Fermat's Last Theorem Over Totally Real Fields

Philippe Michaud-Rodgers

London Junior Number Theory Seminar

16.02.2021

Table of Contents

1. Introduction
2. FLT over Rationals: Preliminaries
3. FLT over Rationals: Proof
4. FLT over Totally Real Fields
5. Results

Table of Contents

1 Introduction

2 FLT over Rationals: Preliminaries

3 FLT over Rationals: Proof

4 FLT over Totally Real Fields

5 Results

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

Theorem (Wiles

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

Theorem (Wiles + many others! 1995)

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.

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 $xyz \neq 0$.

Generalising to Number Fields

What happens if we replace the word integers by

Generalising to Number Fields

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

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 $a, b, c \in \mathcal{O}_K$?

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 $a, b, c \in \mathcal{O}_K$?

- Does this exact statement always hold?

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 $a, b, c \in \mathcal{O}_K$?

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

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 $a, b, c \in \mathcal{O}_K$?

- 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 $\mathbb{Q}$.

Outline of Talk

- Overview the proof of FLT over $\mathbb{Q}$.
- Understand the three 'black boxes' used in the proof.

Outline of Talk

- Overview the proof of FLT over $\mathbb{Q}$.
- Understand the three 'black boxes' used in the proof.
- Try to use the same proof over K.

Outline of Talk

- Overview the proof of FLT over $\mathbb{Q}$.
- Understand the three 'black boxes' used in the proof.
- Try to use the same proof over K.
- Understand where it breaks down and see some of the maths used to overcome these issues.

Outline of Talk

- Overview the proof of FLT over $\mathbb{Q}$.
- Understand the three 'black boxes' used in the proof.
- Try to use the same proof over K.
- Understand where it breaks down and see some of the maths used to overcome these issues.

[Slides available on my webpage.]

Table of Contents

1 Introduction

2 FLT over Rationals: Preliminaries

3 FLT over Rationals: Proof

4 FLT over Totally Real Fields

5 Results

First Observations

- If $n = p \cdot m$ and (x, y, z) satisfies $x^n + y^n = z^n$, then

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

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.

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:

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 Background I

Definition

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.

Elliptic Curves Background I

Definition

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.

- $E(\mathbb{Q})$ is a finitely generated abelian group (Mordell-Weil).

Elliptic Curves Background I

Definition

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.

- $E(\mathbb{Q})$ is a finitely generated abelian group (Mordell-Weil).
- E has a minimal discriminant, $\Delta_{\min}$.

Elliptic Curves Background I

Definition

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.

- $E(\mathbb{Q})$ is a finitely generated abelian group (Mordell-Weil).
- E has a minimal discriminant, $\Delta_{\min}$.
- E has good reduction at $p \iff p \nmid \Delta_{\min}$.

Elliptic Curves Background II

- If $p \nmid \Delta_{\min}$, then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$

Elliptic Curves Background II

- If $p \nmid \Delta_{\min}$, then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ and we define $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$;

Elliptic Curves Background II

- If $p \nmid \Delta_{\min}$, then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ and we define $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$; the 'trace of Frobenius at p'.

Elliptic Curves Background II

- If $p \nmid \Delta_{\min}$, then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ and we define $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$; the 'trace of Frobenius at p'.
- E has a conductor

$$N_E := \prod_{p|\Delta_{\min}} p^{e_p}.$$

Elliptic Curves Background II

- If $p \nmid \Delta_{\min}$, then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ and we define $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$; the 'trace of Frobenius at p'.
- E has a conductor

$$N_E := \prod_{p|\Delta_{\min}} p^{e_p}.$$

- $e_p \geq 1$ measures how 'bad' the reduction at p is.

Elliptic Curves Background II

- If $p \nmid \Delta_{\min}$, then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ and we define $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$; the 'trace of Frobenius at p'.
- E has a conductor

$$N_E := \prod_{p|\Delta_{\min}} p^{e_p}.$$

- $e_p \geq 1$ measures how 'bad' the reduction at p is.
- $p \nmid \Delta_{\min} \iff p \nmid N_E$.

Elliptic Curves Background II

- If $p \nmid \Delta_{\min}$, then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ and we define $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$; the 'trace of Frobenius at p'.
- E has a conductor

$$N_E := \prod_{p|\Delta_{\min}} p^{e_p}.$$

- $e_p \geq 1$ measures how 'bad' the reduction at p is.
- $p \nmid \Delta_{\min} \iff p \nmid N_E$.
- If N is squarefree, E is called semistable.

