta = 2^{-8}(abc)^{2p}.$$

Step 3: (Ribet) Show that the Frey curve $E_{(a,b,c)}$ is not modular.

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)}\colon y^2 = x(x - a^p)(x + b^p)$$
$$j = \frac{2^8\left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}}$$
$$\Delta = 2^{-8}(abc)^{2p}.$$

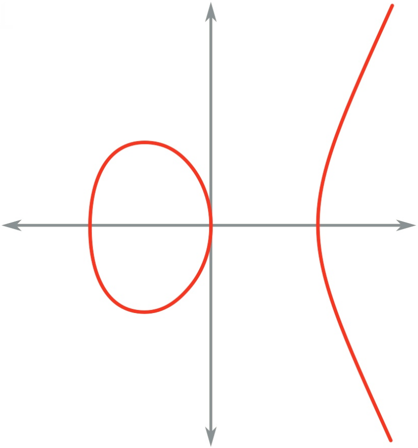
Step 3: (Ribet) Show that the Frey curve $E_{(a,b,c)}$ is not modular.

Step 4: Prove that every elliptic curve over $\mathbb{Q}$ is modular.

Modularity is now a theorem

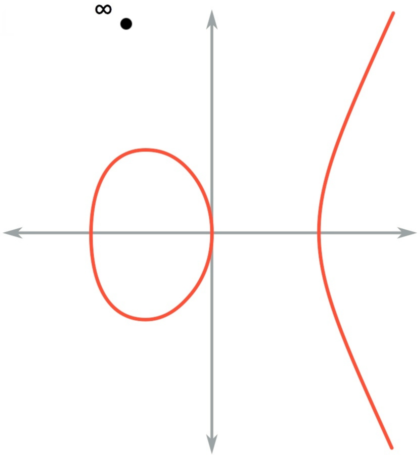
Theorem (Wiles 1995; Breuil-Conrad-Diamond-Taylor 2002)

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



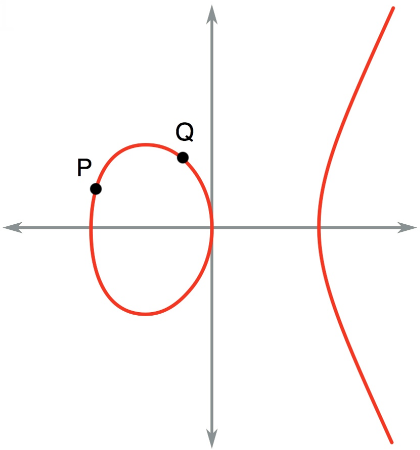
$$E: y^2 = x^3 + ax + b$$

Elliptic Curves - point at infinity



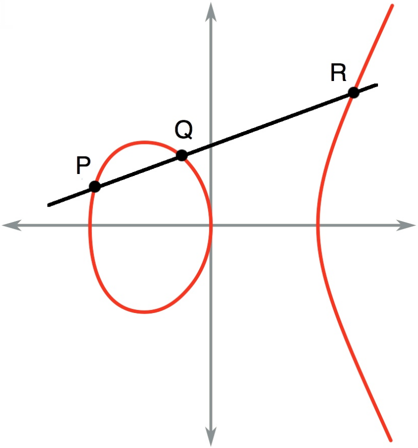
$$E: zy^2 = x^3 + axz^2 + bz^3$$
$$\infty = [0 : 1 : 0]$$

Elliptic Curves – addition



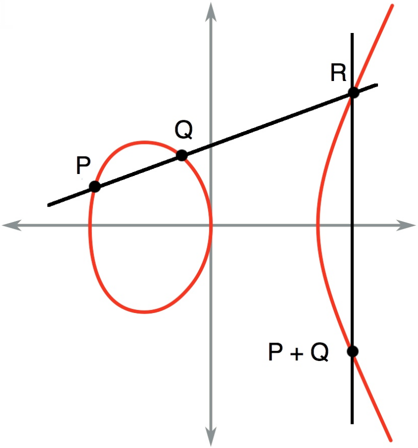
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$Q = (x_1, y_1) \in \mathbb{Q}^2$$

Elliptic Curves – addition



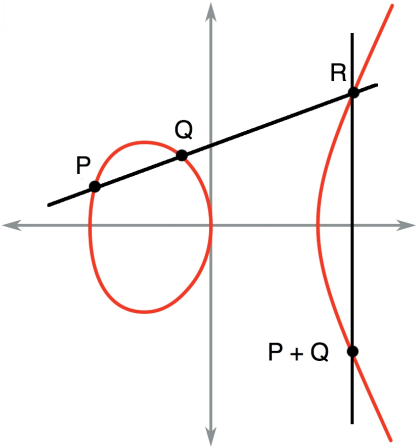
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$Q = (x_1, y_1) \in \mathbb{Q}^2$$
$$R = (x_2, y_2) \in \mathbb{Q}^2$$

Elliptic Curves – addition



$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$Q = (x_1, y_1) \in \mathbb{Q}^2$$
$$R = (x_2, y_2) \in \mathbb{Q}^2$$
$$P + Q = (x_2, -y_2) \in \mathbb{Q}^2$$

Elliptic Curves – addition

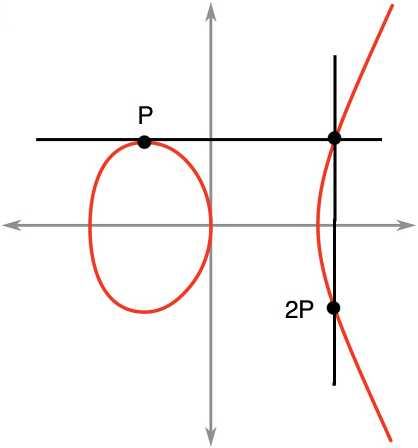


$$E: y^2 = x^3 + ax + b$$

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$$

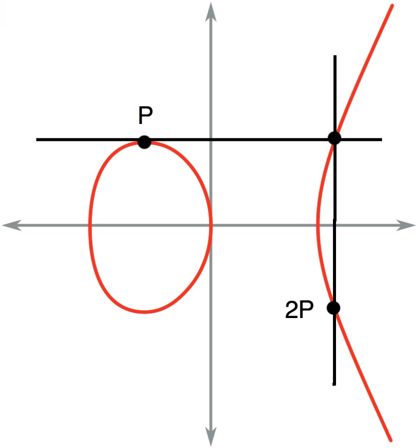
$$(P\ ,\ Q) \quad \mapsto P + Q$$

Elliptic Curves - duplication



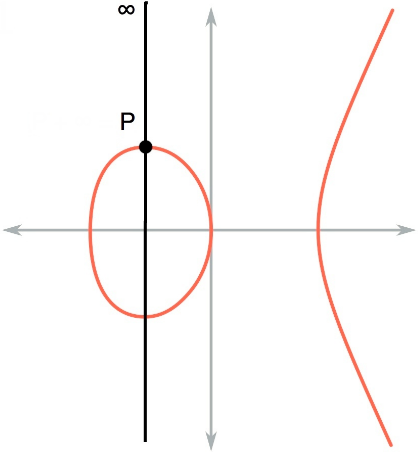
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$

