The Fermat Equation over Totally Real Fields

Nuno Freitas
joint work with Samir Siksek

Universität Bayreuth

January 2014

Motivation

Fermat's Last Theorem

The only solutions (a, b, c) to the equation

$$x^p + y^p + z^p = 0, \qquad a, b, c \in \mathbb{Z} \qquad p \geq 3 \text{ prime}$$

satisfy $abc = 0$.

Motivation

Fermat's Last Theorem

The only solutions (a, b, c) to the equation

$$x^p + y^p + z^p = 0, \qquad a, b, c \in \mathbb{Z} \qquad p \geq 3 \text{ prime}$$

satisfy $abc = 0$.

Theorem (Jarvis–Meekin)

The only solutions (a, b, c) to the equation

$$x^p + y^p + z^p = 0, \qquad a, b, c \in \mathbb{Q}(\sqrt{2}), \qquad p \geq 5 \text{ prime}$$

satisfy $abc = 0$.

Motivation

Theorem (Wiles, Taylor–Wiles)

Semistable elliptic curves over $\mathbb{Q}$ are modular.

Motivation

Theorem (Wiles, Taylor–Wiles)

Semistable elliptic curves over $\mathbb{Q}$ are modular.

Theorem (Breuil–Conrad–Diamond–Taylor)

All elliptic curves over $\mathbb{Q}$ are modular.

Motivation

Theorem (Wiles, Taylor–Wiles)

Semistable elliptic curves over $\mathbb{Q}$ are modular.

Theorem (Breuil–Conrad–Diamond–Taylor)

All elliptic curves over $\mathbb{Q}$ are modular.

Theorem (Jarvis–Manoharmayum)

Semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ are modular.

Definition

Let E be an elliptic curve over a totally real field K. We say that E is **modular** if there is a Hilbert eigenform $\mathfrak{f}$ over K of parallel weight 2 and rational coefficients such that

$$L(E, s) = L(\mathfrak{f}, s)$$

Motivation – proof of FLT:

Suppose a, b, $c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Motivation – proof of FLT:

Suppose a, b, $c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Following Frey, let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Motivation – proof of FLT:

Suppose $a, b, c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Following Frey, let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^{?} \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

Motivation – proof of FLT:

Suppose a, b, $c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Following Frey, let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^? \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

Write $\bar{\rho}_p$ for the mod p representation attached to E. Define

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell \| N \\ p \mid \upsilon_\ell(\Delta)}} \ell.$$

Motivation – proof of FLT:

Suppose a, b, $c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Following Frey, let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16 a^{2p} b^{2p} c^{2p}, \qquad N = 2^? \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

Write $\bar{\rho}_p$ for the mod p representation attached to E. Define

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell \| N \\ p \mid \upsilon_\ell(\Delta)}} \ell.$$

By Wiles E is **modular**.

Motivation – proof of FLT:

Suppose $a, b, c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Following Frey, let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^? \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

Write $\overline{\rho}_p$ for the mod p representation attached to E. Define

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell \| N \\ p \mid \upsilon_\ell(\Delta)}} \ell.$$

By Wiles E is **modular**. By Mazur, $\overline{\rho}_p$ is irreducible.

Motivation – proof of FLT:

Suppose a, b, $c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Following Frey, let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^{?} \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

Write $\overline{\rho}_p$ for the mod p representation attached to E. Define

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell \| N \\ p \mid \upsilon_\ell(\Delta)}} \ell.$$

By Wiles E is **modular**. By Mazur, $\overline{\rho}_p$ is irreducible. By Ribet's **level lowering:** $\overline{\rho}_p$ arises from a newform of weight 2 and level $N(\overline{\rho}_p) = 2$.

Motivation – proof of FLT:

Suppose a, b, $c \in \mathbb{Z}$ and $p \geq 5$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Following Frey, let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^{?} \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

Write $\overline{\rho}_p$ for the mod p representation attached to E. Define

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell \| N \\ p \mid \upsilon_\ell(\Delta)}} \ell.$$

By Wiles E is **modular**. By Mazur, $\overline{\rho}_p$ is irreducible. By Ribet's **level lowering:** $\overline{\rho}_p$ arises from a newform of weight 2 and level $N(\overline{\rho}_p) = 2$. **There are no newforms of weight** 2 **and level** 2!!

Motivation

Question: Can the modular method be applied to the Fermat equation over more number fields?

Motivation

Question: Can the modular method be applied to the Fermat equation over more number fields?

Question: Let $d > 0$ be a squarefree integer. Can we say anything about the Fermat equation over $\mathbb{Q}(\sqrt{d})$?

Motivation

Question: Can the modular method be applied to the Fermat equation over more number fields?

Question: Let $d > 0$ be a squarefree integer. Can we say anything about the Fermat equation over $\mathbb{Q}(\sqrt{d})$?

Question: Can we prove modularity of the Frey curves over $\mathbb{Q}(\sqrt{d})$?

Motivation

Question: Can the modular method be applied to the Fermat equation over more number fields?

Question: Let $d > 0$ be a squarefree integer. Can we say anything about the Fermat equation over $\mathbb{Q}(\sqrt{d})$?

Question: Can we prove modularity of the Frey curves over $\mathbb{Q}(\sqrt{d})$?

These questions for quadratic fields were analysed by Jarvis and Meekin. They find that

> *"... the numerology required to generalise the work of Ribet and Wiles directly continues to hold for $\mathbb{Q}(\sqrt{2})$... there are no other real quadratic fields for which this is true ..."*

What is the "required numerology" ?

The **Fermat equation with exponent** p **over** K is the equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K.$$

We say (a, b, c) is **trivial** if $abc = 0$, otherwise **non-trivial**.

What is the "required numerology" ?

The **Fermat equation with exponent** p **over** K is the equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K.$$

We say (a, b, c) is **trivial** if $abc = 0$, otherwise **non-trivial**.

Let K be totally real and (a, b, c) a non-trivial solution over K. Define the Frey curve

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

What is the "required numerology" ?

The **Fermat equation with exponent p over K** is the equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K.$$

We say (a, b, c) is **trivial** if $abc = 0$, otherwise **non-trivial**.

Let K be totally real and (a, b, c) a non-trivial solution over K. Define the Frey curve

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

1) E is not known to be modular. E is not semistable.

What is the "required numerology" ?

