Fermat's Last Theorem and Modular Curves over Real Quadratic Fields

Philippe Michaud-Rodgers

University of Warwick

Seminar on Number Theory and Algebra - University of Zagreb
17.05.2021

Table of Contents

Table of Contents

Statement of Fermat's Last Theorem over $\mathbb{Q}$

Theorem (Wiles + many others! 1995)

The equation

$$x^n + y^n = z^n,$$

with $n \geq 3$, has no non-trivial solutions for integers x, y, z.

A **non-trivial** solution means $xyz \neq 0$.
(We can also replace 'integers' by 'rationals').

Generalising to Number Fields

What happens if we replace the word integers by $\mathcal{O}_K$, for K a number field?

Question

Let K be a number field. Does the equation

$$a^n + b^n = c^n,$$

with $n \geq 3$, have non-trivial solutions for $a, b, c \in \mathcal{O}_K$?

(We can also replace '$\mathcal{O}_K$' by 'K').

- Does this exact statement always hold?
- For which number fields K, and for which exponents n might it hold?
- How might we prove such statements?

Outline of Talk

- Overview the proof of FLT over $\mathbb{Q}$.
- Try to use the same proof over a **real quadratic field** $K = \mathbb{Q}(\sqrt{d})$.
- Understand main difficulties and see how **modular curves** play a role.

[Slides available on my webpage.]

Table of Contents

First Observations

- If $n = p \cdot m$ and (x, y, z) satisfies $x^n + y^n = z^n$, then
$$(x^m)^p + (y^m)^p = (z^m)^p.$$
- $n = 3$ (Euler, 1770) and $n = 4$ (Fermat, 1670): elementary.

So enough to prove:

FLT

The equation
$$x^p + y^p = z^p,$$
with $p \geq 5$, prime, has no (non-trivial) solutions for integers x, y, z.

Elliptic Curves

An elliptic curve over $\mathbb{Q}$ is a curve given by an equation

$$Y^2 = X^3 + AX^2 + BX + C,$$

where $A, B, C \in \mathbb{Q}$. It is smooth.

- E has a minimal discriminant, $\Delta_{\min}$.
- If $p \nmid \Delta_{\min}$ then $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$; the 'trace of Frobenius at p'.
- E has a conductor

$$N_E := \prod_{p \mid \Delta_{\min}} p^{e_p}, \qquad (e_p \geq 1).$$

- If N is squarefree, E is called semistable.

Newforms

A newform of level N' is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$, where $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{im}(z) > 0\}$ is the upper half-plane.

- f has a **Fourier** or q-**expansion**:

$$f = \sum_{n=1}^{\infty} a_n q^n, \text{ where } a_n \in L, q = e^{\frac{2\pi i}{z}}, z \in \mathcal{H}.$$

- There are finitely many newforms at each level N'.
- **Example**. There are two newforms at level 38:

$$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \cdots$$
$$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \cdots$$

- No newforms at level 2.

The Frey Curve

FLT

The equation $x^p + y^p = z^p$, with $p \geq 5$, prime, has no non-trivial solutions for integers x, y, z.

Suppose (x, y, z) (with x, y, z pairwise coprime) is a non-trivial solution.
Associate to (x, y, z) the Frey Curve

$$E_{x,y,z,p} : Y^2 = X(X - x^p)(X + y^p).$$

This is an elliptic curve $/\mathbb{Q}$.

- $\#E(\mathbb{Q})[2] = 4$.
- $\Delta_{\mathrm{min}} = 2^{-8}(xyz)^{2p}$.
- $N = 2\prod_{p|xyz,\mathrm{odd}} p$, squarefree.

Level-Lowering

Level-Lowering Theorem (Ribet)

Let E be a modular elliptic curve over $\mathbb{Q}$ of conductor N and let $p \geq 5$ be prime. Suppose $\overline{\rho}_{E,p}$ is irreducible. Then E arises mod p from a newform f at level N_p, where

$$N_p = \frac{N}{\prod_{q \| N, p \mid \mathrm{ord}_q(\Delta_{\min})} q}.$$

- W + B + C + D +T: Elliptic curves over $\mathbb{Q}$ are modular.