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition.

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

- f is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$,

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

- f 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.

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

- f 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**:

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

- f 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**:

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

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

- f 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**:

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

- A newform is rational if $a_i \in \mathbb{Q}$ for all i

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

- f 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**:

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

- A newform is rational if $a_i \in \mathbb{Q}$ for all i (then in fact $a_i \in \mathbb{Z}$ for all i),

Newforms I

A newform of level N (where $N \in \mathbb{N}$), say f, is an object with a complicated definition. What do we need to know about them?

- f 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**:

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

- A newform is rational if $a_i \in \mathbb{Q}$ for all i (then in fact $a_i \in \mathbb{Z}$ for all i), and irrational otherwise.

Newforms II

- There are finitely many newforms at each level N.

Newforms II

- There are finitely many newforms at each level N.
- Newforms at level 38:

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

Newforms II

- There are finitely many newforms at each level N.
- Newforms at level 38:

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

Fact

There are no newforms at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.$$

Table of Contents

1 Introduction

2 FLT over Rationals: Preliminaries

3 FLT over Rationals: Proof

4 FLT over Totally Real Fields

5 Results

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform.

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N,

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Modularity Theorem

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Modularity Theorem (Wiles,

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Modularity Theorem (Wiles, Taylor + Wiles,

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Modularity Theorem (Wiles, Taylor + Wiles, B + C + D + T)

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Modularity Theorem (Wiles, Taylor + Wiles, B + C + D + T)

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Then E is modular.

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Modularity Theorem (Wiles, Taylor + Wiles, B + C + D + T)

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Then E is modular. Meaning we can associate to E a level N rational newform $f_E = \sum a_n q^n$ satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Eichler-Shimura and Modularity

Eichler-Shimura

Let $f = \sum a_n q^n$ be a level N rational newform. We can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

Modularity Theorem (Wiles, Taylor + Wiles, B + C + D + T)

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Then E is modular. Meaning we can associate to E a level N rational newform $f_E = \sum a_n q^n$ satisfying $a_p(f) = a_p(E)$ for any $p \nmid N$.

So we have maps **(BLACK BOX 1)**

$$\{\text{Level } N \text{ rational newforms}\} \leftrightarrows \{E/\mathbb{Q} \text{ of conductor } N\}.$$

Arises mod p

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.

Arises mod p

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

Arises mod p

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

Definition

Let p be a prime.

Arises mod p

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

Definition

Let p be a prime. We say E arises modulo p from f

Arises mod p

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

Definition

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

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

Arises mod p

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

Definition

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

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

- This is a natural definition.

Arises mod p

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

Definition

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

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

- This is a natural definition.
- Note: N and N' can differ.

Level-Lowering

(BLACK BOX 2)

Level-Lowering

(BLACK BOX 2)

Level-Lowering Theorem (Ribet)

Let E be a modular elliptic curve over $\mathbb{Q}$

Level-Lowering

(BLACK BOX 2)

Level-Lowering Theorem (Ribet)

Let E be a modular elliptic curve over $\mathbb{Q}$ of conductor N and let $p \geq 5$ be prime.

Level-Lowering

(BLACK BOX 2)

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 E has no **rational p-isogenies**.

Level-Lowering

(BLACK BOX 2)

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 E has no **rational p-isogenies**. Then E arises mod p from a newform f at level N_p,

Level-Lowering

(BLACK BOX 2)

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 E has no **rational p-isogenies**. Then E arises mod p from a newform f at level N_p, where

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

Level-Lowering

(BLACK BOX 2)

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 E has no **rational p-isogenies**. Then E arises mod p from a newform f at level N_p, where

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

- If E satisfies hypotheses and there are no newforms at level N_p, then this gives a contradiction.

Mazur's Theorem

Condition in Level-Lowering Theorem: Suppose E has no rational p-isogenies.

Mazur's Theorem

Condition in Level-Lowering Theorem: Suppose E has no rational p-isogenies.
(BLACK BOX 3)

Mazur's Theorem

Let $E/\mathbb{Q}$ be a semistable elliptic curve with full two-torsion.