The **Fermat equation with exponent p over K** is the equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K.$$

We say (a, b, c) is **trivial** if $abc = 0$, otherwise **non-trivial**.

Let K be totally real and (a, b, c) a non-trivial solution over K. Define the Frey curve

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

1) E is not known to be modular. E is not semistable.
2) Suppose E is modular. After level lowering we obtain

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{p}} \quad \text{for some } \mathfrak{p} \mid p,$$

and we want f to be of level independent of the solution.

What is the “required numerology” ?

The **Fermat equation with exponent p over K** is the equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K.$$

We say (a, b, c) is **trivial** if $abc = 0$, otherwise **non-trivial**.

Let K be totally real and (a, b, c) a non-trivial solution over K. Define the Frey curve

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

1) E is not known to be modular. E is not semistable.
2) Suppose E is modular. After level lowering we obtain

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{p}} \quad \text{for some } \mathfrak{p} \mid p,$$

and we want f to be of level independent of the solution.
3) The final spaces of Hilbert newforms may be non-empty.

Notation and Eichler-Shimura

Conjecture ("Eichler–Shimura")

Let K be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform of level $\mathcal{N}$ and parallel weight 2, and write $\mathbb{Q}_{\mathfrak{f}}$ for its field of coefficients. Suppose that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

Notation and Eichler-Shimura

Conjecture ("Eichler–Shimura")

Let K be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform of level $\mathcal{N}$ and parallel weight 2, and write $\mathbb{Q}_{\mathfrak{f}}$ for its field of coefficients. Suppose that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

For K a totally real field let

$$S = \{\mathfrak{P} \; : \; \mathfrak{P} \text{ is a prime of } K \text{ above } 2\},$$
$$T = \{\mathfrak{P} \in S \; : \; f(\mathfrak{P}/2) = 1\}, \qquad U = \{\mathfrak{P} \in S \; : \; 3 \nmid \operatorname{ord}_{\mathfrak{P}}(2)\},$$

where $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$.

Notation and Eichler-Shimura

Conjecture ("Eichler–Shimura")

Let K be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform of level $\mathcal{N}$ and parallel weight 2, and write $\mathbb{Q}_{\mathfrak{f}}$ for its field of coefficients. Suppose that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

For K a totally real field let

$$S = \{\mathfrak{P} \ : \ \mathfrak{P} \text{ is a prime of } K \text{ above } 2\},$$
$$T = \{\mathfrak{P} \in S \ : \ f(\mathfrak{P}/2) = 1\}, \qquad U = \{\mathfrak{P} \in S \ : \ 3 \nmid \mathrm{ord}_{\mathfrak{P}}(2)\},$$

where $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$. We now do the following assumption on K:

$$\textbf{(ES)} \qquad \begin{cases} \text{either } [K:\mathbb{Q}] \text{ is odd;} \\ \text{or } T \neq \emptyset; \\ \text{the Conjecture above holds for } K. \end{cases}$$

Results – Fermat over totally real fields

Theorem (F.–Siksek)

Let K be a totally real field satisfying assumption **(ES)**. *Let S, T and U be as before. Write $\mathcal{O}_S^*$ for the set of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \qquad \lambda,\, \mu \in \mathcal{O}_S^* .$$

there is

(A) either some $\mathfrak{P} \in T$ that satisfies

$$\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}}(\mu)|\} \leq 4\, \mathrm{ord}_{\mathfrak{P}}(2), \tag{1}$$

(B) or some $\mathfrak{P} \in U$ that satisfies both (3) *and*

$$\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) \equiv \mathrm{ord}_{\mathfrak{P}}(2) \pmod 3.$$

Then there is some constant B_K such that for all $p > B_K$, the Fermat equation with exponent p has no non-trivial solutions.

Results – Fermat over real quadratic fields

Theorem (F.–Siksek)

Let $d \geq 2$ be squarefree, satisfying one of the following conditions

(i) $d \equiv 3 \pmod 8$,

(ii) $d \equiv 6$ *or* $10 \pmod{16}$,

(iii) $d \equiv 2 \pmod{16}$ *and* d *has a prime divisor* $q \equiv 5$ *or* $7 \pmod 8$,

(iv) $d \equiv 14 \pmod{16}$ *and* d *has some prime divisor* $q \equiv 3$ *or* $5 \pmod 8$.

Write $K = \mathbb{Q}(\sqrt{d})$. *Then there is an* **effectively computable** *constant* B_K *such that for all primes* $p > B_K$, *the Fermat equation with exponent* p *has no non-trivial solutions.*

Results – Fermat over real quadratic fields

Theorem (F.–Siksek)

Let $d \geq 2$ be squarefree, satisfying one of the following conditions

(i) $d \equiv 3 \pmod 8$,

(ii) $d \equiv 6$ *or* $10 \pmod{16}$,

(iii) $d \equiv 2 \pmod{16}$ *and* d *has a prime divisor* $q \equiv 5$ *or* $7 \pmod 8$,

(iv) $d \equiv 14 \pmod{16}$ *and* d *has some prime divisor* $q \equiv 3$ *or* $5 \pmod 8$.

Write $K = \mathbb{Q}(\sqrt{d})$*. Then there is an* **effectively computable** *constant* B_K *such that for all primes* $p > B_K$*, the Fermat equation with exponent* p *has no non-trivial solutions.*

Moreover, for $d > 5$ *satisfying* $d \equiv 5 \pmod 8$*, supposing that* K *satisfies assumption* (**ES**)*, the same conclusion holds.*

Solutions to the S-unit equation over real quadratic fields.

For any totally real field K there are the rational solutions $(2,-1)$, $(-1,2)$ and $(1/2,1/2)$. These always satisfy (A) if $T \neq \emptyset$ and (B) if $U \neq \emptyset$. We call them **irrelevant** solutions.

Solutions to the S-unit equation over real quadratic fields.

For any totally real field K there are the rational solutions $(2, -1)$, $(-1, 2)$ and $(1/2, 1/2)$. These always satisfy (A) if $T \neq \emptyset$ and (B) if $U \neq \emptyset$. We call them **irrelevant** solutions.

Let $d \not\equiv 1 \pmod{8}$ be squarefree. We computed the **relevant** solutions to the S-unit equation over $\mathbb{Q}(\sqrt{d})$:

Solutions to the S-unit equation over real quadratic fields.