Elliptic Curves - duplication



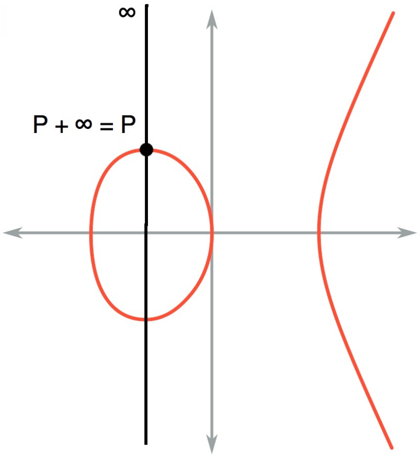
$$E\colon y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$2P = (x_3, y_3) \in \mathbb{Q}^2$$

Elliptic Curves – identity



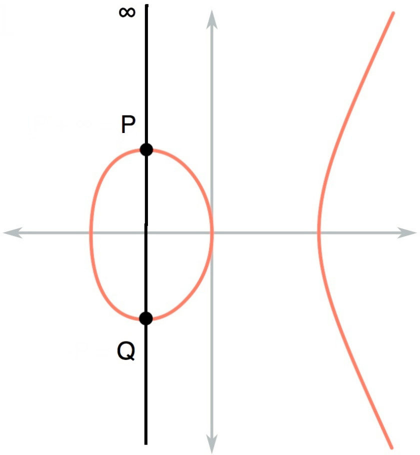
$$E\colon y^2 = x^3 + ax + b$$

Elliptic Curves – identity



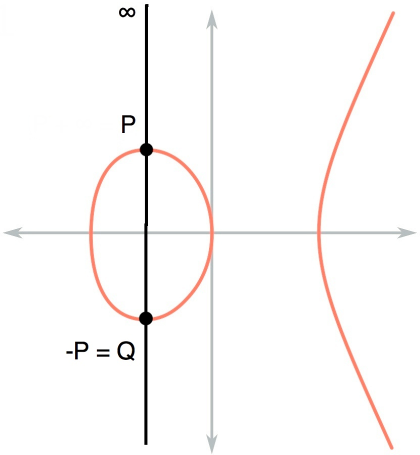
$$E: y^2 = x^3 + ax + b$$

Elliptic Curves – inverses



$$E : y^2 = x^3 + ax + b$$

Elliptic Curves – inverses



$$E : y^2 = x^3 + ax + b$$

Elliptic Curves – torsion subgroup

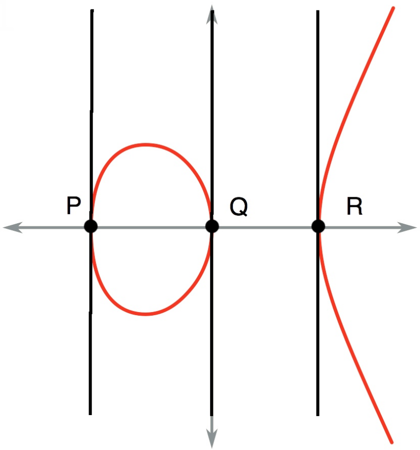
Let $n \in \mathbb{Z}$ be an integer.

Definition

The *n-torsion subgroup* $E[n]$ of E is defined to be

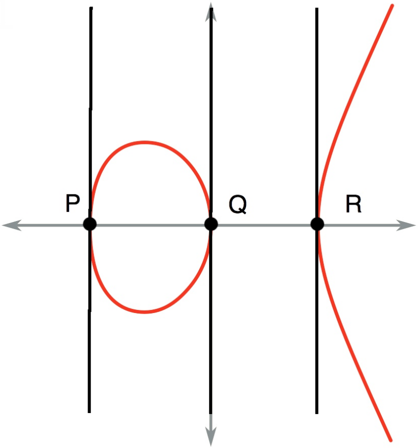
$$\ker\left(E \xrightarrow{[n]} E\right) := \{P \in E : nP := P + \ldots + P = \infty\}.$$

Elliptic Curves – two torsion



$$E\colon y^2 = x^3 + ax + b$$

Elliptic Curves – two torsion



$$E: y^2 = x^3 + ax + b$$
$$2P = 2Q = 2R = \infty$$

Elliptic Curves – structure of torsion

Let E be given by the equation $y^2 = f(x) = x^3 + ax + b$.

- $E[n](\mathbb{C}) = E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Elliptic Curves – structure of torsion

Let E be given by the equation $y^2 = f(x) = x^3 + ax + b$.

- $E[n](\mathbb{C}) = E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$.
- $E[n](\mathbb{Q})$ may be smaller,

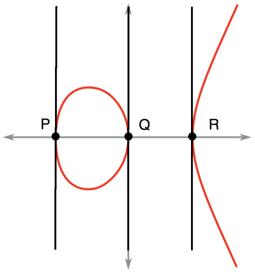
Elliptic Curves – structure of torsion

Let E be given by the equation $y^2 = f(x) = x^3 + ax + b$.

- $E[n](\mathbb{C}) = E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$.
- $E[n](\mathbb{Q})$ may be smaller, e.g.,

$$E[2](\mathbb{Q}) \cong \begin{cases} \{\infty\} & \text{if } f(x) \text{ has 0 rational roots} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } f(x) \text{ has 1 rational roots} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } f(x) \text{ has 3 rational roots} \end{cases}$$

Elliptic Curves – torsion



$$E[2](\mathbb{Q}) \cong \begin{cases} \{\infty\} & \text{if } f(x) \text{ has 0 rational roots} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } f(x) \text{ has 1 rational roots} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } f(x) \text{ has 3 rational roots} \end{cases}$$

Galois Representations associated to an elliptic curve

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Q}$.

Galois Representations associated to an elliptic curve

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Q}$.

