Isogenies of elliptic curves and Diophantine equations

Philippe Michaud-Jacobs

University of Warwick

Seminar on Number Theory and Algebra University of Zagreb 3rd May 2023

Results

Proofs 0000000000 Examples 0000

Section 1

Motivation

Motivation 000000		Results 000	Proofs ocococococo	Examples 0000	
	Fermat's Last Th	eorem			
	The equation				
	$x^n + y^n = z^n,$				
	with $n \ge 3$, has no solutions for $x, y, z \in \mathbb{Z}$ with $xyz \ne 0$.				

Proof.

- 1. Classical for $n \in \{3, 4\}$.
- 2. Let $n = p \ge 5$ be prime and suppose $x^p + y^p = z^p$ with $xyz \ne 0$.
- 3. Define the **Frey** elliptic curve $E : Y^2 = X(X x^p)(X + y^p)$.
- 4. E does not admit a rational p-isogeny (Mazur's isogeny thm).
- 5. E is a modular elliptic curve (Wiles' modularity thm).
- 6. *E* 'corresponds' to a newform at level 2 (*Ribet's level-lowering thm*) → contradiction.

Examples 0000

Mazur's isogeny theorem, 1978

Let p be a prime such that there exists an elliptic curve E/\mathbb{Q} that admits a rational p-isogeny. Then

```
p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.
```

Why is this an important theorem?

- Isogenies are the basic building blocks of maps between elliptic curves.
- It's proof introduced many important concepts and techniques.
- Leads to a deeper understanding of **modular curves** and **Galois representations**.
- Plays a crucial role in the modular method.

Key question: Does this theorem generalise to number fields?

Results

Proofs 0000000000 Examples 0000

Let E_1, E_2 be elliptic curves over a number field K.

- An isogeny between elliptic curves is a non-constant morphism $\varphi: E_1 \to E_2$ that induces a group homomorphism.
- The degree of an isogeny is the size of its kernel. If φ has prime degree p, we say it is a p-isogeny.
- An isogeny is *K*-rational if it can be expressed using rational functions with coefficients in *K*.

Example.

$$E_1: Y^2 = X^3 + X^2 - X, \quad E_2: Y^2 = X^3 - 2X^2 + 5X.$$
$$\varphi: (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 + 1)}{x^2}\right).$$

 $\ker(\varphi) = \{\mathbf{0}_{E_1}, (\mathbf{0}, \mathbf{0})\}$, it is a (Q-)rational 2-isogeny.

Motivation
0000000

Question

Let K be a number field. For which primes p does there exist an elliptic curve E/K admitting a K-rational p-isogeny?

This is an **open problem** for any given number field other than \mathbb{Q} .

Why is this an important question?

- Isogenies are the basic building blocks of maps between elliptic curves.
- An answer would lead to a deeper understanding of **modular curves** and **Galois representations**.
- An answer would lead to a simpler application of the **modular method over number fields**.

Examples 0000

The modular method over number fields

• Start with an equation:

$$\begin{aligned} x^p + y^p &= z^p, \quad \text{for } x, y, z \in \mathcal{K}. \\ x^{2p} + y^{2p} &= z^7, \quad \text{for } x, y, z \in \mathbb{Z}. \\ x^{2p} + 6x^p + 1 &= 8y^2, \quad \text{for } x, y \in \mathbb{Z}. \end{aligned}$$

- Write down a Frey elliptic curve E/K.
- Prove that *E* is modular.
- Prove that *E* does not admit a *K*-rational *p*-isogeny.
- Apply a level-lowering theorem to obtain a contradiction.

No set method for proving that E does not admit a K-rational p-isogeny.

Examples 0000

Aims and concessions

Aims:

- Obtain general results to help solve Diophantine equations using the modular method over number fields.
- Understand more about isogenies of elliptic curves.
- Understand more about modular curves and Galois representations.

Concessions:

• Assume E/K is semistable at all primes of K above p.

If E/K is an elliptic curve and $\mathfrak{p} \mid p$ is a prime of K, then E is semistable at \mathfrak{p} if E has good or multiplicative reduction at \mathfrak{p} .

- This is not a very restrictive assumption.
- It is *already* an assumption in the modular method for the level-lowering theorem.

Results

Proofs 0000000000 Examples 0000

Section 2

Results

Proofs 0000000000 Examples 0000

We will work with quadratic fields.

- Most useful for applications of the modular method.
- More techniques available.
- Sharper results are more easily obtained.

Theorem (M., 2022)

Let $K = \mathbb{Q}(\sqrt{5})$ and let p be a prime. There exists an elliptic curve E/K which admits a K-rational p-isogeny and is semistable at all primes of K above p if and only if $p \in \{2, 3, 5, 7, 13, 17, 37\}$.

