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
Section 1

Motivation
Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).
Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).

**Proof.**

1. Classical for \( n \in \{3, 4\} \).
Motivation

Results

Proofs

Examples

Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).

Proof.

1. Classical for \( n \in \{3, 4\} \).
2. Let \( n = p \geq 5 \) be prime and suppose \( x^p + y^p = z^p \) with \( xyz \neq 0 \).
Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).

Proof.

1. Classical for \( n \in \{3, 4\} \).
2. Let \( n = p \geq 5 \) be prime and suppose \( x^p + y^p = z^p \) with \( xyz \neq 0 \).
3. Define the Frey elliptic curve \( E: Y^2 = X(X - x^p)(X + y^p) \).
Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).

Proof.

1. Classical for \( n \in \{3, 4\} \).
2. Let \( n = p \geq 5 \) be prime and suppose \( x^p + y^p = z^p \) with \( xyz \neq 0 \).
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**).
Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).

Proof.

1. Classical for \( n \in \{3, 4\} \).
2. Let \( n = p \geq 5 \) be prime and suppose \( x^p + y^p = z^p \) with \( xyz \neq 0 \).
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).
Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).

Proof.

1. Classical for \( n \in \{3, 4\} \).
2. Let \( n = p \geq 5 \) be prime and suppose \( x^p + y^p = z^p \) with \( xyz \neq 0 \).
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) \( \leadsto \) contradiction.
Fermat’s Last Theorem

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no solutions for \( x, y, z \in \mathbb{Z} \) with \( xyz \neq 0 \).

Proof.

1. Classical for \( n \in \{3, 4\} \).
2. Let \( n = p \geq 5 \) be prime and suppose \( x^p + y^p = z^p \) with \( xyz \neq 0 \).
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) \( \leadsto \) contradiction.
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

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$
# 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.
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?
Let $E_1, E_2$ be elliptic curves over a number field $K$. 

- An isogeny between elliptic curves is a non-constant morphism $\phi: E_1 \to E_2$ that induces a group homomorphism.
- The degree of an isogeny is the size of its kernel. If $\phi$ 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.**

$E_1$: $Y^2 = X^3 + X^2 - X$,

$E_2$: $Y^2 = X^3 - 2X^2 + 5X$.

$\phi$: $(x, y) \mapsto (y^2x^2, y(x^2 + 1)x^2)$. 

$\ker(\phi) = \{(0, E_1), (0, 0)\}$, it is a ($\mathbb{Q}$-)rational 2-isogeny.
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.
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 $\varphi$ has prime degree $p$, we say it is a $p$-isogeny.
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 $\varphi$ 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 $K$. 

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 $\varphi$ 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.

$$E_1 : Y^2 = X^3 + X^2 - X, \quad E_2 : Y^2 = X^3 - 2X^2 + 5X.$$  

$$\varphi : (x, y) \mapsto \left( \frac{y^2}{x^2}, \frac{y(x^2 + 1)}{x^2} \right).$$  

$\ker(\varphi) = \{0_{E_1}, (0, 0)\}$, it is a ($\mathbb{Q}$-)rational 2-isogeny.
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?
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 $\mathbb{Q}$. 
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.
The modular method over number fields

- Start with an equation:

\[ x^p + y^p = z^p, \quad \text{for } x, y, z \in K. \]
\[ x^{2p} + y^{2p} = z^7, \quad \text{for } x, y, z \in \mathbb{Z}. \]
\[ x^{2p} + 6x^p + 1 = 8y^2, \quad \text{for } x, y \in \mathbb{Z}. \]
The modular method over number fields

- Start with an equation:
  \[ x^p + y^p = z^p, \quad \text{for } x, y, z \in K. \]
  \[ x^{2p} + y^{2p} = z^7, \quad \text{for } x, y, z \in \mathbb{Z}. \]
  \[ x^{2p} + 6x^p + 1 = 8y^2, \quad \text{for } x, y \in \mathbb{Z}. \]

- Write down a Frey elliptic curve \( E/K \).
The modular method over number fields

• Start with an equation:

\[ x^p + y^p = z^p, \quad \text{for } x, y, z \in K. \]
\[ x^{2p} + y^{2p} = z^7, \quad \text{for } x, y, z \in \mathbb{Z}. \]
\[ x^{2p} + 6x^p + 1 = 8y^2, \quad \text{for } x, y \in \mathbb{Z}. \]

• Write down a Frey elliptic curve \( E/K \).