- Let $G_{\mathbb{Q}} := \mathrm{Aut}(\overline{\mathbb{Q}})$

Galois Representations associated to an elliptic curve

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Q}$.

- Let $G_{\mathbb{Q}} := \mathrm{Aut}(\overline{\mathbb{Q}}) \cong \varprojlim_K \mathrm{Aut}(K)$.

Galois Representations associated to an elliptic curve

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Q}$.

- Let $G_{\mathbb{Q}} := \mathrm{Aut}(\overline{\mathbb{Q}}) \cong \varprojlim_K \mathrm{Aut}(K)$.
- Let $\sigma \in G_{\mathbb{Q}}$, $P = (x, y) \in E(\overline{\mathbb{Q}}) \rightsquigarrow P^\sigma = (x^\sigma, y^\sigma) \in E(\overline{\mathbb{Q}})$.

Galois Representations associated to an elliptic curve

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Q}$.

- Let $G_{\mathbb{Q}} := \mathrm{Aut}(\overline{\mathbb{Q}}) \cong \varprojlim_K \mathrm{Aut}(K)$.
- Let $\sigma \in G_{\mathbb{Q}}$, $P = (x, y) \in E(\overline{\mathbb{Q}}) \rightsquigarrow P^\sigma = (x^\sigma, y^\sigma) \in E(\overline{\mathbb{Q}})$.
- If $P \in E[n]$, then $P^\sigma \in E[n]$.

Galois Representations associated to an elliptic curve

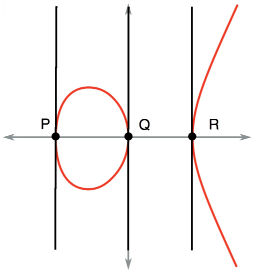
Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Q}$.

- Let $G_{\mathbb{Q}} := \mathrm{Aut}(\overline{\mathbb{Q}}) \cong \varprojlim_K \mathrm{Aut}(K)$.
- Let $\sigma \in G_{\mathbb{Q}}$, $P = (x, y) \in E(\overline{\mathbb{Q}}) \rightsquigarrow P^\sigma = (x^\sigma, y^\sigma) \in E(\overline{\mathbb{Q}})$.
- If $P \in E[n]$, then $P^\sigma \in E[n]$.

Definition

The mod n Galois representation associated to E is the homomorphism

$$G_{\mathbb{Q}} \to Aut(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$



$$E[2](\mathbb{Q}) \cong \begin{cases} \{\infty\} & \text{if } f(x) \text{ has 0 rational roots} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } f(x) \text{ has 1 rational roots} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } f(x) \text{ has 3 rational roots} \end{cases}$$

Galois Representations: examples

Example

Suppose that $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. (E.g., $E\colon y^2 = x(x-1)(x-\lambda)$ with $\lambda \in \mathbb{Q}$.) Then

$$\rho_{E,2}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

is the trivial homomorphism.

Galois Representations: examples

Example

Suppose that $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. (E.g., $E\colon y^2 = x(x-1)(x-\lambda)$ with $\lambda \in \mathbb{Q}$.) Then

$$\rho_{E,2}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

is the trivial homomorphism.

Example

Suppose that $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. (E.g., $E\colon y^2 = (x^2 + D)(x - \lambda)$ with $D, \lambda \in \mathbb{Q}$ and $D > 0$.) Then we can choose a basis for $E(\overline{\mathbb{Q}})[2]$ so that any $\sigma \in G_{\mathbb{Q}}$ acts as a matrix of the form

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}.$$

Galois Representations from modular forms

Let $\mathcal{H} := \{\tau = x + yi \in \mathbb{C} : y > 0\}$ be the complex upper half plane.

Galois Representations from modular forms

Let $\mathcal{H} := \{\tau = x + yi \in \mathbb{C} : y > 0\}$ be the complex upper half plane.

The formula $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \dfrac{a\tau + b}{c\tau + d}$ defines an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$.

Galois Representations from modular forms

Let $\mathcal{H} := \{\tau = x + yi \in \mathbb{C} : y > 0\}$ be the complex upper half plane.

The formula $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \dfrac{a\tau + b}{c\tau + d}$ defines an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$.

Definition

- A **modular function** is a complex analytic function $f : \mathcal{H} \to \mathbb{C}$ which is invariant under the action of a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ such that f is holomorphic at ∞.
- A **modular form of weight** $2k$ is a complex analytic function $f : \mathcal{H} \to \mathbb{C}$ such that $f(z)(dz)^k$ is invariant under the action of a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ such that f is holomorphic at ∞.

Let $\mathcal{H} := \{\tau = x + yi \in \mathbb{C} : y > 0\}$ be the complex upper half plane.

The formula $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \dfrac{a\tau + b}{c\tau + d}$ defines an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$.

Definition

- A **modular function** is a complex analytic function $f : \mathcal{H} \to \mathbb{C}$ which is invariant under the action of a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ such that f is holomorphic at ∞.
- A **modular form of weight** $2k$ is a complex analytic function $f : \mathcal{H} \to \mathbb{C}$ such that $f(z)(dz)^k$ is invariant under the action of a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ such that f is holomorphic at ∞.

$$\begin{tikzcd} f \arrow[r, rightsquigarrow] \arrow[d, rightsquigarrow] & E_f \arrow[d, rightsquigarrow] \\ \rho_{f,n} \arrow[r, equal] & \rho_{E_f,n} \end{tikzcd}$$

Galois Representations from modular forms

Fact

Galois representations associated to modular forms are easy to understand **and classify**.

Galois Representations from modular forms

Fact

Galois representations associated to modular forms are easy to understand **and classify**.

Theorem (Modularity)

Every elliptic curve over $\mathbb{Q}$ *arises from a modular form.*

Galois Representations from modular forms

Fact

Galois representations associated to modular forms are easy to understand **and classify**.

Theorem (Modularity)

Every elliptic curve over $\mathbb{Q}$ arises from a modular form.

$$\begin{tikzcd} f \arrow[r, rightsquigarrow] \arrow[d, rightsquigarrow] & E_f \arrow[d, rightsquigarrow] \\ \rho_{f,n} \arrow[r, equal] & \rho_{E_f,n} \end{tikzcd}$$

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)} \colon y^2 = x(x - a^p)(x + b^p)$$

$$j = \frac{2^8 \left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}}$$

$$\Delta = 2^{-8}(abc)^{2p}.$$

Step 3: (Ribet) Show that the Frey curve $E_{(a,b,c)}$ is not modular.

Step 4: Prove that every elliptic curve over $\mathbb{Q}$ is modular.