Mazur's Theorem

Condition in Level-Lowering Theorem: Suppose E has no rational p-isogenies.
(BLACK BOX 3)

Mazur's Theorem

Let $E/\mathbb{Q}$ be a semistable elliptic curve with full two-torsion. Then E has no rational p-isogenies for $p \geq 5$.

The Frey Curve

Recall:

FLT

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

The Frey Curve

Recall:

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) is a solution and define the Frey Curve

$$E : Y^2 = X(X - x^p)(X + y^p).$$

The Frey Curve

Recall:

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) is a solution and define the Frey Curve

$$E : Y^2 = X(X - x^p)(X + y^p).$$

This is an elliptic curve.

The Frey Curve

Recall:

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) is a solution and define the Frey Curve

$$E : Y^2 = X(X - x^p)(X + y^p).$$

This is an elliptic curve.

- E has full two-torsion.

The Frey Curve

Recall:

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) is a solution and define the Frey Curve

$$E : Y^2 = X(X - x^p)(X + y^p).$$

This is an elliptic curve.

- E has full two-torsion.
- $\Delta_{\min} = 2^{-8}(xyz)^{2p}$,

The Frey Curve

Recall:

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) is a solution and define the Frey Curve

$$E : Y^2 = X(X - x^p)(X + y^p).$$

This is an elliptic curve.

- E has full two-torsion.
- $\Delta_{\min} = 2^{-8}(xyz)^{2p}$, $N = 2\prod_{p|xyz,\text{odd}} p$ is squarefree.

Level-Lowering the Frey Curve

- We level-lower (Black Box 2):

Level-Lowering the Frey Curve

- We level-lower (Black Box 2): E arises mod p from a newform f at level N_p.

Level-Lowering the Frey Curve

- We level-lower (Black Box 2): E arises mod p from a newform f at level N_p.
- Here

$$N_p = \frac{N}{\prod_{q \| N, p | \mathrm{ord}_q(\Delta_{\min})} q} = 2.$$

Level-Lowering the Frey Curve

- We level-lower (Black Box 2): E arises mod p from a newform f at level N_p.
- Here

$$N_p = \frac{N}{\prod_{q \| N, p | \mathrm{ord}_q(\Delta_{\min})} q} = 2.$$

- So $N_p = 2$

Level-Lowering the Frey Curve

- We level-lower (Black Box 2): E arises mod p from a newform f at level N_p.
- Here

$$N_p = \frac{N}{\prod_{q \| N, p | \mathrm{ord}_q(\Delta_{\min})} q} = 2.$$

- So $N_p = 2$ (no longer dependent on solution (x, y, z)).

Level-Lowering the Frey Curve

- We level-lower (Black Box 2): E arises mod p from a newform f at level N_p.
- Here

$$N_p = \frac{N}{\prod_{q \| N, p | \mathrm{ord}_q(\Delta_{\min})} q} = 2.$$

- So $N_p = 2$ (no longer dependent on solution (x, y, z)).
- But!

Level-Lowering the Frey Curve

- We level-lower (Black Box 2): E arises mod p from a newform f at level N_p.
- Here

$$N_p = \frac{N}{\prod_{q \| N, p | \mathrm{ord}_q(\Delta_{\min})} q} = 2.$$

- So $N_p = 2$ (no longer dependent on solution (x, y, z)).
- But! There are no newforms at level 2, contradiction.

Table of Contents

1 Introduction

2 FLT over Rationals: Preliminaries

3 FLT over Rationals: Proof

4 FLT over Totally Real Fields

5 Results

What changes over a number field?

Let K be a number field. Does the equation

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

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

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

- Same general method:

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

- Same general method: level-lower a Frey curve.

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

- Same general method: level-lower a Frey curve.
- Frey curve $E : Y^2 = X(X - a^p)(X + b^p)$, now $/K$.

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

- Same general method: level-lower a Frey curve.
- Frey curve $E : Y^2 = X(X - a^p)(X + b^p)$, now $/K$. Conductor $\mathcal{N}$ is an ideal of $\mathcal{O}_K$.

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

- Same general method: level-lower a Frey curve.
- Frey curve $E : Y^2 = X(X - a^p)(X + b^p)$, 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 $\mathcal{O}_K$.

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

- Same general method: level-lower a Frey curve.
- Frey curve $E : Y^2 = X(X - a^p)(X + b^p)$, 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 $\mathcal{N}$ (K totally real).