For any totally real field K there are the rational solutions $(2, -1)$, $(-1, 2)$ and $(1/2, 1/2)$. These always satisfy (A) if $T \neq \emptyset$ and (B) if $U \neq \emptyset$. We call them **irrelevant** solutions.

Let $d \not\equiv 1 \pmod 8$ be squarefree. We computed the **relevant** solutions to the S-unit equation over $\mathbb{Q}(\sqrt{d})$:

d	relevant elements of Λ_S up to the action of $\mathfrak{S}_3$ and Galois conjugation	extra conditions
$d = 2$	$(\sqrt{2}, 1-\sqrt{2})$, $(-16+12\sqrt{2}, 17-12\sqrt{2})$, $(4+2\sqrt{2}, -3+2\sqrt{2})$, $(-2+2\sqrt{2}, 3-2\sqrt{2})$	
$d = 3$	$(2+\sqrt{3}, -1-\sqrt{3})$, $(8+4\sqrt{3}, -7-4\sqrt{3})$	
$d = 5$	$((1+\sqrt{5})/2, (1-\sqrt{5})/2)$, $(-8+4\sqrt{5}, 9-4\sqrt{5})$, $(-1+\sqrt{5}, 2-\sqrt{5})$	
$d = 6$	$(-4+2\sqrt{6}, 5-2\sqrt{6})$	
$d \equiv 3 \pmod 8$, $d \neq 3$	none	
$d \equiv 5 \pmod 8$, $d \neq 5$	none	
$d \equiv 7 \pmod 8$	$(2^{2s+1} + 2^{s+1} w\sqrt{d},\ 1 - 2^{2s+1} - 2^{s+1} w\sqrt{d})$	$4^s - 1 = dw^2$, $s \geq 2$, $w \neq 0$
$d \equiv 2 \pmod{16}$, $d \neq 2$	$(-2^{2s} + 2^s w\sqrt{d}, 1 + 2^{2s} - 2^s w\sqrt{d})$	$4^s + 2 = dw^2$, $s \geq 2$, $w \neq 0$
$d \equiv 6 \pmod{16}$, $d \neq 6$	none	
$d \equiv 10 \pmod{16}$	none	
$d \equiv 14 \pmod{16}$	$(2^{2s} + 2^s w\sqrt{d}, 1 - 2^{2s} - 2^s w\sqrt{d})$	$4^s - 2 = dw^2$, $s \geq 2$, $w \neq 0$

Solutions to the S-unit equation over real quadratic fields.

For any totally real field K there are the rational solutions $(2,-1)$, $(-1,2)$ and $(1/2,1/2)$. These always satisfy (A) if $T \neq \emptyset$ and (B) if $U \neq \emptyset$. We call them **irrelevant** solutions.

Let $d \not\equiv 1 \pmod 8$ be squarefree. We computed the **relevant** solutions to the S-unit equation over $\mathbb{Q}(\sqrt{d})$:

d	relevant elements of Λ_S up to the action of $\mathfrak{S}_3$ and Galois conjugation	extra conditions
$d=2$	$(\sqrt{2}, 1-\sqrt{2})$, $(-16+12\sqrt{2}, 17-12\sqrt{2})$, $(4+2\sqrt{2}, -3+2\sqrt{2})$, $(-2+2\sqrt{2}, 3-2\sqrt{2})$	
$d=3$	$(2+\sqrt{3}, -1-\sqrt{3})$, $(8+4\sqrt{3}, -7-4\sqrt{3})$	
$d=5$	$((1+\sqrt{5})/2, (1-\sqrt{5})/2)$, $(-8+4\sqrt{5}, 9-4\sqrt{5})$, $(-1+\sqrt{5}, 2-\sqrt{5})$	
$d=6$	$(-4+2\sqrt{6}, 5-2\sqrt{6})$	
$d \equiv 3 \pmod 8$, $d \neq 3$	none	
$d \equiv 5 \pmod 8$, $d \neq 5$	none	
$d \equiv 7 \pmod 8$	$(2^{2s+1}+2^{s+1}w\sqrt{d},\ 1-2^{2s+1}-2^{s+1}w\sqrt{d})$	$4^s-1=dw^2$, $s \geq 2,\ w \neq 0$
$d \equiv 2 \pmod{16}$, $d \neq 2$	$(-2^{2s}+2^s w\sqrt{d}, 1+2^{2s}-2^s w\sqrt{d})$	$4^s+2=dw^2$, $s \geq 2,\ w \neq 0$
$d \equiv 6 \pmod{16}$, $d \neq 6$	none	
$d \equiv 10 \pmod{16}$	none	
$d \equiv 14 \pmod{16}$	$(2^{2s}+2^s w\sqrt{d}, 1-2^{2s}-2^s w\sqrt{d})$	$4^s-2=dw^2$, $s \geq 2,\ w \neq 0$

1) Modularity of the Frey curves

After progress with modularity lifting by **Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, . . .**

1) Modularity of the Frey curves

After progress with modularity lifting by **Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, ...**

Theorem (Le Hung–F.–Siksek)

Let K be a totally real field. There are at most finitely many j-invariants of elliptic curves over K that are non-modular.

1) Modularity of the Frey curves

After progress with modularity lifting by **Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, . . .**

Theorem (Le Hung–F.–Siksek)

Let K be a totally real field. There are at most finitely many j-invariants of elliptic curves over K that are non-modular.

Corollary

There is some constant A_K, depending only on K, such that for $p \geq A_K$ the Frey curve $E : Y^2 = X(X - a^p)(X + b^p)$ is modular.

1) Modularity of the Frey curves

After progress with modularity lifting by **Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, . . .**

Theorem (Le Hung–F.–Siksek)

Let K be a totally real field. There are at most finitely many j-invariants of elliptic curves over K that are non-modular.

Corollary

There is some constant A_K, depending only on K, such that for $p \geq A_K$ the Frey curve $E : Y^2 = X(X - a^p)(X + b^p)$ is modular.

Theorem (Le Hung–F.–Siksek)

Let $\mathcal{C}/K$ be a an elliptic curve over a real quadratic field K. Then $\mathcal{C}$ is modular over K.

Back to the original proof

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | v_\ell(\Delta)}} \ell.$$

Back to the original proof

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = (q).$$

Back to the original proof

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = (q).$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Back to the original proof

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose $a, b, c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = (q).$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

By Tate's algorithm, E has additive reduction at q. So $q^2 \mid\mid N$.