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$\begin{aligned} E_{(a,b,c)} \colon y^2 &= x(x - a^p)(x + b^p) \\ j &= \frac{2^8 \left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}} \\ \Delta &= 2^{-8}(abc)^{2p}. \end{aligned}$$

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$\begin{aligned} E_{(a,b,c)} \colon y^2 &= x(x - a^p)(x + b^p) \\ j &= \frac{2^8\left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}} \\ \Delta &= 2^{-8}(abc)^{2p}. \end{aligned}$$

Step 3: (Ribet) **Classify possibilities** for $E_{(a,b,c),p}$ (modularity is one tool used in this classification).

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)} \colon y^2 = x(x - a^p)(x + b^p)$$
$$j = \frac{2^8 \left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}}$$
$$\Delta = 2^{-8}(abc)^{2p}.$$

Step 3: (Ribet) **Classify possibilities** for $E_{(a,b,c),p}$ (modularity is one tool used in this classification).

Step 4: The output of step 3 turns out to be empty!

Other applications of the modular method

The ideas behind the proof of FLT now permeate the study of diophantine problems.

Other applications of the modular method

The ideas behind the proof of FLT now permeate the study of diophantine problems.

Theorem (Bugeaud, Mignotte, Siksek 2006)

The only Fibonacci numbers that are perfect powers are

$$F_0 = 0,\ F_1 = F_2 = 1,\ F_6 = 8,\ F_{12} = 144.$$

More applications of the modular method

Theorem (Darmon, Merel 1997)

Any pairwise coprime integer solution to the equation

$$x^n + y^n = z^2, n \geq 4$$

satisfies $xyz = 0$.

Template for the proof of Darmon-Merel

Step 1: Assume there is a counterexample $a^p + b^p = c^2$.

Step 1: Assume there is a counterexample $a^p + b^p = c^2$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)}\colon y^2 + xy = x^3 + \frac{c-1}{4}x^2 + \frac{a^p}{2^6}x$$

$$\Delta = \frac{1}{2^{12}}(a^2 b)^p$$

$$j = -\frac{2^6(3a^p - 4c^2)^3}{(a^2 b)^p}$$

if ab is even.

Template for the proof of Darmon-Merel

Step 1: Assume there is a counterexample $a^p + b^p = c^2$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$
\begin{aligned}
E_{(a,b,c)}\colon y^2 &= x^3 + 2cx^2 + a^p x \\
\Delta &= 2^6 (a^2 b)^p \\
j &= -\frac{2^6 (3a^p - 4c^2)^3}{(a^2 b)^p}
\end{aligned}
$$

if ab is odd.

Template for the proof of Darmon-Merel

Step 1: Assume there is a counterexample $a^p + b^p = c^2$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)}: \begin{cases} y^2 + xy = x^3 + \frac{c-1}{4}x^2 + \frac{a^p}{2^6}x & \text{if } ab \text{ is even} \\ y^2 = x^3 + 2cx^2 + a^p x & \text{if } ab \text{ is odd} \end{cases}$$

Template for the proof of Darmon-Merel

Step 1: Assume there is a counterexample $a^p + b^p = c^2$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)}: \begin{cases} y^2 + xy = x^3 + \frac{c-1}{4}x^2 + \frac{a^p}{2^6}x & \text{if } ab \text{ is even} \\ y^2 = x^3 + 2cx^2 + a^p x & \text{if } ab \text{ is odd} \end{cases}$$

Step 3: $E_{(a,b,c)}$ **has CM (complex multiplication)**.

Template for the proof of Darmon-Merel

Step 1: Assume there is a counterexample $a^p + b^p = c^2$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)}: \begin{cases} y^2 + xy = x^3 + \frac{c-1}{4}x^2 + \frac{a^p}{2^6}x & \text{if } ab \text{ is even} \\ y^2 = x^3 + 2cx^2 + a^p x & \text{if } ab \text{ is odd} \end{cases}$$

Step 3: $E_{(a,b,c)}$ **has CM (complex multiplication)**.
Step 4: There are only finitely many $E/\mathbb{Q}$ with CM (up to twists).

Template for the proof of Darmon-Merel

Step 1: Assume there is a counterexample $a^p + b^p = c^2$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)}: \begin{cases} y^2 + xy = x^3 + \frac{c-1}{4}x^2 + \frac{a^p}{2^6}x & \text{if } ab \text{ is even} \\ y^2 = x^3 + 2cx^2 + a^p x & \text{if } ab \text{ is odd} \end{cases}$$

Step 3: $E_{(a,b,c)}$ **has CM (complex multiplication)**.
Step 4: There are only finitely many $E/\mathbb{Q}$ with CM (up to twists).
Step 5: (Easy) Find all triples (a, b, c) such that $E_{(a,b,c)}$ has CM.

Generalized Fermat Equations

Fix $p, q, r \in \mathbb{N}$ such that $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

Fix $p, q, r \in \mathbb{N}$ such that $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

Theorem (Darmon, Granville 1995)

The equation

$$x^p + y^q = z^r$$

has only finitely many coprime solutions with $xyz \neq 0$.

Examples of Generalized Fermat Equations

$$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{7} - 1 = -\frac{1}{42} < 0$$

Examples of Generalized Fermat Equations

$$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{7} - 1 = -\frac{1}{42} < 0$$

Theorem (Poonen, Schaefer, Stoll 2008)

The coprime integer solutions to $x^2 + y^3 = z^7$ are the 16 triples

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113),$$
$$(\pm 21063928, -76271, 17).$$

Generalized Fermat Equations – Known Solutions

The 'known' solutions to the equation $x^p + y^q = z^r$ with $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$ and $xyz \neq 0$ are the following:

The 'known' solutions to the equation $x^p + y^q = z^r$ with $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$ and $xyz \neq 0$ are the following:

$$1^p + 2^3 = 3^2 \quad (-1)^{2p} + 2^3 = 3^2 \quad 2^5 + 7^2 = 3^4$$

$$7^3 + 13^2 = 2^9 \quad 2^7 + 17^3 = 71^2 \quad 3^5 + 11^4 = 122^2$$

$$17^7 + 76271^3 = 21063928^2 \quad 1414^3 + 2213459^2 = 65^7$$

$$9262^3 + 15312283^2 = 113^7 \quad 43^8 + 96222^3 = 30042907^2$$

$$33^8 + 1549034^2 = 15613^3$$

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman-Zagier)

This is a complete list of coprime non-zero solutions such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman-Zagier)

This is a complete list of coprime non-zero solutions such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

\$100,000 prize for proof of conjecture...