Arises mod p

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.
- Let $f = \sum a_n q^n$ be a newform of level N'.

Definition

Let p be a prime. We say E arises modulo p from f if for all primes $l \nmid pNN'$,

$$a_l(f) \equiv a_l(E) \pmod{p}.$$

Mazur's Theorem

Condition in Level-Lowering Theorem: Suppose $\overline{\rho}_{E,p}$ is irreducible.

- $\overline{\rho}_{E,p}$ is the **mod-p Galois representation** associated to E.

The following conditions are equivalent:

- $\overline{\rho}_{E,p}$ is reducible.
- E has a rational cyclic subgroup of size p.
- E admits a rational p-isogeny.

Mazur's Theorem

Let $E/\mathbb{Q}$ be a semistable elliptic curve with $\#E(\mathbb{Q})[2] = 4$. Then $\overline{\rho}_{E,p}$ is irreducible for $p \geq 5$.

This holds for our Frey curve $E_{x,y,z,p}$.

Level-Lowering the Frey Curve

- We level-lower: E arises mod p from a newform f at level N_p.
- Here
$$N_p = \frac{N}{\prod_{q \| N, p \mid \mathrm{ord}_q(\Delta_{\min})} q} = 2,$$
which is no longer dependent on the solution (x, y, z).
- But! There are no newforms at level 2, contradiction.
- Conclusion: Fermat's Last Theorem is true.

Table of Contents

What changes over a number field?

Fix a real quadratic field $K = \mathbb{Q}(\sqrt{d})$. Does the equation

$$a^p + b^p = c^p,$$

with $p \geq 5$, have (non-trivial) solutions for $a, b, c \in \mathcal{O}_K$?

- Same general method: level-lower a Frey curve.
- Frey curve $E_{a,b,c,p} : Y^2 = X(X - a^p)(X + b^p)$, now $/K$.
  Conductor $\mathcal{N}$ is an ideal of $\mathcal{O}_K$.
  Values $a_p(E) \rightsquigarrow a_{\mathfrak{p}}(E)$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.
- Newform of level $N' \rightsquigarrow$ Hilbert newform of level $\mathcal{N}'$.
  Values $a_p(f) \rightsquigarrow a_{\mathfrak{p}}(\mathfrak{f})$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.

Three Main Issues

We have an analogue of the level-lowering theorem. There are three main issues.

- Modularity. To level-lower, E must be modular. Elliptic curves over real quadratic fields are modular (Freitas, Le Hung, Siksek, 2013). ✓
- Irreducibility. To level-lower, $\overline{\rho}_{E,p}$ must be irreducible.
- Newforms. Need to **calculate** and **eliminate** Hilbert newforms appearing at level $\mathcal{N}_p$ (over $\mathbb{Q}$ there were none at level $N_p = 2$; contradiction right away).

Focus for the rest of the talk: irreducibility.

Table of Contents

The Modular Curve $X_0(p)$

- $\Gamma_0(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{p} \right\}$.
- As a compact Riemann surface: $X_0(p) = \Gamma_0(p) \backslash \mathcal{H} + \{\infty, 0\}$.
- Obtain $X_0(p)$ as an algebraic curve $/\mathbb{Q}$ with $0, \infty \in X_0(p)(\mathbb{Q})$.
- **Example.** The modular curve $X_0(31)$ is a hyperelliptic curve. Here is a model $/\mathbb{Q}$:

$$y^2 = x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3.$$

- **Example.** The modular curve $X_0(43)$ is a curve of genus 3. It admits the following plane quartic model in $\mathbb{P}^3$:

$$64X^4 + 48X^3Y + 16X^2Y^2 + 8XY^3 - 3Y^4 + (16X^2 + 8XY + 2Y^2)T^2 + T^4 = 0.$$

From Irreducibility to Modular Curves

$X_0(p)$ parametrises elliptic curves with cyclic subgroups of size p.