• Prove that \( E \) is modular.
The modular method over number fields

- Start with an equation:
  \[ x^p + y^p = z^p, \quad \text{for } x, y, z \in K. \]
  \[ x^{2p} + y^{2p} = z^7, \quad \text{for } x, y, z \in \mathbb{Z}. \]
  \[ x^{2p} + 6x^p + 1 = 8y^2, \quad \text{for } x, y \in \mathbb{Z}. \]

- Write down a Frey elliptic curve \( E/K \).
- Prove that \( E \) is modular.
- Prove that \( E \) does not admit a \( K \)-rational \( p \)-isogeny.
The modular method over number fields

- Start with an equation:
  \[ x^p + y^p = z^p, \quad \text{for } x, y, z \in K. \]
  \[ x^{2p} + y^{2p} = z^7, \quad \text{for } x, y, z \in \mathbb{Z}. \]
  \[ x^{2p} + 6x^p + 1 = 8y^2, \quad \text{for } x, y \in \mathbb{Z}. \]

- 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.
The modular method over number fields

- Start with an equation:
  \[ x^p + y^p = z^p, \quad \text{for } x, y, z \in K. \]
  \[ x^{2p} + y^{2p} = z^7, \quad \text{for } x, y, z \in \mathbb{Z}. \]
  \[ x^{2p} + 6x^p + 1 = 8y^2, \quad \text{for } x, y \in \mathbb{Z}. \]

- 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.
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 \( p \) is a prime of \( K \), then \( E \) is semistable at \( p \) if \( E \) has good or multiplicative reduction at \( p \).

• This is not a very restrictive assumption.

• It is already an assumption in the modular method for the level-lowering theorem.
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 $p$. 
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 $p | p$ is a prime of $K$, then $E$ is semistable at $p$ if $E$ has good or multiplicative reduction at $p$. 
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 $p | p$ is a prime of $K$, then $E$ is semistable at $p$ if $E$ has good or multiplicative reduction at $p$.

• This is not a very restrictive assumption.
• It is *already* an assumption in the modular method for the level-lowering theorem.
Section 2

Results
We will work with **quadratic fields**.

- Most useful for applications of the modular method.
- More techniques available.
- Sharper results are more easily obtained.
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* $p \in \{2, 3, 5, 7, 13, 17, 37\}$. 
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* $p \in \{2, 3, 5, 7, 13, 37, 43\}$. 
Theorem (M., 2023)

Let $K$ be a real quadratic field with $h(K) \leq 7$ and let $\epsilon$ 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

(i) $p$ ramifies in $K$; or

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

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

• This gives a simple criterion for ruling out primes.
• Any leftover primes can normally be dealt with separately.
Theorem (M., 2023)

Let $K$ be a real quadratic field with $h(K) \leq 7$ and let $\epsilon$ 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

(i) $p$ ramifies in $K$; or

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

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

• This gives a simple criterion for ruling out primes.
• Any leftover primes can normally be dealt with separately.
Section 3

Proofs
Modular curves and Galois representations

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

Strategy:
Modular curves and Galois representations

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

**Strategy:**

- Choose $q \nmid p$ a prime (of $K$).
Let $E/K$ be an elliptic curve that admits a $K$-rational $p$-isogeny, $\varphi$.

Strategy:

- Choose $q \nmid p$ a prime (of $K$).
- Case (i): $q$ is a prime of \textit{potentially multiplicative reduction for $E$} (meaning $v_q(j(E)) < 0$). Use the theory of \textbf{modular curves}.
Modular curves and Galois representations

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

Strategy:

- Choose $q \nmid p$ 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 $v_q(j(E)) \geq 0$). Use the theory of *Galois representations*. 
The modular curve $X_0(p)$

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

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

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

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

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

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

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

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

The pair $(E, \varphi)$ 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 $j : X_0(p) \to \mathbb{P}^1$ that satisfies $j(x) = j(E)$. 
The modular curve $X_0(p)$

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

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

The pair $(E, \varphi)$ 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.
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)).
A prime of potentially multiplicative reduction

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

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

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

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

- $\nu_q(j(E)) = \nu_q(j(x)) < 0$. 

• $v_q(j(E)) = v_q(j(x)) < 0$. 
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)).

- $\nu_q(j(E)) = \nu_q(j(x)) < 0$.
- So $x \pmod{q}$ is a pole of the $j$-map mod $q$. 
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)).

- $\nu_q(j(E)) = \nu_q(j(x)) < 0$.
- So $x \pmod{q}$ is a pole of the $j$-map mod $q$.
- $x \pmod{q} = \infty \pmod{q}$ or $0 \pmod{q}$.
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)).