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman-Zagier)

This is a complete list of coprime non-zero solutions such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

$100,000 prize for proof of conjecture...

...or even for a counterexample.

(p, q, r) such that $\chi < 0$ and the solutions to $x^p + y^q = z^r$ have been determined.

$\{n, n, n\}$	Wiles, Taylor-Wiles, building on work of many others
$\{2, n, n\}$	Darmon-Merel, others for small n
$\{3, n, n\}$	Darmon-Merel, others for small n
$\{5, 2n, 2n\}$	Bennett
$(2, 4, n)$	Ellenberg, Bruin, Ghioca $n \geq 4$
$(2, n, 4)$	Bennett-Skinner; $n \geq 4$
$\{2, 3, n\}$	Poonen-Shaefer-Stoll, Bruin. $6 \leq n \leq 9$
$\{2, 2\ell, 3\}$	Chen, Dahmen, Siksek; primes $7 < \ell < 1000$ with $\ell \neq 31$
$\{3, 3, n\}$	Bruin; $n = 4, 5$
$\{3, 3, \ell\}$	Kraus; primes $17 \leq \ell \leq 10000$
$(2, 2n, 5)$	Chen $n \geq 3^*$
$(4, 2n, 3)$	Bennett-Chen $n \geq 3$
$(6, 2n, 2)$	Bennett-Chen $n \geq 3$
$(2, 6, n)$	Bennett-Chen $n \geq 3$

Main Theorem

$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{10} - 1 = -\frac{1}{15}$ is maximal among unsolved Fermat equations.

Main Theorem

$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{10} - 1 = -\frac{1}{15}$ is maximal among unsolved Fermat equations.

Theorem (B., 2011)

The only coprime integer solutions to the equation

$$x^2 + y^3 = z^{10}$$

are the 12 triples

$$(\pm 1, -1, 0), (\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 3, -2, \pm 1).$$

Main Theorem

$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{10} - 1 = -\frac{1}{15}$ is maximal among unsolved Fermat equations.

Theorem (B., 2011)

The only coprime integer solutions to the equation

$$x^2 + y^3 = z^{10}$$

are the 12 triples

$$(\pm 1, -1, 0), (\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 3, -2, \pm 1).$$

It is the first generalized Fermat equation of the form $x^2 + y^3 = z^n$ conjectured to have only trivial solutions.

$(3^2 + (-2)^3 = 1^n$ is considered to be trivial.)

Framework for solving $x^2 + y^3 = z^n$

Step 1: Assume there is a counterexample $a^2 + b^3 = c^n$.

Framework for solving $x^2 + y^3 = z^n$

Step 1: Assume there is a counterexample $a^2 + b^3 = c^n$.

Step 2: Study the elliptic curve

$$\begin{aligned} E_{(a,b,c)}: y^2 &= x^3 + 3bx - 2a \\ \Delta &= -12^3 c^n \\ j &= 12^3 b^3 / c^n. \end{aligned}$$

Framework for solving $x^2 + y^3 = z^n$

Step 1: Assume there is a counterexample $a^2 + b^3 = c^n$.

Step 2: Study the elliptic curve

$$\begin{aligned} E_{(a,b,c)}\colon y^2 &= x^3 + 3bx - 2a \\ \Delta &= -12^3 c^n \\ j &= 12^3 b^3 / c^n. \end{aligned}$$

Step 3: Explicitly classify possibilities for $\rho_{E_{(a,b,c)},n}$.

Framework for solving $x^2 + y^3 = z^n$

Step 1: Assume there is a counterexample $a^2 + b^3 = c^n$.

Step 2: Study the elliptic curve

$$\begin{aligned} E_{(a,b,c)}\colon y^2 &= x^3 + 3bx - 2a \\ \Delta &= -12^3 c^n \\ j &= 12^3 b^3 / c^n. \end{aligned}$$

Step 3: Explicitly classify possibilities for $\rho_{E_{(a,b,c)},n}$.

Step 4: For such ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

Framework for solving $x^2 + y^3 = z^n$

Step 1: Assume there is a counterexample $a^2 + b^3 = c^n$.

Step 2: Study the elliptic curve

$$\begin{aligned} E_{(a,b,c)}\colon y^2 &= x^3 + 3bx - 2a \\ \Delta &= -12^3 c^n \\ j &= 12^3 b^3 / c^n. \end{aligned}$$

Step 3: Explicitly classify possibilities for $\rho_{E_{(a,b,c)},n}$.

Step 4: For such ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

Step 5: For each such E, find all (a, b, c) such that $E \cong E_{(a,b,c)}$.

Framework for solving $x^2 + y^3 = z^n$

For large n, this template (conjecturally) works!

Step 3:

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},n}$.

Framework for solving $x^2 + y^3 = z^n$

For large n, this template (conjecturally) works!

Step 3:

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},n}$.

- For large n, there are 13 possibilities for $\rho_{E_{(a,b,c)},n}$, which are 'independent of n'.

Framework for solving $x^2 + y^3 = z^n$

For large n, this template (conjecturally) works!

Step 4:

For a fixed ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

Framework for solving $x^2 + y^3 = z^n$

For large n, this template (conjecturally) works!

Step 4:

For a fixed ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

- This would follow from a standard conjecture:

Framework for solving $x^2 + y^3 = z^n$

For large n, this template (conjecturally) works!

Step 4:

For a fixed ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

- This would follow from a standard conjecture:

Conjecture (Frey-Mazur)

Let $p > 23$ be a prime and E and E' be elliptic curves such that $\rho_{E,p} \cong \rho_{E',p}$. Then E is isogenous to E'.

Template breaks down for $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 3:

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},10}$.

Template breaks down for $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 3:

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},10}$.

- Known tools for classifying $\rho_{E_{(a,b,c)},10}$ fail.

Template breaks down for $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 3:

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},10}$.

- Known tools for classifying $\rho_{E_{(a,b,c)},10}$ fail.
  - E.g., Ribet's level lowering theorem fails for $n = 2$.

Template breaks down for $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)}\colon y^2 = x^3 + 3bx - 2a$$

Step 3:

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},10}$.

- Known tools for classifying $\rho_{E_{(a,b,c)},10}$ fail.
  - E.g., Ribet's level lowering theorem fails for $n = 2$.
  - $\rho_{E_{(a,b,c)},n}$ may be reducible for both $n = 2$ and 5.

Template breaks down for $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 3:

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},10}$.