Back to the original proof

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = (q).$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

By Tate's algorithm, E has additive reduction at q. So $q^2 \mid\mid N$.
Thus $N(\overline{\rho}_p) = 2q^2$.

Back to the original proof

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = (q).$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

By Tate's algorithm, E has additive reduction at q. So $q^2 \mid\mid N$. Thus $N(\overline{\rho}_p) = 2q^2$.

Number of newforms of weight 2 and level $2q^2$ is roughly $q^2/6$.

Back to the original proof

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = (q).$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

By Tate's algorithm, E has additive reduction at q. So $q^2 \mid\mid N$. Thus $N(\overline{\rho}_p) = 2q^2$.

Number of newforms of weight 2 and level $2q^2$ is roughly $q^2/6$.

Fortunate Fact: $h(\mathbb{Q}) = 1$.

Class Group

Let K be a totally real number field.

Convention: Choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h \nmid 6$ that are representatives for the class group $\mathrm{Cl}(K)$ and have smallest possible norm.

Class Group

Let K be a totally real number field.

Convention: Choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h \nmid 6$ that are representatives for the class group $\mathrm{Cl}(K)$ and have smallest possible norm.

Suppose (a, b, c) is a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Class Group

Let K be a totally real number field.

Convention: Choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h \nmid 6$ that are representatives for the class group $\mathrm{Cl}(K)$ and have smallest possible norm.

Suppose (a, b, c) is a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Write $\gcd(a, b, c) = a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K$. Then, in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}_i], \qquad \text{for some } i.$$

Class Group

Let K be a totally real number field.

Convention: Choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h \nmid 6$ that are representatives for the class group $\mathrm{Cl}(K)$ and have smallest possible norm.

Suppose (a, b, c) is a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Write $\gcd(a, b, c) = a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K$. Then, in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}_i], \qquad \text{for some } i.$$

By appropriate scaling $\gcd(a, b, c) = \mathfrak{p}_i$ for some i.

Class Group

Let K be a totally real number field.

Convention: Choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h \nmid 6$ that are representatives for the class group $\mathrm{Cl}(K)$ and have smallest possible norm.

Suppose (a, b, c) is a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Write $\gcd(a, b, c) = a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K$. Then, in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}_i], \qquad \text{for some } i.$$

By appropriate scaling $\gcd(a, b, c) = \mathfrak{p}_i$ for some i.

Then, by Tate's algorithm the conductor of the Frey curve is

$$\mathcal{N} = \mathfrak{p}_i^2 \cdot \prod_{\mathfrak{P} \mid 2} \mathfrak{P}^{u_\mathfrak{P}} \cdot \prod_{\mathfrak{q} \nmid 2\mathfrak{p}_i} \mathfrak{q}, \quad \text{thus} \quad N(\overline{\rho}_p) = \mathfrak{p}_i^2 \cdot \prod_{\mathfrak{P} \mid 2} \mathfrak{P}^{u_\mathfrak{P}}.$$

Level Lowering—after Fujiwara, Jarvis and Rajaei

Let E/K an elliptic curve of conductor $\mathcal{N}$. Denote by $\Delta_{\mathfrak{q}}$ the discriminant of a local minimal model for E at $\mathfrak{q}$. Let

$$\mathcal{M}_p := \prod_{\substack{\mathfrak{q} \| \mathcal{N}, \\ p \mid \mathrm{ord}_{\mathfrak{q}}(\Delta_{\mathfrak{q}})}} \mathfrak{q}, \qquad N(\bar{\rho}_{E,p}) := \frac{\mathcal{N}}{\mathcal{M}_p}. \tag{2}$$

Level Lowering—after Fujiwara, Jarvis and Rajaei

Let E/K an elliptic curve of conductor $\mathcal{N}$. Denote by $\Delta_\mathfrak{q}$ the discriminant of a local minimal model for E at $\mathfrak{q}$. Let

$$\mathcal{M}_p := \prod_{\substack{\mathfrak{q} \| \mathcal{N}, \\ p \mid \mathrm{ord}_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}, \qquad N(\bar{\rho}_{E,p}) := \frac{\mathcal{N}}{\mathcal{M}_p}. \tag{2}$$

Theorem (Level Lowering recipe)

With the above notation, suppose the following

(i) $p \geq 5$ *and* p *is unramified in* K,

(ii) E *is modular,*

(iii) $\overline{\rho}_{E,p}$ *is irreducible,*

(iv) E *is semistable at all* $\mathfrak{p} \mid p$,

(v) $p \mid \mathrm{ord}_\mathfrak{p}(\Delta_\mathfrak{p})$ *for all* $\mathfrak{p} \mid p$.

Then, there is a Hilbert eigenform $\mathfrak{f}$ *of parallel weight 2 that is new at level* $N(\bar{\rho}_{E,p})$ *and some* $\lambda \mid p$ *in* $\mathbb{Q}_\mathfrak{f}$ *such that* $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\lambda}$.

Level Lowering for the Frey curves

Recall that to a solution of

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0,$$

we associate the Frey curve $\qquad E : Y^2 = X(X - a^p)(X + b^p).$

Level Lowering for the Frey curves

Recall that to a solution of

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0,$$

we associate the Frey curve $\qquad E : Y^2 = X(X - a^p)(X + b^p).$

Write $\overline{\rho}_p$ for the representation arising from the p-torsion of E.

Level Lowering for the Frey curves

Recall that to a solution of

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0,$$

we associate the Frey curve $\qquad E : Y^2 = X(X - a^p)(X + b^p).$

Write $\overline{\rho}_p$ for the representation arising from the p-torsion of E.

Fact

There is a constant C'_K such that $\overline{\rho}_p$ is irreducible for all $p > C'_K$.

Level Lowering for the Frey curves

Recall that to a solution of

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0,$$

we associate the Frey curve $\qquad E : Y^2 = X(X - a^p)(X + b^p).$

Write $\overline{\rho}_p$ for the representation arising from the p-torsion of E.

Fact

There is a constant C'_K such that $\overline{\rho}_p$ is irreducible for all $p > C'_K$.

Corollary (of Level Lowering)

There is some constant B_K such that if $p > B_K$ then $\overline{\rho}_p$ arises from a Hilbert eigenform $\mathfrak{f}$ of level $N(\overline{\rho}_p)$.