- $v_q(j(E)) = v_q(j(x)) < 0$.
- So $x \pmod{q}$ is a pole of the $j$-map mod $q$.
- $x \pmod{q} = \infty \pmod{q}$ or $0 \pmod{q}$.
- Argue that $x = \infty$ or $0$, a contradiction (think of Hensel's lemma!).
The mod $p$ Galois representation

Let $E/K$ be an elliptic curve and $p$ a prime. Write $E[p] \subset E(K)$ for the $p$-torsion points of $E$. 
The mod $p$ Galois representation

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

The group $G_K = \text{Gal}(\bar{K}/K)$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ and gives rise to the \textbf{mod $p$ Galois representation} attached to $E$:

$$\bar{\rho}_{E,p} : G_K \to \text{GL}_2(\mathbb{F}_p).$$
The mod $p$ Galois representation

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

The group $G_K = \text{Gal}(\overline{K}/K)$ 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 $E$:

$$\overline{\rho}_{E,p} : G_K \to \text{GL}_2(\mathbb{F}_p).$$

Fix a basis $(R_1, R_2)$ of $E[p]$. 
The mod $p$ Galois representation

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

The group $G_K = \text{Gal}(\bar{K}/K)$ 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 $E$:

$$\bar{\rho}_{E,p} : G_K \to \text{GL}_2(\mathbb{F}_p).$$

Fix a basis $(R_1, R_2)$ of $E[p]$.

For $\sigma \in G_K$,

$$R_1^\sigma = aR_1 + bR_2,$$

$$R_2^\sigma = cR_1 + dR_2.$$
The mod $p$ Galois representation

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

The group $G_K = \text{Gal}(K/K)$ 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 $E$:

$$
\overline{\rho}_{E,p} : G_K \to \text{GL}_2(\mathbb{F}_p).
$$

Fix a basis $(R_1, R_2)$ of $E[p]$.

For $\sigma \in G_K$,

$$
R_1^\sigma = aR_1 + bR_2, \\
R_2^\sigma = cR_1 + dR_2.
$$

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

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, $\varphi$.

(ii) $\bar{\rho}_{E,p} : G_K \to \text{GL}_2(\mathbb{F}_p)$ is reducible.
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, $\varphi$.
(ii) $\bar{\rho}_{E,p} : G_K \to \text{GL}_2(\mathbb{F}_p)$ is reducible.

Proof.

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

(ii) \( \bar{\rho}_{E,p} : G_K \to \text{GL}_2(\mathbb{F}_p) \) is reducible.

**Proof.**

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

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

\[
\bar{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \chi' \end{pmatrix}.
\]

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. \( \square \)
The isogeny character

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

\[
\bar{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix}.
\]
The isogeny character

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

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix}.$$ 

The isogeny character

$\lambda : G_K \rightarrow \mathbb{F}_p^\times$ is the **isogeny character** of $(E, \varphi)$. 
Let $E/K$ be an elliptic such that $\bar{\rho}_{E,p}$ is reducible. So

$$\bar{\rho}_{E,p} \sim \begin{pmatrix} \lambda & \ast \\ 0 & \lambda' \end{pmatrix}.$$

The isogeny character

$\lambda : G_K \to \mathbb{F}_p^\times$ is the **isogeny character** of $(E, \varphi)$.

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

  $$R_1^\sigma = \lambda(\sigma)R_1.$$
The isogeny character

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

$$\bar{\rho}_{E,p} \sim \begin{pmatrix} \lambda & \ast \\ 0 & \lambda' \end{pmatrix}.$$ 

The isogeny character

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

- $\lambda$ tells us how $G_{K}$ acts on ker$(\varphi)$: if ker$(\varphi) = \langle R_{1} \rangle$, then for $\sigma \in G_{K}$,

$$R_{1}^{\sigma} = \lambda(\sigma)R_{1}.$$ 

We study $\lambda$ as it encodes key information about $E$ and $\varphi.$
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.
The group $G_K$ and Frobenius elements

We want to study $\lambda : G_K \rightarrow \mathbb{F}_p^\times$. 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 $\text{Gal}(\overline{k}/k)$, where $k = \mathcal{O}_K/q$. 
The group $G_K$ and Frobenius elements

We want to study $\lambda : G_K \rightarrow \mathbb{F}_p^\times$. 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 $\text{Gal}(\overline{k}/k)$, where $k = \mathcal{O}_K/q$.

We study $\lambda(\sigma_q) \in \mathbb{F}_p^\times$. 
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 $p$. 
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 $q^r = \alpha O_K$ is principal.
A prime of potentially good reduction

Let $E/K$ be an elliptic such that $\bar{\rho}_{E,p}$ 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) $X^2 - aX + \text{Norm}(q)$ for some $|a| \leq 2\sqrt{\text{Norm}(q)}$. 