- Known tools for classifying $\rho_{E_{(a,b,c)},10}$ fail.
  - E.g., Ribet's level lowering theorem fails for $n = 2$.
  - $\rho_{E_{(a,b,c)},n}$ may be reducible for both $n = 2$ and 5.

Definition

We say that $\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is *reducible* if there is some subspace $W \subset \mathbb{F}_\ell^2$ such that for every $P \in W$, $P^{\rho(\sigma)} \in W$.

Template breaks down forth $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 4:

For a fixed ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

Template breaks down forth $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 4:

For a fixed ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

- Using one prime is not enough.

Template breaks down forth $x^2 + y^3 = z^{10}$

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 4:

For a fixed ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

- Using one prime is not enough.
  - E.g., there are infinitely many elliptic curves over $\mathbb{Q}$ with trivial mod 2 representation ($E \colon y^2 = x(x-1)(x-\lambda)$).

Template breaks down forth $x^2 + y^3 = z^{10}$

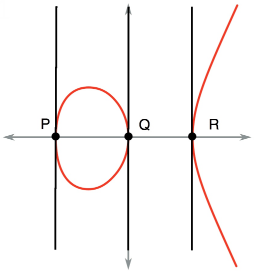
$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a$$

Step 4:

For a fixed ρ, classify **all** elliptic curves E for which $\rho_{E,n} \cong \rho$.

- Using one prime is not enough.
  - E.g., there are infinitely many elliptic curves over $\mathbb{Q}$ with trivial mod 2 representation ($E \colon y^2 = x(x-1)(x-\lambda)$).
- Multiprime approaches seem to be computationally infeasible.

Elliptic Curves – torsion



$$E[2](\mathbb{Q}) \cong \begin{cases} \{\infty\} & \text{if } f(x) \text{ has 0 rational roots} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } f(x) \text{ has 1 rational roots} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } f(x) \text{ has 3 rational roots} \end{cases}$$

Step 3: Classifying mod 2 Galois representations

Let E be given by the equation $y^2 = f(x) := x^3 + 3bx - 2a$

Fact

The splitting field of the polynomial $f(x)$ completely determines $\rho_{E,2}$.

Step 3: Classifying mod 2 Galois representations

Let E be given by the equation $y^2 = f(x) := x^3 + 3bx - 2a$

Fact

The splitting field of the polynomial $f(x)$ completely determines $\rho_{E,2}$.

- The splitting field K of $x^3 + 3bx - 2a$ is unramified outside of $\{2, 3\}$ and of degree at most 6.

Step 3: Classifying mod 2 Galois representations

Let E be given by the equation $y^2 = f(x) := x^3 + 3bx - 2a$

Fact

The splitting field of the polynomial $f(x)$ completely determines $\rho_{E,2}$.

- The splitting field K of $x^3 + 3bx - 2a$ is unramified outside of $\{2, 3\}$ and of degree at most 6.
- (Hermite) There are only finitely many such fields.

Step 3: Classifying mod 2 Galois representations

Let E be given by the equation $y^2 = f(x) := x^3 + 3bx - 2a$

Fact

The splitting field of the polynomial $f(x)$ completely determines $\rho_{E,2}$.

- The splitting field K of $x^3 + 3bx - 2a$ is unramified outside of $\{2, 3\}$ and of degree at most 6.
- (Hermite) There are only finitely many such fields.
- These days there are sophisticated algorithms for enumerating such K.

Step 3: Progress for $\ell = 2$

Lemma

There are elliptic curves $\{E_1, \ldots, E_n\}$ such that for every (a, b, c) such that $a^2 + b^3 = c^{10}$, there is an i such that

$$\rho_{E_{(a,b,c)},2} \cong \rho_{E_i,2}.$$

Step 3: Progress for $\ell = 2$

Lemma

There are elliptic curves $\{E_1, \ldots, E_n\}$ such that for every (a, b, c) such that $a^2 + b^3 = c^{10}$, there is an i such that

$$\rho_{E_{(a,b,c)},2} \cong \rho_{E_i,2}.$$

- **Wanted**: a similar lemma for $\rho_{E_{(a,b,c)},5}$.

Step 3: Progress for $\ell = 2$

Lemma

There are elliptic curves $\{E_1, \ldots, E_n\}$ such that for every (a, b, c) such that $a^2 + b^3 = c^{10}$, there is an i such that

$$\rho_{E_{(a,b,c)},2} \cong \rho_{E_i,2}.$$

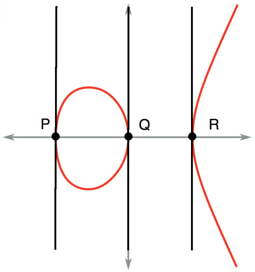
- **Wanted**: a similar lemma for $\rho_{E_{(a,b,c)},5}$.
- **Problem**: $\rho_{E_{(a,b,c)},5}$ may be reducible, thus modularity won't help!

Parameter spaces for Galois representations

Definition

$X_E(n)$ is the parameter space for pairs (E', ψ), where E' is an elliptic curve and $\psi\colon \rho_{E,n} \to \rho_{E',n}$ is a symplectic isomorphism of mod n Galois representations.

Elliptic Curves – torsion



$$E[2](\mathbb{Q}) \cong \begin{cases} \{\infty\} & \text{if } f(x) \text{ has 0 rational roots} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } f(x) \text{ has 1 rational roots} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } f(x) \text{ has 3 rational roots} \end{cases}$$

Parameter spaces for Galois representations

Definition

$X_E(n)$ is the parameter space for pairs (E', ψ), where E' is an elliptic curve and $\psi\colon \rho_{E,n} \to \rho_{E',n}$ is a symplectic isomorphism of mod n Galois representations.

Example

Let E be an elliptic curve with $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ (so that $\rho_{E,2}$ is trivial). Then E is of the form

$$E\colon y^2 = x(x-1)(x-\lambda).$$

Other parameter spaces

Recall that $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is *reducible* if there is some subspace $W \subset \mathbb{F}_\ell^2$ such that for every $P \in W$, $P^{\rho(\sigma)} \in W$.

Other parameter spaces

Recall that $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is *reducible* if there is some subspace $W \subset \mathbb{F}_\ell^2$ such that for every $P \in W$, $P^{\rho(\sigma)} \in W$.

Definition

$X_0(p)$ is the parameter space for elliptic curves such that $\rho_{E,p}$ is reducible (more precisely – pairs $(E, W \subset E[p])$, where E is an elliptic curve and W is an invariant subgroup of size p).