Level Lowering for the Frey curves

Recall that to a solution of

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0,$$

we associate the Frey curve $\qquad E : Y^2 = X(X - a^p)(X + b^p).$

Write $\overline{\rho}_p$ for the representation arising from the p-torsion of E.

Fact

There is a constant C'_K such that $\overline{\rho}_p$ is irreducible for all $p > C'_K$.

Corollary (of Level Lowering)

There is some constant B_K such that if $p > B_K$ then $\overline{\rho}_p$ arises from a Hilbert eigenform $\mathfrak{f}$ of level $N(\overline{\rho}_p)$.

Theorem

Let K be a totally real field satisfying assumption **(ES)**. *There is a constant C_K such that for $p > C_K$ then $\mathfrak{f}$ corresponds to an elliptic curve E' defined over K with full 2-torsion.*

Elliptic Curves with Full 2-Torsion

Corollary

For $p > C_K$ then there is an elliptic curve E'/K of conductor $N(\overline{\rho}_p)$ with full 2-torsion such that

$$\overline{\rho}_p \sim \overline{\rho}'_p$$

where $\overline{\rho}'_p$ arises from the p-torsion of E'.

Elliptic Curves with Full 2-Torsion

Corollary

For $p > C_K$ then there is an elliptic curve E'/K of conductor $N(\overline{\rho}_p)$ with full 2-torsion such that

$$\overline{\rho}_p \sim \overline{\rho}'_p$$

where $\overline{\rho}'_p$ arises from the p-torsion of E'.

Objective: We want to control elliptic curves E' with full 2-torsion and conductor

$$N(\overline{\rho}_p) = \mathfrak{p}^2 \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{u_{\mathfrak{P}}}, \qquad \mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}.$$

Elliptic Curves with Full 2-Torsion

Corollary

For $p > C_K$ then there is an elliptic curve E'/K of conductor $N(\overline{\rho}_p)$ with full 2-torsion such that

$$\overline{\rho}_p \sim \overline{\rho}'_p$$

where $\overline{\rho}'_p$ arises from the p-torsion of E'.

Objective: We want to control elliptic curves E' with full 2-torsion and conductor

$$N(\overline{\rho}_p) = \mathfrak{p}^2 \cdot \prod_{\mathfrak{P} \mid 2} \mathfrak{P}^{u_{\mathfrak{P}}}, \qquad \mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}.$$

We can write E' as

$$E' : y^2 = x(x-r)(x+s), \qquad r+s+t=0, \qquad r,s,t \in \mathcal{O}_K \backslash \{0\}.$$

Elliptic Curves with Full 2-Torsion

We want elliptic curves E' with full 2-torsion and conductor

$$N(\overline{\rho}_p) = \mathfrak{p}^2 \cdot \prod_{\mathfrak{P} | 2} \mathfrak{P}^{u_{\mathfrak{P}}}, \qquad \mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}.$$

$$E' : y^2 = x(x-r)(x+s), \qquad r+s+t=0, \qquad r,s,t \in \mathcal{O}_K \backslash \{0\}.$$

Elliptic Curves with Full 2-Torsion

We want elliptic curves E' with full 2-torsion and conductor

$$N(\overline{\rho}_p) = \mathfrak{p}^2 \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{u_\mathfrak{P}}, \qquad \mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}.$$

$$E' : y^2 = x(x-r)(x+s), \qquad r+s+t=0, \qquad r,s,t \in \mathcal{O}_K \backslash \{0\}.$$

Write

$$(r) = \mathfrak{p}^\alpha \cdot \prod \mathfrak{q}^{\lambda_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^? \quad (s) = \mathfrak{p}^\beta \cdot \prod \mathfrak{q}^{\mu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^? \quad (t) = \mathfrak{p}^\gamma \cdot \prod \mathfrak{q}^{\nu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^?$$

where $\mathfrak{q} \nmid (2) \cdot \mathfrak{p}$.

Elliptic Curves with Full 2-Torsion

We want elliptic curves E' with full 2-torsion and conductor

$$N(\overline{\rho}_p) = \mathfrak{p}^2 \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{u_\mathfrak{P}}, \qquad \mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}.$$

$$E' : y^2 = x(x-r)(x+s), \qquad r+s+t=0, \qquad r, s, t \in \mathcal{O}_K \backslash \{0\}.$$

Write

$$(r) = \mathfrak{p}^\alpha \cdot \prod \mathfrak{q}^{\lambda_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^? \quad (s) = \mathfrak{p}^\beta \cdot \prod \mathfrak{q}^{\mu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^? \quad (t) = \mathfrak{p}^\gamma \cdot \prod \mathfrak{q}^{\nu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^?$$

where $\mathfrak{q} \nmid (2) \cdot \mathfrak{p}$. From Tate's Algorithm:

For all $\mathfrak{q}$,

$$\lambda_\mathfrak{q} = \mu_\mathfrak{q} = \nu_\mathfrak{q} \in 2\mathbb{Z}.$$

$\min\{\alpha, \beta, \gamma\} \in 2\mathbb{Z}+1.$

Elliptic Curves with Full 2-Torsion

Write where $\mathfrak{q} \nmid (2) \cdot \mathfrak{p}$.

$$(r) = \mathfrak{p}^{\alpha} \cdot \prod \mathfrak{q}^{\lambda_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (s) = \mathfrak{p}^{\beta} \cdot \prod \mathfrak{q}^{\mu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (t) = \mathfrak{p}^{\gamma} \cdot \prod \mathfrak{q}^{\nu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?}$$

From Tate's Algorithm:

For all $\mathfrak{q}$,

$$\lambda_\mathfrak{q} = \mu_\mathfrak{q} = \nu_\mathfrak{q} \in 2\mathbb{Z}.$$

$\min\{\alpha, \beta, \gamma\} \in 2\mathbb{Z} + 1.$

Elliptic Curves with Full 2-Torsion

Write where $\mathfrak{q} \nmid (2) \cdot \mathfrak{p}$.

$$(r) = \mathfrak{p}^{\alpha} \cdot \prod \mathfrak{q}^{\lambda_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (s) = \mathfrak{p}^{\beta} \cdot \prod \mathfrak{q}^{\mu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (t) = \mathfrak{p}^{\gamma} \cdot \prod \mathfrak{q}^{\nu_\mathfrak{q}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?}$$

From Tate's Algorithm:

For all $\mathfrak{q}$,

$$\lambda_\mathfrak{q} = \mu_\mathfrak{q} = \nu_\mathfrak{q} \in 2\mathbb{Z}.$$

$\min\{\alpha, \beta, \gamma\} \in 2\mathbb{Z} + 1$. WLOG $\alpha = 2u + 1$.