- Let E/K be an elliptic curve and let C be a K-rational cyclic subgroup of E of size p. Then $[(E, C)] \in X_0(p)(K)$ is a non-cuspidal K-rational point.

So $\overline{\rho}_{E,p}$ reducible $\Rightarrow$ E has a K-rational cyclic subgroup of size p $\Rightarrow$ $E \rightsquigarrow x \in X_0(p)(K)$, a non-cuspidal K-rational point.

- If $X_0(p)(K)$ has no points that come from the Frey curve E, then $\overline{\rho}_{E,p}$ is irreducible.

Example. Let $E/\mathbb{Q}(\sqrt{26})$. Is $\overline{\rho}_{E,31}$ irreducible? Yes, since $X_0(31)(\mathbb{Q}(\sqrt{26})) = \{(1:1:0),(1:-1:0)\} = \{\infty, 0\}$, the two cusps.

Quadratic Points on Modular Curves

Definition

We say $x \in X_0(p)$ is a **quadratic point** if $x \in X_0(p)(K)$ for some quadratic field K. Quadratic points come in pairs: (x, x^σ).

Note. $X_0(31)$ has infinitely many quadratic points (as K ranges over all quadratic fields), but finitely many over a fixed quadratic field.

Two basic types of quadratic points (x, x^σ) on $X_0(p)$:

- either $w_p(x) = x^\sigma$;
- or $w_p(x) \neq x^\sigma$,

where w_p, which is defined $/\mathbb{Q}$, is the **Atkin-Lehner involution** on $X_0(p)$.

For $p < 80$ say, we can study quadratic points using a model of $X_0(p)$. But, we want to study all p!

We need to use properties of the Frey curve.

Primes of multiplicative reduction

Theorem (Najman and Turcas ($p > 71$) 2020, M. 2021)

Let $p > 19$, $p \neq 37$. Let E/K. Let q, with $q > 5$, $q \neq p$, be a rational prime that does not split in K, such that the unique prime of K above q is of multiplicative reduction for E. Then $\overline{\rho}_{E,p}$ is irreducible.

Conclusion. Knowing a non-split prime of multiplicative reduction for E allows us to bound p.

Idea. If $\overline{\rho}_{E,p}$ is reducible then $E \rightsquigarrow x, x^\sigma \in X_0(p)(K)$. Reduce mod q:

$$X_0(p) \longrightarrow \widetilde{X}_0(p)$$
$$x, x^\sigma \longmapsto \widetilde{\infty}, \widetilde{\infty} \text{ or } \widetilde{0}, \widetilde{0}.$$

This is a very restrictive condition! (Obtain contradiction using Eisenstein quotient and formal immersions.)

Problem. Conductor of Frey curve depends on solution. Cannot find (non-split) primes of multiplicative reduction...

Primes of Good Reduction

Write ϵ for the fundamental unit of K and $n_{\mathfrak{q}}$ for the norm of $\mathfrak{q}$.

Theorem (Freitas–Siksek, 2015)

Let $p \geq 17$ be prime, let E/K and let $\mathfrak{q} \mid q$ be a prime of good reduction for E, with $q \neq p$. Let $r_{\mathfrak{q}} = 1$ if $\mathfrak{q}$ is principal and $r_{\mathfrak{q}} = 2$ otherwise. Let

$$R_{\mathfrak{q}} := \mathrm{lcm}\{\mathrm{Res}(X^2 - aX + n_{\mathfrak{q}}, X^{12 r_{\mathfrak{q}}} - 1) : a \in \mathcal{A}_{\mathfrak{q}}\},$$

where $\mathcal{A}_{\mathfrak{q}} = \{a \in \mathbb{Z} : |a| \leq 2\sqrt{n_{\mathfrak{q}}}, \quad n_{\mathfrak{q}} + 1 - a \equiv 0 \pmod 4\}$. If $p \nmid \Delta_K \cdot \mathrm{Norm}(\epsilon^{12} - 1) \cdot R_{\mathfrak{q}}$ then $\overline{\rho}_{E,p}$ is irreducible.