What changes over a number field?

Let K be a number field. Does the equation

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

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

! Approximate maths from now on, proceed with caution !

- Same general method: level-lower a Frey curve.
- Frey curve $E : Y^2 = X(X - a^p)(X + b^p)$, 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 $\mathcal{N}$ (K totally real). Values $a_p(f) \rightsquigarrow a_{\mathfrak{p}}(\mathfrak{f})$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.

Three Small (ish) Issues

- E is no longer semistable so we can't calculate $\mathcal{N}$.

Three Small (ish) Issues

- E is no longer semistable so we can't calculate $\mathcal{N}$. (actually quite a big issue!).

Three Small (ish) Issues

- E is no longer semistable so we can't calculate $\mathcal{N}$. (actually quite a big issue!). But we can obtain a finite list of possibilities for $\mathcal{N}$ and treat each one separately.

Three Small (ish) Issues

- E is no longer semistable so we can't calculate $\mathcal{N}$. (actually quite a big issue!). But we can obtain a finite list of possibilities for $\mathcal{N}$ and treat each one separately.
- $\mathcal{O}_K$ may not be a UFD.

Three Small (ish) Issues

- E is no longer semistable so we can't calculate $\mathcal{N}$. (actually quite a big issue!). But we can obtain a finite list of possibilities for $\mathcal{N}$ and treat each one separately.
- $\mathcal{O}_K$ may not be a UFD. Class group C_K plays a role.

Three Small (ish) Issues

- E is no longer semistable so we can't calculate $\mathcal{N}$. (actually quite a big issue!). But we can obtain a finite list of possibilities for $\mathcal{N}$ and treat each one separately.
- $\mathcal{O}_K$ may not be a UFD. Class group C_K plays a role.
- May be solutions for small p (e.g. $p = 3$).

Three Big Issues

- Modularity.

Three Big Issues

- Modularity. To level-lower, E must be modular.

Three Big Issues

- Modularity. To level-lower, E must be modular.
- Irreducibility.

Three Big Issues

- Modularity. To level-lower, E must be modular.
- Irreducibility. To level-lower, E must have no (K-rational) p-isogenies.

Three Big Issues

- Modularity. To level-lower, E must be modular.
- Irreducibility. To level-lower, E must have no (K-rational) p-isogenies.
- Newforms.

Three Big Issues

- Modularity. To level-lower, E must be modular.
- Irreducibility. To level-lower, E must have no (K-rational) p-isogenies.
- Newforms. Need to **calculate** and **eliminate** newforms appearing at level $\mathcal{N}_p$

Three Big Issues

- Modularity. To level-lower, E must be modular.
- Irreducibility. To level-lower, E must have no (K-rational) p-isogenies.
- Newforms. Need to **calculate** and **eliminate** newforms appearing at level $\mathcal{N}_p$ (over $\mathbb{Q}$ there were none at level $N_p = 2$; contradiction right away).

Modularity over number fields

What does it mean for an E/K to be modular?

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real...

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real... results are all conjectural.

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real... results are all conjectural. From now on we take K totally real.

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real... results are all conjectural. From now on we take K totally real.

- E/K of conductor $\mathcal{N}$ is modular if there exists a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}$ such that $a_{\mathfrak{p}}(E) = a_{\mathfrak{p}}(\mathfrak{f})$ for all $\mathfrak{p} \nmid \mathcal{N}$.

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real... results are all conjectural. From now on we take K totally real.

- E/K of conductor $\mathcal{N}$ is modular if there exists a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}$ such that $a_{\mathfrak{p}}(E) = a_{\mathfrak{p}}(\mathfrak{f})$ for all $\mathfrak{p} \nmid \mathcal{N}$.
- Elliptic curves over real quadratic fields are modular (Freitas, Le Hung, Siksek, 2013).

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real... results are all conjectural. From now on we take K totally real.

- E/K of conductor $\mathcal{N}$ is modular if there exists a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}$ such that $a_{\mathfrak{p}}(E) = a_{\mathfrak{p}}(\mathfrak{f})$ for all $\mathfrak{p} \nmid \mathcal{N}$.
- Elliptic curves over real quadratic fields are modular (Freitas, Le Hung, Siksek, 2013).
- Elliptic curves over totally real cubic fields are modular (Derickx, Najman, Siksek, 2019).