Other parameter spaces

Recall that $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is *reducible* if there is some subspace $W \subset \mathbb{F}_\ell^2$ such that for every $P \in W$, $P^{\rho(\sigma)} \in W$.

Definition

$X_0(p)$ is the parameter space for elliptic curves such that $\rho_{E,p}$ is reducible (more precisely – pairs $(E, W \subset E[p])$, where E is an elliptic curve and W is an invariant subgroup of size p).

Example ($X_0(5)$)

Let $E\colon y^2 = x^3 + 3bx - 2a$, and suppose $\rho_{E,5}$ is reducible. Then there exists a $t \in \mathbb{Z}$ such that

$$12^3 \frac{b^3}{a^2 + b^3} = \frac{(t^2 + 250t + 3125)^3}{t^5}.$$

Step 3: Intermediate Modular curves

Goal

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},5}$.

Step 3: Intermediate Modular curves

Goal

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},5}$.

$$\begin{tikzcd}
X(10) \arrow[rr] \arrow[dd] & & X(5) \arrow[d] \\
 & & X_0(5) \arrow[d] \\
X(2) \arrow[r, "\pi"] & X_0(2) \arrow[r] & X(1)
\end{tikzcd}$$

Step 3: Intermediate Modular curves

Goal

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},5}$.

$$\begin{tikzcd}
X(10) \arrow[rr] \arrow[dd] & & X(5) \arrow[d] \\
& & X_0(5) \arrow[d] \\
X(2) \arrow[r, "\pi"] & X_0(2) \arrow[r] & X(1)
\end{tikzcd}$$

- $\pi\colon (E, \psi\colon \rho_{\text{triv}} \cong \rho_{E,2}) \mapsto (E, W)$.

Step 3: Intermediate Modular curves: $p = 2$

- $\mathrm{Aut}(X(2)/X(1)) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

$$\begin{tikzcd} & X_0(2) \arrow[dr] & \\ X(2) \arrow[ur] \arrow[dr] & & X(1) \\ & X_\Delta \arrow[ur] & \end{tikzcd}$$

- $\mathrm{Aut}(X(2)/X(1)) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.
- $X_0(2)$ is the quotient of $X(2)$ by a transposition.

$$\begin{tikzcd} & X_0(2) \arrow[dr] & \\ X(2) \arrow[ur] \arrow[dr] & & X(1) \\ & X_\Delta \arrow[ur] & \end{tikzcd}$$

Step 3: Intermediate Modular curves: $p = 2$

- Define X_Δ to be the quotient of $X(2)$ by the normal subgroup A_3.

$$\begin{tikzcd} & X_0(2) \arrow[dr] & \\ X(2) \arrow[ur] \arrow[dr] & & X(1) \\ & X_\Delta \arrow[ur] & \end{tikzcd}$$

Step 3: Intermediate Modular curves: $p = 2$

- Define X_Δ to be the quotient of $X(2)$ by the normal subgroup A_3.
- X_Δ classifies pairs (E, z) such that $z^2 = j(E) - 12^3 = c_6(E)^2/\Delta_E$.

$$\begin{tikzcd} & X_0(2) \arrow[dr] & \\ X(2) \arrow[ur] \arrow[dr] & & X(1) \\ & X_\Delta \arrow[ur] & \end{tikzcd}$$

Goal

Explicitly classify possibilities for $\rho_{E_{(a,b,c)},5}$.

$$\begin{tikzcd}
X(10) \arrow[rr] \arrow[ddd] & & X(5) \arrow[d] \\
& & X_0(5) \arrow[dd] \\
& & \\
X(2) \arrow[r] & X_\Delta \arrow[r] & X(1)
\end{tikzcd}$$

Step 3: Intermediate Modular curves

$$\begin{tikzcd}
X(10) \arrow[rr] \arrow[dr, dashed] \arrow[dd] & & X(5) \arrow[d] \\
& X \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\
X(2) \arrow[r] & X_\Delta \arrow[r] & X(1)
\end{tikzcd}$$

Step 3: Intermediate Modular curves

$$\begin{tikzcd}
X(10) \arrow[rr] \arrow[dd] \arrow[dr, dashed] & & X(5) \arrow[d] \\
& X \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\
X(2) \arrow[r] & X_\Delta \arrow[r] & X(1)
\end{tikzcd}$$

- X classifies **triples** (E, W, z) such that
  - $z^2 = j(E) - 12^2 = c_4(E)^2/\Delta_E$,
  - W is an invariant subspace of $E[5]$ of order 5.

$$E_{(a,b,c)}\colon\ y^2 = x^3 + 3bx - 2a$$
$$\Delta = -12^3 c^{10} = -3(2^3 \cdot 3 \cdot c^5)^2$$

$$\begin{tikzcd} X \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\ X_\Delta \arrow[r] & X(1) \end{tikzcd}$$

Step 3: Intermediate Modular curves

$$E_{(a,b,c)}\colon y^2 = x^3 + 3bx - 2a$$
$$\Delta = -12^3 c^{10} = -3(2^3 \cdot 3 \cdot c^5)^2$$

$$\begin{array}{ccc} X_{(-3)} & \longrightarrow & X_0(5) \\ \downarrow & & \downarrow \\ X_{(-3\Delta)} & \longrightarrow & X(1) \end{array}$$

Step 3: Intermediate Modular curves

$$E_{(a,b,c)}\colon y^2 = x^3 + 3bx - 2a$$
$$\Delta = -12^3 c^{10} = -3(2^3 \cdot 3 \cdot c^5)^2$$

$$\begin{tikzcd} X_{(-3)} \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\ X_{(-3\Delta)} \arrow[r] & X(1) \end{tikzcd}$$

- $X_{(-3)}$ classifies **triples** (E, W, z) such that
    - $-3z^2 = c_4(E)^2/\Delta_E$,
    - W is an invariant subspace of $E[5]$ of order 5.

Step 3: Intermediate Modular curves

$$E_{(a,b,c)}\colon y^2 = x^3 + 3bx - 2a$$
$$\Delta = -12^3 c^{10} = -3(2^3 \cdot 3 \cdot c^5)^2$$

$$\begin{tikzcd}
X_{(-3)} \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\
X_{(-3\Delta)} \arrow[r] & X(1)
\end{tikzcd}$$

- Reducible $\rho_{E_{(a,b,c)},5}$ thus give rise to a point on $X_{(-3)}(\mathbb{Q})$.