Conclusion. Knowing a prime of good reduction for E allows us to bound p. Good bound using many $\mathfrak{q}$ and taking GCD.
Problem. Conductor of Frey curve depends on solution. Cannot find primes of good reduction... But...

Combining the two

We know which primes $\mathfrak{q}$ are of **semistable** reduction for E, i.e. primes which are either of good reduction *or* of multiplicative reduction (even if we don't know which).
Combine both theorems to obtain a bound (take the union).

Example. $E/\mathbb{Q}(\sqrt{26})$. If $\mathfrak{q} \nmid 2, 5$ then it is of semistable reduction for E. Use non-split primes $\mathfrak{q}$ with $7 \leq n_{\mathfrak{q}} \leq 10000$. Conclude $\overline{\rho}_{E,p}$ is irreducible unless $p \leq 19$ or $p \in \{37, 101, 103\}$.

How can we deal with leftover primes?

For a fixed prime p, we *can* (usually) obtain split primes of multiplicative reduction.

Split primes of multiplicative reduction

Theorem (M. 2021)

Let $p > 19$, $p \neq 37$. Let E/K. Let q, with $q > 5$, $q \neq p$, be a rational prime that splits in K, such that both prime of K above q are of multiplicative reduction for E. Suppose that in $X_0(p)(K)$, $w_p(x) \neq x^\sigma$ for any pair x, x^σ. Then $\overline{\rho}_{E,p}$ is irreducible.

Why is the split case different?

$$X_0(p) \longrightarrow \widetilde{X}_0(p)$$
$$x, x^\sigma \longmapsto \widetilde{\infty}, \widetilde{\infty} \text{ or } \widetilde{0}, \widetilde{0} \text{ or } \widetilde{0}, \widetilde{\infty} \text{ or } \widetilde{\infty}, \widetilde{0}.$$

Proof uses *Relative Symmetric Chabauty*.

Example. $E/\mathbb{Q}(\sqrt{26})$. Is $\overline{\rho}_{E,103}$ irreducible? Both primes of $\mathbb{Q}(\sqrt{26})$ above 1031 are of multiplicative reduction for E. We find that no pairs of quadratic points in $X_0(103)(\mathbb{Q}(\sqrt{26}))$ are interchanged by w_{103}. Conclusion: $\overline{\rho}_{E,103}$ is irreducible.

Table of Contents

Previous Results

Theorem (Jarvis and Meekin, 2003)

The equation

$$x^n + y^n = z^n, \quad x, y, z \in K,$$

has no non-trivial solutions for $n \geq 4$ *and* $K = \mathbb{Q}(\sqrt{2})$.

For $K = \mathbb{Q}(\sqrt{2})$ the Frey curve is semistable; closer to rational case.

Theorem (Freitas and Siksek, 2014)

The equation

$$x^n + y^n = z^n, \quad x, y, z \in K,$$

has no non-trivial solutions for $n \geq 4$ *and* $K = \mathbb{Q}(\sqrt{d})$, *when* $d \in \{3, 6, 7, 10, 11, 13, 14, 15, 19, 21, 22, 23\}$.

Fewer irreducibility results needed. No issues computing newforms.

Results

Theorem (M. 2021)

The equation

$$x^n + y^n = z^n, \quad x, y, z \in K,$$

has no non-trivial solutions for $n \geq 4$ *and* $K = \mathbb{Q}(\sqrt{d})$*, when* $d \in \{26, 29, 30, 31, 35, 37, 38, 42, 43, 46, 47, 51, 53, 58, 59, 61, 62, 65, 66, 67, 69, 71, 73, 74, 77, 79, 82, 83, 85, 86, 87, 91, 93, 94, 97\}$.

Partial results obtained for some other $26 \leq d \leq 97$.
No results obtained for $d = 39, 70, 78, 95$.
Main new tools:

- New irreducibilty methods.
- Avoiding computation of newforms.

Hope to use methods developed to solve other Diophantine equations; both over the rationals and over number fields.

Thank you for listening! :)