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real... results are all conjectural. From now on we take K totally real.

- E/K of conductor $\mathcal{N}$ is modular if there exists a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}$ such that $a_{\mathfrak{p}}(E) = a_{\mathfrak{p}}(\mathfrak{f})$ for all $\mathfrak{p} \nmid \mathcal{N}$.
- Elliptic curves over real quadratic fields are modular (Freitas, Le Hung, Siksek, 2013).
- Elliptic curves over totally real cubic fields are modular (Derickx, Najman, Siksek, 2019).
- Frey curve E is modular for $p > A_K$,

Modularity over number fields

What does it mean for an E/K to be modular? If K is not totally real... results are all conjectural. From now on we take K totally real.

- E/K of conductor $\mathcal{N}$ is modular if there exists a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}$ such that $a_{\mathfrak{p}}(E) = a_{\mathfrak{p}}(\mathfrak{f})$ for all $\mathfrak{p} \nmid \mathcal{N}$.
- Elliptic curves over real quadratic fields are modular (Freitas, Le Hung, Siksek, 2013).
- Elliptic curves over totally real cubic fields are modular (Derickx, Najman, Siksek, 2019).
- Frey curve E is modular for $p > A_K$, an **ineffective** constant.

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

E has a K-rational p-isogeny $\iff \overline{\rho}_{E,p}$ is reducible

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

E has a K-rational p-isogeny $\iff \overline{\rho}_{E,p}$ is reducible , where $\overline{\rho}_{E,p}$ is the **mod-p Galois representation** associated to E.

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

E has a K-rational p-isogeny $\iff \overline{\rho}_{E,p}$ is reducible , where $\overline{\rho}_{E,p}$ is the **mod-p Galois representation** associated to E.

- There exists an **effective** constant C_K such that for $p > C_K$, $\overline{\rho}_{E,p}$ is irreducible for the Frey curve E.

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

E has a K-rational p-isogeny $\iff \overline{\rho}_{E,p}$ is reducible , where $\overline{\rho}_{E,p}$ is the **mod-p Galois representation** associated to E.

- There exists an **effective** constant C_K such that for $p > C_K$, $\overline{\rho}_{E,p}$ is irreducible for the Frey curve E.
- If $\overline{\rho}_{E,p}$ is reducible, E gives rise to a non-cuspidal K-point on the modular curve $X_0(p)$.

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

E has a K-rational p-isogeny $\iff$ $\overline{\rho}_{E,p}$ is reducible , where $\overline{\rho}_{E,p}$ is the **mod-p Galois representation** associated to E.

- There exists an **effective** constant C_K such that for $p > C_K$, $\overline{\rho}_{E,p}$ is irreducible for the Frey curve E.
- If $\overline{\rho}_{E,p}$ is reducible, E gives rise to a non-cuspidal K-point on the modular curve $X_0(p)$.

Example: $X_0(19)(\mathbb{Q}(\sqrt{30}))$ consists of only cusps.

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

E has a K-rational p-isogeny $\iff \overline{\rho}_{E,p}$ is reducible , where $\overline{\rho}_{E,p}$ is the **mod-p Galois representation** associated to E.

- There exists an **effective** constant C_K such that for $p > C_K$, $\overline{\rho}_{E,p}$ is irreducible for the Frey curve E.
- If $\overline{\rho}_{E,p}$ is reducible, E gives rise to a non-cuspidal K-point on the modular curve $X_0(p)$.

Example: $X_0(19)(\mathbb{Q}(\sqrt{30}))$ consists of only cusps. So $E/\mathbb{Q}(\sqrt{30})$ has no K-rational 19-isogenies.

Irreducibility

To level-lower, we need E to have no K-rational p-isogenies.

E has a K-rational p-isogeny $\iff \overline{\rho}_{E,p}$ is reducible , where $\overline{\rho}_{E,p}$ is the **mod-p Galois representation** associated to E.

- There exists an **effective** constant C_K such that for $p > C_K$, $\overline{\rho}_{E,p}$ is irreducible for the Frey curve E.
- If $\overline{\rho}_{E,p}$ is reducible, E gives rise to a non-cuspidal K-point on the modular curve $X_0(p)$.

Example: $X_0(19)(\mathbb{Q}(\sqrt{30}))$ consists of only cusps. So $E/\mathbb{Q}(\sqrt{30})$ has no K-rational 19-isogenies. (i.e. $\overline{\rho}_{E,19}$ is irreducible).