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, $t \in \{0, 4, 6, 8, 12\}$. 
A prime of potentially good reduction

Let $E/K$ be an elliptic such that $\bar{\rho}_{E,p}$ 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) $X^2 - aX + \text{Norm}(q)$ for some $|a| \leq 2\sqrt{\text{Norm}(q)}$.

Considering all cases restricts the possible values of $p$. 
A prime of potentially good reduction

Let $E/K$ be an elliptic such that $\bar{\rho}_{E,p}$ 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) $X^2 - aX + \text{Norm}(q)$ for some $|a| \leq 2\sqrt{\text{Norm}(q)}$.

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, $t \in \{0, 4, 6, 8, 12\}$.
An algorithm

- Fix a number field $K$. 
An algorithm

- Fix a number field $K$.
- Choose some primes $q_1, \ldots, q_t$ of $K$. 
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 $p \in \mathcal{P}_i$. 
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.
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.
Section 4

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 $p$. 
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 $q_1 = 3 \cdot O_K$.
- By considering $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_1$.
- By considering $\rho_{E,p}$, $p \in P_1 := \{37, 43, 61, 73, 89, 97, 109, 157, 313, 1489\}$.
- Now use $q_2 = \sqrt{2} \cdot O_K$ to study $p \in P_1$.
- By considering $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_2$.
- By considering $\rho_{E,p}$: find that $p = 37$.

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

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 $q_1 = 3 \cdot \mathcal{O}_K$. 
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 $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_1$. 

Conclusion: $p \leq 19$ or $p = 37$. 
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 $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_1$.
- By considering $\bar{\rho}_{E,p}$:

$$p \in \mathcal{P}_1 := \{37, 43, 61, 73, 89, 97, 109, 157, 313, 1489\}.$$
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 $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_1$.
- By considering $\bar{\rho}_{E,p}$:
  \[ 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 $p \in \mathcal{P}_1$. 
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 $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_1$.
- 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 $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_2$. 
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 \( X_0(p) \): either \( p = 37 \) or \( E \) has potentially good reduction at \( q_1 \).
- By considering \( \rho_{E,p} \):

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

- Now use \( q_2 = \sqrt{2} \cdot \mathcal{O}_K \) to study \( p \in \mathcal{P}_1 \).
- By considering \( X_0(p) \): either \( p = 37 \) or \( E \) has potentially good reduction at \( q_2 \).
- By considering \( \rho_{E,p} \): find that \( p = 37 \).
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 $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_1$.
- By considering $\bar{\rho}_{E,p}$:
  
  $$p \in \mathcal{P}_1 := \{37, 43, 61, 73, 89, 97, 109, 157, 313, 1489\}.$$  

Now use $q_2 = \sqrt{2} \cdot \mathcal{O}_K$ to study $p \in \mathcal{P}_1$.
- By considering $X_0(p)$: either $p = 37$ or $E$ has potentially good reduction at $q_2$.
- By considering $\bar{\rho}_{E,p}$: find that $p = 37$.

Conclusion: $p \leq 19$ or $p = 37$. 
The Fermat equation over $K = \mathbb{Q}(\sqrt{2})$

**Theorem (Jarvis–Meekin, 2004)**

The equation

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

with $n \geq 4$ has no solutions for $x, y, z \in K = \mathbb{Q}(\sqrt{2})$ with $xyz \neq 0$. 
The Fermat equation over $K = \mathbb{Q}(\sqrt{2})$

**Theorem (Jarvis–Meekin, 2004)**

The equation

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

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

- 'Classical' for $n \in \{4, 5, 6, 7, 9, 11, 13\}$.
- Let $n = p \geq 17$ be prime and suppose $x^p + y^p = z^p$ with $xyz \neq 0$.
- 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 $\sqrt{2} \cdot \mathcal{O}_K \leadsto$ contradiction.
We need to prove that $E$ does not admit a $K$-rational $p$-isogeny for $p \geq 17$. 
We need to prove that $E$ does not admit a $K$-rational $p$-isogeny for $p \geq 17$.

**Proof.**

• From example: $p \in \{17, 19, 37\}$. 
We need to prove that $E$ does not admit a $K$-rational $p$-isogeny for $p \geq 17$.

**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 $X_0(38)$.


Hvala!
We need to prove that $E$ does not admit a $K$-rational $p$-isogeny for $p \geq 17$.

**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 $X_0(38)$.
We need to prove that $E$ does not admit a $K$-rational $p$-isogeny for $p \geq 17$.

**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 $X_0(38)$.
We need to prove that $E$ does not admit a $K$-rational $p$-isogeny for $p \geq 17$.

**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 $X_0(38)$.

Hvala!