Elliptic Curves with Full 2-Torsion

Write where $\mathfrak{q} \nmid (2) \cdot \mathfrak{p}$.

$$(r) = \mathfrak{p}^{\alpha} \cdot \prod \mathfrak{q}^{\lambda_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (s) = \mathfrak{p}^{\beta} \cdot \prod \mathfrak{q}^{\mu_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (t) = \mathfrak{p}^{\gamma} \cdot \prod \mathfrak{q}^{\nu_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?}$$

From Tate's Algorithm:

For all $\mathfrak{q}$,

$$\lambda_{\mathfrak{q}} = \mu_{\mathfrak{q}} = \nu_{\mathfrak{q}} \in 2\mathbb{Z}.$$

$\min\{\alpha, \beta, \gamma\} \in 2\mathbb{Z} + 1$. WLOG $\alpha = 2u + 1$. Write $\lambda_{\mathfrak{q}} = 2\delta_{\mathfrak{q}}$.

Elliptic Curves with Full 2-Torsion

Write where $\mathfrak{q} \nmid (2) \cdot \mathfrak{p}$.

$$(r) = \mathfrak{p}^{\alpha} \cdot \prod \mathfrak{q}^{\lambda_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (s) = \mathfrak{p}^{\beta} \cdot \prod \mathfrak{q}^{\mu_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (t) = \mathfrak{p}^{\gamma} \cdot \prod \mathfrak{q}^{\nu_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?}$$

From Tate's Algorithm:

For all $\mathfrak{q}$,

$$\lambda_{\mathfrak{q}} = \mu_{\mathfrak{q}} = \nu_{\mathfrak{q}} \in 2\mathbb{Z}.$$

$\min\{\alpha, \beta, \gamma\} \in 2\mathbb{Z} + 1$. WLOG $\alpha = 2u + 1$. Write $\lambda_{\mathfrak{q}} = 2\delta_{\mathfrak{q}}$.

Then

$$(r) = \mathfrak{p} \cdot \left(\mathfrak{p}^{u} \cdot \prod \mathfrak{q}^{\delta_{\mathfrak{q}}}\right)^2 \prod_{\mathfrak{P}|2} \mathfrak{P}^{?}.$$

Elliptic Curves with Full 2-Torsion

Write where $\mathfrak{q} \nmid (2) \cdot \mathfrak{p}$.

$$(r) = \mathfrak{p}^{\alpha} \cdot \prod \mathfrak{q}^{\lambda_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (s) = \mathfrak{p}^{\beta} \cdot \prod \mathfrak{q}^{\mu_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?} \quad (t) = \mathfrak{p}^{\gamma} \cdot \prod \mathfrak{q}^{\nu_{\mathfrak{q}}} \cdot \prod_{\mathfrak{P}|2} \mathfrak{P}^{?}$$

From Tate's Algorithm:

For all $\mathfrak{q}$,

$$\lambda_{\mathfrak{q}} = \mu_{\mathfrak{q}} = \nu_{\mathfrak{q}} \in 2\mathbb{Z}.$$

$\min\{\alpha, \beta, \gamma\} \in 2\mathbb{Z} + 1$. WLOG $\alpha = 2u + 1$. Write $\lambda_{\mathfrak{q}} = 2\delta_{\mathfrak{q}}$.

Then

$$(r) = \mathfrak{p} \cdot \left(\mathfrak{p}^{u} \cdot \prod \mathfrak{q}^{\delta_{\mathfrak{q}}}\right)^2 \prod_{\mathfrak{P}|2} \mathfrak{P}^{?}.$$

Hence

$$[\mathfrak{p}] = [\mathfrak{a}]^2 \prod_{\mathfrak{P}|2} [\mathfrak{P}]^{?} \qquad \text{in } \mathrm{Cl}(K).$$

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Started with (a, b, c) a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Started with (a, b, c) a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Noted that in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}],$$

where $\mathfrak{p}$ is one of the representatives $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ of $\mathrm{Cl}(K)$.

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Started with (a, b, c) a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Noted that in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}],$$

where $\mathfrak{p}$ is one of the representatives $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ of $\mathrm{Cl}(K)$.
We scaled a, b, c so that $\gcd(a, b, c) = \mathfrak{p}$.

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Started with (a, b, c) a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Noted that in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}],$$

where $\mathfrak{p}$ is one of the representatives $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ of $\mathrm{Cl}(K)$.
We scaled a, b, c so that $\gcd(a, b, c) = \mathfrak{p}$.
We found (for $p > C_K$) $[\gcd(a, b, c)] = [\mathfrak{p}] = [\mathfrak{a}]^2 \prod_{\mathfrak{P}|2} [\mathfrak{P}]^?$.

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Started with (a, b, c) a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Noted that in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}],$$

where $\mathfrak{p}$ is one of the representatives $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ of $\mathrm{Cl}(K)$.
We scaled a, b, c so that $\gcd(a, b, c) = \mathfrak{p}$.
We found (for $p > C_K$) $[\gcd(a, b, c)] = [\mathfrak{p}] = [\mathfrak{a}]^2 \prod_{\mathfrak{P}|2} [\mathfrak{P}]^?$.
Thus

$$[\gcd(a, b, c)] = [\mathfrak{p}']^2 \prod_{\mathfrak{P}|2} [\mathfrak{P}]^?, \qquad \mathfrak{p}' \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}.$$

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Started with (a, b, c) a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K, \qquad abc \neq 0.$$

Noted that in $\mathrm{Cl}(K)$

$$[\gcd(a, b, c)] = [\mathfrak{p}],$$

where $\mathfrak{p}$ is one of the representatives $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ of $\mathrm{Cl}(K)$.
We scaled a, b, c so that $\gcd(a, b, c) = \mathfrak{p}$.
We found (for $p > C_K$) $[\gcd(a, b, c)] = [\mathfrak{p}] = [\mathfrak{a}]^2 \prod_{\mathfrak{P}|2} [\mathfrak{P}]^?$.
Thus

$$[\gcd(a, b, c)] = [\mathfrak{p}']^2 \prod_{\mathfrak{P}|2} [\mathfrak{P}]^?, \qquad \mathfrak{p}' \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}.$$