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$.

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E (i.e. most primes)

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E (i.e. most primes), $a_{\mathfrak{q}}(\mathfrak{f})$ and $a_{\mathfrak{q}}(E)$ 'match mod-p'.

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E (i.e. most primes), $a_\mathfrak{q}(\mathfrak{f})$ and $a_\mathfrak{q}(E)$ 'match mod-p'. Deduce $p \mid \mathrm{Norm}(a_\mathfrak{q}(\mathfrak{f}) - a_\mathfrak{q}(E))$.

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E (i.e. most primes), $a_\mathfrak{q}(\mathfrak{f})$ and $a_\mathfrak{q}(E)$ 'match mod-p'. Deduce $p \mid \mathrm{Norm}(a_\mathfrak{q}(\mathfrak{f}) - a_\mathfrak{q}(E))$.

Problem: We don't know $a_\mathfrak{q}(E)$ (depends on solution).

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E (i.e. most primes), $a_\mathfrak{q}(\mathfrak{f})$ and $a_\mathfrak{q}(E)$ 'match mod-p'. Deduce $p \mid \mathrm{Norm}(a_\mathfrak{q}(\mathfrak{f}) - a_\mathfrak{q}(E))$.

Problem: We don't know $a_\mathfrak{q}(E)$ (depends on solution).
But, by Hasse-Weil, $a_\mathfrak{q}(E) \in \mathcal{A} := \{a \in \mathbb{Z} : a \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}\}$.

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E (i.e. most primes), $a_\mathfrak{q}(\mathfrak{f})$ and $a_\mathfrak{q}(E)$ 'match mod-p'. Deduce $p \mid \mathrm{Norm}(a_\mathfrak{q}(\mathfrak{f}) - a_\mathfrak{q}(E))$.

Problem: We don't know $a_\mathfrak{q}(E)$ (depends on solution).
But, by Hasse-Weil, $a_\mathfrak{q}(E) \in \mathcal{A} := \{a \in \mathbb{Z} : a \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}\}$.

So $p \mid \prod_{a \in \mathcal{A}} \mathrm{Norm}(a_\mathfrak{q}(\mathfrak{f}) - a)$.

Eliminating Newforms

Suppose E arises mod p from a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ **and** suppose we can calculate the newforms at level $\mathcal{N}_p$. How can we achieve a contradiction?

Idea: for $\mathfrak{q}$ a prime of good reduction for E (i.e. most primes), $a_\mathfrak{q}(\mathfrak{f})$ and $a_\mathfrak{q}(E)$ 'match mod-p'. Deduce $p \mid \mathrm{Norm}(a_\mathfrak{q}(\mathfrak{f}) - a_\mathfrak{q}(E))$.

Problem: We don't know $a_\mathfrak{q}(E)$ (depends on solution).
But, by Hasse-Weil, $a_\mathfrak{q}(E) \in \mathcal{A} := \{a \in \mathbb{Z} : a \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}\}$.

So $p \mid \prod_{a \in \mathcal{A}} \mathrm{Norm}(a_\mathfrak{q}(\mathfrak{f}) - a)$. We use this idea to bound p.

Calculating Newforms

- List of conductors $\mathcal{N} \rightsquigarrow$ List of levels $\mathcal{N}_p$.

Calculating Newforms

- List of conductors $\mathcal{N} \rightsquigarrow$ List of levels $\mathcal{N}_p$.
- Cannot compute Hilbert newforms at large levels.

Calculating Newforms

- List of conductors $\mathcal{N} \rightsquigarrow$ List of levels $\mathcal{N}_p$.
- Cannot compute Hilbert newforms at large levels.
- Values $a_{\mathfrak{q}}(\mathfrak{f})$ are eigenvalues for Hecke operator $T_{\mathfrak{q}}$.

Calculating Newforms

- List of conductors $\mathcal{N} \rightsquigarrow$ List of levels $\mathcal{N}_p$.
- Cannot compute Hilbert newforms at large levels.
- Values $a_{\mathfrak{q}}(\mathfrak{f})$ are eigenvalues for Hecke operator $T_{\mathfrak{q}}$.
- Partially reconstruct newforms $\mathfrak{f}$ by working directly with Hecke operators.