Theorem (M., 2022)

Let $K = \mathbb{Q}(\sqrt{-5})$ and let p be a prime. There exists an elliptic curve E/K which admits a K-rational p-isogeny and is semistable at all primes of K above p if and only if $p \in \{2, 3, 5, 7, 13, 37, 43\}$.

Results

Proofs 0000000000 Examples 0000

Theorem (M., 2023)

Let K be a real quadratic field with $h(K) \le 7$ and let ϵ be a fundamental unit of K. Let p be a prime such that there exists an elliptic curve E/K which admits a K-rational p-isogeny and is semistable at all primes of K above p. Then either

(ii)
$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$$
; or

(iii) p splits in K and $p \mid \operatorname{Norm}_{K/\mathbb{Q}}(\epsilon^{12} - 1)$.

- This gives a simple criterion for ruling out primes.
- Any leftover primes can normally be dealt with separately.

Results

Proofs ●000000000

Examples 0000

Section 3

Proofs

Proofs ○●○○○○○○○○ Examples 0000

Modular curves and Galois representations

Let E/K be an elliptic curve that admits a K-rational p-isogeny, φ .

Strategy:

- Choose $\mathfrak{q} \nmid p$ a prime (of K).
- Case (i): q is a prime of *potentially multiplicative reduction* for E (meaning v_q(j(E)) < 0). Use the theory of modular curves.
- Case (ii): q is a prime of *potentially good reduction for E* (meaning vq(j(E)) ≥ 0). Use the theory of Galois representations.

Results

Proofs 00●0000000 Examples 0000

The modular curve $X_0(p)$

Let E/K be an elliptic curve that admits a K-rational p-isogeny, φ .

The curve $X_0(p)$ is an algebraic curve defined over \mathbb{Q} whose points parametrise elliptic curves with a *p*-isogeny.

The pair (E, φ) gives rise to a non-cuspidal *K*-rational point on the modular curve $X_0(p)$:

$$[E,\varphi] = x \in X_0(p)(K) \setminus \{0,\infty\}.$$

- We have the *j*-map $j : X_0(p) \longrightarrow \mathbb{P}^1$ that satisfies j(x) = j(E).
- The cusps $0, \infty \in X_0(p)(\mathbb{Q})$ are the poles of the *j*-map.

Proofs 000●000000

A prime of potentially multiplicative reduction

Let E/K be an elliptic curve that admits a K-rational p-isogeny, $\varphi.$ We have

 $[E,\varphi] = x \in X_0(p)(K) \setminus \{0,\infty\}.$

We know j(x) = j(E).

Suppose $q \nmid p$ is a prime of potentially multiplicative reduction for E (this is Case (i)).

•
$$v_{\mathfrak{q}}(j(E)) = v_{\mathfrak{q}}(j(x)) < 0.$$

- So x (mod q) is a pole of the *j*-map mod q.
- $x \pmod{\mathfrak{q}} = \infty \pmod{\mathfrak{q}}$ or $0 \pmod{\mathfrak{q}}$.
- Argue that $x = \infty$ or 0, a contradiction (think of **Hensel's** lemma!).

Examples 0000

The mod p Galois representation

Let E/K be an elliptic curve and p a prime. Write $E[p] \subset E(\overline{K})$ for the *p*-torsion points of *E*.

The group $G_{\mathcal{K}} = \operatorname{Gal}(\overline{\mathcal{K}}/\mathcal{K})$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ and gives rise to the **mod** p **Galois representation attached to** E:

$$\overline{\rho}_{E,p}: \mathcal{G}_{\mathcal{K}} \to \mathrm{GL}_2(\mathbb{F}_p).$$

Fix a basis (R_1, R_2) of E[p]. For $\sigma \in G_K$,

$$\begin{split} R_1^\sigma &= aR_1 + bR_2, \\ R_2^\sigma &= cR_1 + dR_2. \end{split}$$

Then $\overline{\rho}_{E,p}(\sigma) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

Results

Proofs 0000000000 Examples 0000

A key equivalence

Let E/K be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a K-rational p-isogeny, φ .
- (ii) $\overline{\rho}_{E,p}: \mathcal{G}_{\mathcal{K}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is reducible.

Proof.

(i)
$$\implies$$
 (ii) ker(φ) is a nontrivial proper G_K -submodule of $E[p]$.

(ii)
$$\implies$$
 (i) For some basis $\{R_1, R_2\} \subset E[p]$,

$$\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix} \right).$$

Then $\langle R_1 \rangle \subset E[p]$ is a *K*-rational subgroup of order *p*. Quotienting out by this subgroup gives rise to a *K*-rational *p*-isogeny.

Results

Proofs 0000000000 Examples 0000

The isogeny character

Let E/K be an elliptic such that $\overline{\rho}_{E,p}$ is reducible. So

$$\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right).$$

The isogeny character

 $\lambda: G_{\mathcal{K}} \to \mathbb{F}_{p}^{\times}$ is the **isogeny character** of (E, φ) .