Can rescale (a, b, c) so that

$$\gcd(a, b, c) = \mathfrak{p}'^2 \prod_{\mathfrak{P}|2} \mathfrak{P}^?.$$

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Can rescale (a, b, c) so that

$$\gcd(a, b, c) = \mathfrak{p}'^2 \prod_{\mathfrak{P}|2} \mathfrak{P}^?.$$

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Can rescale (a, b, c) so that

$$\gcd(a, b, c) = \mathfrak{p}'^2 \prod_{\mathfrak{P} \mid 2} \mathfrak{P}^{?}.$$

So, again by Tate's algorithm, $E_{(a,b,c)}$ is semistable at $\mathfrak{p}'$, thus

$$N(\overline{\rho}_p) = \prod_{\mathfrak{P} \mid 2} \mathfrak{P}^{?}.$$

2) Removing the dependence of $N(\overline{\rho}_p)$ on the solution

Can rescale (a, b, c) so that

$$\gcd(a, b, c) = \mathfrak{p}'^2 \prod_{\mathfrak{P}|2} \mathfrak{P}^?.$$

So, again by Tate's algorithm, $E_{(a,b,c)}$ is semistable at $\mathfrak{p}'$, thus

$$N(\overline{\rho}_p) = \prod_{\mathfrak{P}|2} \mathfrak{P}^?.$$

Corollary (of Level Lowering)

There is a constant D_K such that for $p > D_K$ there is an elliptic curve E'/K of conductor $N(\overline{\rho}_p) = \prod_{\mathfrak{P}|2} \mathfrak{P}^?$ with full 2-torsion such that

$$\overline{\rho}_p \sim \overline{\rho}'_p$$

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes.

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$ (gives singular E')

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$ (gives singular E')

$1^p + \omega^p + (\omega^2)^p = 0$

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$ (gives singular E')

$1^p + \omega^p + (\omega^2)^p = 0$ (gives E' of conductor 144)

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$ (gives singular E')

$1^p + \omega^p + (\omega^2)^p = 0$ (gives E' of conductor 144)

$1^p + 1^p = 2 \times 1^p$

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$ (gives singular E')

$1^p + \omega^p + (\omega^2)^p = 0$ (gives E' of conductor 144)

$1^p + 1^p = 2 \times 1^p$ (TROUBLE!!)

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$ (gives singular E')

$1^p + \omega^p + (\omega^2)^p = 0$ (gives E' of conductor 144)

$1^p + 1^p = 2 \times 1^p$ (TROUBLE!!)

$$E' \; : \; y^2 = x(x-1)(x+1) \qquad (32A2), \qquad j = 1728.$$

has conductor $\prod_{\mathfrak{P}|2} \mathfrak{P}^?$.

3) Non-empty space of newforms at level $N(\overline{\rho}_p)$

We have $\overline{\rho}_p \sim \overline{\rho}'_p$ for some E' with full 2-torsion and good reduction outside primes dividing 2.

Question: Are there candidates for E'?

Unfortunately, yes. For example, we can get candidates from 'solutions':

solutions satisfying $abc = 0$ (gives singular E')

$1^p + \omega^p + (\omega^2)^p = 0$ (gives E' of conductor 144)

$1^p + 1^p = 2 \times 1^p$ (TROUBLE!!)

$$E' \ : \ y^2 = x(x-1)(x+1) \qquad (32A2), \qquad j = 1728.$$

has conductor $\prod_{\mathfrak{P}|2} \mathfrak{P}^?$.

Question: Can we rule out $\overline{\rho}_p \sim \overline{\rho}'_p$?

Candidates for E'

Suppose $T \neq \emptyset$**:** there exists $\mathfrak{P} \mid 2$ in K such that $f(\mathfrak{P}/2) = 1$, i.e. $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$.

Candidates for E'

Suppose $T \neq \emptyset$**:** there exists $\mathfrak{P} \mid 2$ in K such that $f(\mathfrak{P}/2) = 1$, i.e. $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$.

As $a^p + b^p + c^p = 0$, one of $\upsilon_{\mathfrak{P}}(a^p)$, $\upsilon_{\mathfrak{P}}(b^p)$, $\upsilon_{\mathfrak{P}}(c^p)$ is much larger than the others. Write $E = E_{a,b,c}$.

Candidates for E'

Suppose $T \neq \emptyset$**:** there exists $\mathfrak{P} \mid 2$ in K such that $f(\mathfrak{P}/2) = 1$, i.e. $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$.

As $a^p + b^p + c^p = 0$, one of $\upsilon_{\mathfrak{P}}(a^p)$, $\upsilon_{\mathfrak{P}}(b^p)$, $\upsilon_{\mathfrak{P}}(c^p)$ is much larger than the others. Write $E = E_{a,b,c}$. Then, for large p,

- we have $\mathrm{ord}_{\mathfrak{P}}(j(E)) < 0$,

Candidates for E'

Suppose $T \neq \emptyset$: there exists $\mathfrak{P} \mid 2$ in K such that $f(\mathfrak{P}/2) = 1$, i.e. $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$.

As $a^p + b^p + c^p = 0$, one of $\upsilon_{\mathfrak{P}}(a^p)$, $\upsilon_{\mathfrak{P}}(b^p)$, $\upsilon_{\mathfrak{P}}(c^p)$ is much larger than the others. Write $E = E_{a,b,c}$. Then, for large p,

- we have $\mathrm{ord}_{\mathfrak{P}}(j(E)) < 0$, hence $E/K_{\mathfrak{P}}$ is a Tate curve (after possibly taking a quadratic extension)
- and $p \nmid \mathrm{ord}_{\mathfrak{P}}(j(E))$,

Candidates for E'

Suppose $T \neq \emptyset$: there exists $\mathfrak{P} \mid 2$ in K such that $f(\mathfrak{P}/2) = 1$, i.e. $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$.

As $a^p + b^p + c^p = 0$, one of $\upsilon_{\mathfrak{P}}(a^p)$, $\upsilon_{\mathfrak{P}}(b^p)$, $\upsilon_{\mathfrak{P}}(c^p)$ is much larger than the others. Write $E = E_{a,b,c}$. Then, for large p,

- we have $\mathrm{ord}_{\mathfrak{P}}(j(E)) < 0$, hence $E/K_{\mathfrak{P}}$ is a Tate curve (after possibly taking a quadratic extension)
- and $p \nmid \mathrm{ord}_{\mathfrak{P}}(j(E))$, hence $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.