Calculating Newforms

- List of conductors $\mathcal{N} \rightsquigarrow$ List of levels $\mathcal{N}_p$.
- Cannot compute Hilbert newforms at large levels.
- Values $a_{\mathfrak{q}}(\mathfrak{f})$ are eigenvalues for Hecke operator $T_{\mathfrak{q}}$.
- Partially reconstruct newforms $\mathfrak{f}$ by working directly with Hecke operators.
- Often provides enough information to eliminate newforms.

Table of Contents

1 Introduction

2 FLT over Rationals: Preliminaries

3 FLT over Rationals: Proof

4 FLT over Totally Real Fields

5 Results

Asymptotic Results

Asymptotic FLT: No non-trivial solutions for $p > B_K$.

Asymptotic Results

Asymptotic FLT: No non-trivial solutions for $p > B_K$.

Theorem (Freitas, Siksek, 2014)

Effective asymptotic FLT holds for $5/6$*ths of real quadratic fields.*

Asymptotic Results

Asymptotic FLT: No non-trivial solutions for $p > B_K$.

Theorem (Freitas, Siksek, 2014)

Effective asymptotic FLT holds for 5/6ths of real quadratic fields.

Theorem (Freitas, Kraus, Siksek, 2019)

Let K be a totally real field in which 2 is totally ramified and $h^+_{K,2}$ divides the order of the unique prime above 2 in Cl_K.

Asymptotic Results

Asymptotic FLT: No non-trivial solutions for $p > B_K$.

Theorem (Freitas, Siksek, 2014)

Effective asymptotic FLT holds for 5/6ths of real quadratic fields.

Theorem (Freitas, Kraus, Siksek, 2019)

Let K be a totally real field in which 2 is totally ramified and $h^+_{K,2}$ divides the order of the unique prime above 2 in Cl_K. Then asymptotic FLT holds over K.

Asymptotic Results

Asymptotic FLT: No non-trivial solutions for $p > B_K$.

Theorem (Freitas, Siksek, 2014)

Effective asymptotic FLT holds for 5/6ths of real quadratic fields.

Theorem (Freitas, Kraus, Siksek, 2019)

Let K be a totally real field in which 2 is totally ramified and $h^+_{K,2}$ divides the order of the unique prime above 2 in Cl_K. Then asymptotic FLT holds over K.

- Many more asymptotic results known.

Complete Results

Theorem (Jarvis and Meekin, 2003)

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

Complete Results

Theorem (Jarvis and Meekin, 2003)

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

Theorem (Freitas and Siksek, 2014)

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

Complete Results

Theorem (Jarvis and Meekin, 2003)

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

Theorem (Freitas and Siksek, 2014)

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

Theorem (Kraus, 2017)

No non-trivial solutions for cubic fields K *of discriminant* $148,404,564$ *and* $n \geq 4$.

Some More Results

Theorem (M. 2021)

No non-trivial solutions for $K = \mathbb{Q}(\sqrt{d})$ *and* $n \geq 4$, *for*
$d \in \{29, 30, 31, 38, 42, 43, 46, 47, 51, 53, 58, 59, 62, 65, 67, 69, 71,$
$73, 77, 83, 85, 86, 87, 91, 93 + \textit{more} < 100\}$.

Some More Results

Theorem (M. 2021)

No non-trivial solutions for $K = \mathbb{Q}(\sqrt{d})$ *and* $n \geq 4$, *for*
$d \in \{29, 30, 31, 38, 42, 43, 46, 47, 51, 53, 58, 59, 62, 65, 67, 69, 71,$
$73, 77, 83, 85, 86, 87, 91, 93 + \textit{more} < 100\}$.

- Partial results obtained for many other squarefree $d < 100$.

Some More Results

Theorem (M. 2021)

No non-trivial solutions for $K = \mathbb{Q}(\sqrt{d})$ *and* $n \geq 4$, *for*
$d \in \{29, 30, 31, 38, 42, 43, 46, 47, 51, 53, 58, 59, 62, 65, 67, 69, 71,$
$73, 77, 83, 85, 86, 87, 91, 93 + \textit{more} < 100\}$.

- Partial results obtained for many other squarefree $d < 100$.
- **Example:** No non-trivial solutions for $K = \mathbb{Q}(\sqrt{37})$ and $p \geq 5, p \neq 37$.

Thank you for listening! :)