Step 3: Intermediate Modular curves

$$E_{(a,b,c)}\colon y^2 = x^3 + 3bx - 2a$$
$$\Delta = -12^3 c^{10} = -3(2^3 \cdot 3 \cdot c^5)^2$$

$$\begin{tikzcd} X_{(-3)} \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\ X_{(-3\Delta)} \arrow[r] & X(1) \end{tikzcd}$$

- Reducible $\rho_{E_{(a,b,c)},5}$ thus give rise to a point on $X_{(-3)}(\mathbb{Q})$.
- $X_{(-3)}$ turns out to be an elliptic curve, with $X_{(-3)}(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

Step 3: Classifying $\rho_{E_{(a,b,c)},\ell}$

Lemma

There are elliptic curves $\{E_1, \ldots, E_n\}$ *and* $\{E'_1, \ldots, E'_{n'}\}$ *such that for every* (a, b, c) *such that* $a^2 + b^3 = c^{10}$*, there exists an* i *and* j *such that*

$$\rho_{E_{(a,b,c)},2} \cong \rho_{E_i,2}$$

and

$$\rho_{E_{(a,b,c)},5} \cong \rho_{E'_j,5}.$$

Step 3: Classifying $\rho_{E_{(a,b,c)},\ell}$

Lemma

There are elliptic curves $\{E_1, \ldots, E_n\}$ *and* $\{E'_1, \ldots, E'_{n'}\}$ *such that for every* (a, b, c) *such that* $a^2 + b^3 = c^{10}$*, there exists an* i *and* j *such that*

$$\rho_{E_{(a,b,c)},2} \cong \rho_{E_i,2}$$

and

$$\rho_{E_{(a,b,c)},5} \cong \rho_{E'_j,5}.$$

Thus, $E_{(a,b,c)}$ gives rise to a point on $X_{E_i}(2)(\mathbb{Q})$ and a point on $X_{E'_j}(5)(\mathbb{Q})$.

Step 4: Classify elliptic curves with a given pair of Galois representations

Thus, $E_{(a,b,c)}$ gives rise to a point on $X_{E_i}(2)(\mathbb{Q})$ and a point on $X_{E'_j}(5)(\mathbb{Q})$.

Step 4:

For a fixed i, j, classify **all** elliptic curves E for which $\rho_{E,2} \cong \rho_{E_i,2}$ and $\rho_{E,5} \cong \rho_{E'_j,2}$.

Step 4: Elliptic Chabauty

$$
\begin{tikzcd}
X_{E_i,E'_j}(10) \arrow[rr] \arrow[dr, dashed, "/K_{E'_j}"'] \arrow[dd] & & X_{E'_j}(5) \arrow[d, "/K_{E'_j}"] \\
& X_{E_i} \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\
X_{E_i}(2) \arrow[r] & X_{\Delta_{E_i}} \arrow[r] & X(1)
\end{tikzcd}
$$

Step 4: Elliptic Chabauty

$$
\begin{tikzcd}
X_{E_i,E'_j}(10) \arrow[rr] \arrow[dr, dashed, "/K_{E'_j}"'] \arrow[dd] & & X_{E'_j}(5) \arrow[d, "/K_{E'_j}"] \\
 & X_{E_i} \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\
X_{E_i}(2) \arrow[r] & X_{\Delta_{E_i}} \arrow[r] & X(1)
\end{tikzcd}
$$

- For every coprime (a, b, c) such that $a^2 + b^3 = c^{10}$, we can find some E_i, E'_j and a point on $P \in X_{E_i}(K_{E'_j})$ such that $j(P) \in X(1)(\mathbb{Q})$.

Step 4: Elliptic Chabauty

$$\begin{tikzcd}
X_{E_i,E_j'}(10) \arrow[rr] \arrow[dd] \arrow[dr, dashed, "/K_{E_j'}"'] & & X_{E_j'}(5) \arrow[d, "/K_{E_j'}"] \\
& X_{E_i} \arrow[r] \arrow[d] & X_0(5) \arrow[d] \\
X_{E_i}(2) \arrow[r] & X_{\Delta_{E_i}} \arrow[r] & X(1)
\end{tikzcd}$$

- For every coprime (a, b, c) such that $a^2 + b^3 = c^{10}$, we can find some E_i, E_j' and a point on $P \in X_{E_i}(K_{E_j'})$ such that $j(P) \in X(1)(\mathbb{Q})$.
- This latter set is finite, and in fact *computable* (via p-adic integration and other methods).

Conclusion: New ideas for $x^2 + y^3 = z^{10}$

The template fails for $x^2 + y^3 = z^{10}$.

1) Known tools for classifying $\rho_{E_{(a,b,c)},\ell}$ fail for $\ell = 2, 5$.

Conclusion: New ideas for $x^2 + y^3 = z^{10}$

The template fails for $x^2 + y^3 = z^{10}$.

1) Known tools for classifying $\rho_{E_{(a,b,c)},\ell}$ fail for $\ell = 2, 5$.
   - New idea: supplement classical classification techniques with number field enumeration and non-traditional parameter spaces.

Conclusion: New ideas for $x^2 + y^3 = z^{10}$

The template fails for $x^2 + y^3 = z^{10}$.

1) Known tools for classifying $\rho_{E_{(a,b,c)},\ell}$ fail for $\ell = 2, 5$.
    - New idea: supplement classical classification techniques with number field enumeration and non-traditional parameter spaces.
2) Its not enough to classify only the mod 2 or the mod 5 representation.

Conclusion: New ideas for $x^2 + y^3 = z^{10}$

The template fails for $x^2 + y^3 = z^{10}$.

1) Known tools for classifying $\rho_{E_{(a,b,c)},\ell}$ fail for $\ell = 2, 5$.
   - New idea: supplement classical classification techniques with number field enumeration and non-traditional parameter spaces.
2) Its not enough to classify only the mod 2 or the mod 5 representation.
3) Classifying both the mod 2 and mod 5 at the same time leads to 'high genus parameter spaces'.

Conclusion: New ideas for $x^2 + y^3 = z^{10}$

The template fails for $x^2 + y^3 = z^{10}$.

1) Known tools for classifying $\rho_{E_{(a,b,c)},\ell}$ fail for $\ell = 2, 5$.
    - New idea: supplement classical classification techniques with number field enumeration and non-traditional parameter spaces.
2) Its not enough to classify only the mod 2 or the mod 5 representation.
3) Classifying both the mod 2 and mod 5 at the same time leads to 'high genus parameter spaces'.
    - New idea: translate the work to low genus parameter spaces, but over larger number fields than $\mathbb{Q}$.