• λ tells us how G_K acts on ker (φ) : if ker $(\varphi) = \langle R_1 \rangle$, then for $\sigma \in G_K$,

$$R_1^{\sigma} = \lambda(\sigma) R_1.$$

We study λ as it encodes key information about E and φ .

Proofs 0000000●00 Examples 0000

The group G_K and Frobenius elements

We want to study $\lambda : G_K \to \mathbb{F}_p^{\times}$. The group G_K is complicated and we want to work with concrete elements.

Let q be a prime of K and let $\sigma_q \in G_K$ be a **Frobenius element** at q. This is any element that maps to the Frobenius automorphism in $\operatorname{Gal}(\overline{k}/k)$, where $k = \mathcal{O}_K/q$.

We study $\lambda(\sigma_{\mathfrak{q}}) \in \mathbb{F}_{p}^{\times}$.

Examples 0000

A prime of potentially good reduction

Let E/K be an elliptic such that $\overline{\rho}_{E,p}$ is reducible and is semistable at the primes of K above p.

Suppose $q \nmid p$ is a prime of potentially good reduction for E (this is Case (ii)). Choose r such that $q^r = \alpha \mathcal{O}_K$ is principal.

Can prove: $\lambda(\sigma_q)$ is a root of the following polynomials (after reducing mod p):

(I)
$$X^{12} - \alpha^t$$
 for some $t \in \{0, 12\}$; and
(II) $X^2 - aX + \operatorname{Norm}(\mathfrak{q})$ for some $|a| \le 2\sqrt{\operatorname{Norm}(\mathfrak{q})}$.

Considering all cases restricts the possible values of p.

The fact that *E* is semistable at the primes of *K* above *p* means that $t \in \{0, 12\}$. Otherwise, $t \in \{0, 4, 6, 8, 12\}$.

Result

Proofs 000000000 Examples 0000

An algorithm

- Fix a number field K.
- Choose some primes q_1, \ldots, q_t of K.
- For each q_i , obtain a finite list of primes \mathcal{P}_i such that if there exists an elliptic curve E/K that admits a K-rational *p*-isogeny and is semistable at the primes of K above *p*, then $p \in \mathcal{P}_i$.
- Intersect the sets \mathcal{P}_i to obtain a finite list of primes.
- Use additional techniques to try and remove even more primes.

Results

Proofs 0000000000 Examples •000

Section 4

Examples

Proofs 0000000000 Examples

Example:
$$K = \mathbb{Q}(\sqrt{2})$$

Suppose E/K is an elliptic curve and that p is a prime such that E/K admits a K-rational p-isogeny and is semistable at the primes of K above p.

- Assume *p* > 19.
- Start with $q_1 = 3 \cdot \mathcal{O}_K$.
- By considering X₀(p): either p = 37 or E has potentially good reduction at q₁.
- By considering \$\overline{\rho}_{E,p}\$:

 $p \in \mathcal{P}_1 := \{37, 43, 61, 73, 89, 97, 109, 157, 313, 1489\}.$

- Now use $q_2 = \sqrt{2} \cdot \mathcal{O}_K$ to study $p \in \mathcal{P}_1$.
- By considering X₀(p): either p = 37 or E has potentially good reduction at q₂.
- By considering $\overline{\rho}_{E,p}$: find that p = 37.

Conclusion: $p \le 19$ or p = 37.

Results

Proofs 0000000000 Examples

The Fermat equation over $K = \mathbb{Q}(\sqrt{2})$

Theorem (Jarvis-Meekin, 2004)

The equation

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

with $n \ge 4$ has no solutions for $x, y, z \in K = \mathbb{Q}(\sqrt{2})$ with $xyz \ne 0$.

- 'Classical' for $n \in \{4, 5, 6, 7, 9, 11, 13\}$.
- Let $n = p \ge 17$ be prime and suppose $x^p + y^p = z^p$ with $xyz \ne 0$.
- Define the Frey elliptic curve $E: Y^2 = X(X x^p)(X + y^p)$.
- *E* does not admit a *K*-rational *p*-isogeny.
- E is modular.
- *E* 'corresponds' to a newform at level $\sqrt{2} \cdot \mathcal{O}_K \rightsquigarrow$ contradiction.

Results	Proofs	Examples
000	000000000	0000

We need to prove that E does not admit a K-rational p-isogeny for p > 17.

Proof.

- From example: $p \in \{17, 19, 37\}$.
- E has a 2-torsion point defined over K, so E gives rise to a non-cuspidal K-rational point on $X_0(2p)$.
- (Ozman–Siksek, 2019): No non-cuspidal K-rational points on $X_0(34)$ or $X_0(38)$.
- (Adžaga–Keller–M.–Najman–Ozman–Vukorepa, 2023): No non-cuspidal K-rational points on $X_0(74)$.

Hvala