Candidates for E'

Suppose $T \neq \emptyset$**:** there exists $\mathfrak{P} \mid 2$ in K such that $f(\mathfrak{P}/2) = 1$, i.e. $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$.

As $a^p + b^p + c^p = 0$, one of $\upsilon_{\mathfrak{P}}(a^p)$, $\upsilon_{\mathfrak{P}}(b^p)$, $\upsilon_{\mathfrak{P}}(c^p)$ is much larger than the others. Write $E = E_{a,b,c}$. Then, for large p,

- we have $\mathrm{ord}_{\mathfrak{P}}(j(E)) < 0$, hence $E/K_{\mathfrak{P}}$ is a Tate curve (after possibly taking a quadratic extension)
- and $p \nmid \mathrm{ord}_{\mathfrak{P}}(j(E))$, hence $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.

On the other hand,

- The curve E' has potentially good reduction at $\mathfrak{P}$;

Candidates for E'

Suppose $T \neq \emptyset$**:** there exists $\mathfrak{P} \mid 2$ in K such that $f(\mathfrak{P}/2) = 1$, i.e. $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$.

As $a^p + b^p + c^p = 0$, one of $\upsilon_{\mathfrak{P}}(a^p)$, $\upsilon_{\mathfrak{P}}(b^p)$, $\upsilon_{\mathfrak{P}}(c^p)$ is much larger than the others. Write $E = E_{a,b,c}$. Then, for large p,

- we have $\mathrm{ord}_{\mathfrak{P}}(j(E)) < 0$, hence $E/K_{\mathfrak{P}}$ is a Tate curve (after possibly taking a quadratic extension)
- and $p \nmid \mathrm{ord}_{\mathfrak{P}}(j(E))$, hence $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.

On the other hand,

- The curve E' has potentially good reduction at $\mathfrak{P}$;

  Hence, $\overline{\rho}_{E',p}(I_{\mathfrak{P}})$ has order 1, 2, 3, 4, 6 or 24;

  This gives a contradiction for $p \geq 5$!

Candidates for E'

Theorem

Let K be a totally real field satisfying assumption **(ES)**. *There is a constant B_K depending only on K such that the following hold. Let (a, b, c) be a non-trivial solution to the Fermat equation with prime exponent $p > B_K$. Then, after proper rescaling, there is an elliptic curve E' over K such that*

(i) *the conductor of E' is divisible only by primes in S;*

(ii) $\#E'(K)[2] = 4$;

(iii) $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$;

Write j' for the j-invariant of E'. Then,

(a) *for $\mathfrak{P} \in T$, we have $\mathrm{ord}_{\mathfrak{P}}(j') < 0$;*

(b) *for $\mathfrak{P} \in U$, we have either $\mathrm{ord}_{\mathfrak{P}}(j') < 0$ or $3 \nmid \mathrm{ord}_{\mathfrak{P}}(j')$.*

Results – Fermat over totally real fields

Theorem (F.–Siksek)

Let K be a totally real field satisfying assumption **(ES)**. *Let S, T and U be as before. Write $\mathcal{O}_S^*$ for the set of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \qquad \lambda,\, \mu \in \mathcal{O}_S^*\,.$$

there is

(A) either some $\mathfrak{P} \in T$ that satisfies

$$\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}}(\mu)|\} \leq 4\,\mathrm{ord}_{\mathfrak{P}}(2), \tag{3}$$

(B) or some $\mathfrak{P} \in U$ that satisfies both (3) *and*

$$\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) \equiv \mathrm{ord}_{\mathfrak{P}}(2) \pmod 3.$$

Then there is some constant B_K such that for all $p > B_K$, the Fermat equation with exponent p has no non-trivial solutions.

Results – a density theorem

For a subset $\mathcal{U} \subseteq \mathbb{N}^{\mathrm{sf}}$, define the **relative density of $\mathcal{U}$** as

$$\delta_{\mathrm{rel}}(\mathcal{U}) = \lim_{X \to \infty} \frac{\#\{d \in \mathcal{U} : d \leq X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} : d \leq X\}}.$$

Results – a density theorem

For a subset $\mathcal{U} \subseteq \mathbb{N}^{\mathrm{sf}}$, define the **relative density of $\mathcal{U}$** as

$$\delta_{\mathrm{rel}}(\mathcal{U}) = \lim_{X \to \infty} \frac{\#\{d \in \mathcal{U} : d \leq X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} : d \leq X\}}.$$

Define also

$$\mathcal{C} = \{d \in \mathbb{N}^{\mathrm{sf}} : \text{the } S\text{-unit equation has no relevant solutions in } \mathbb{Q}(\sqrt{d})\}$$

$$\mathcal{D} = \{d \in \mathcal{C} \ : \ d \not\equiv 5 \pmod 8\}.$$

Results – a density theorem

For a subset $\mathcal{U} \subseteq \mathbb{N}^{\mathrm{sf}}$, define the **relative density of $\mathcal{U}$** as

$$\delta_{\mathrm{rel}}(\mathcal{U}) = \lim_{X \to \infty} \frac{\#\{d \in \mathcal{U} : d \le X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} : d \le X\}}.$$

Define also

$$\mathcal{C} = \{d \in \mathbb{N}^{\mathrm{sf}} : \text{the } S\text{-unit equation has no relevant solutions in } \mathbb{Q}(\sqrt{d})\}$$

$$\mathcal{D} = \{d \in \mathcal{C} \ : \ d \not\equiv 5 \pmod 8\}.$$

Theorem

Let $\mathcal{C}$ and $\mathcal{D}$ be as above. Then

$$\delta_{\mathrm{rel}}(\mathcal{C}) = 1, \qquad \delta_{\mathrm{rel}}(\mathcal{D}) = \frac{5}{6}. \tag{4}$$

Results – a density theorem

For a subset $\mathcal{U} \subseteq \mathbb{N}^{\mathrm{sf}}$, define the **relative density of $\mathcal{U}$** as

$$\delta_{\mathrm{rel}}(\mathcal{U}) = \lim_{X\to\infty} \frac{\#\{d \in \mathcal{U} : d \le X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} : d \le X\}}.$$

Define also

$$\mathcal{C} = \{d \in \mathbb{N}^{\mathrm{sf}} : \text{the } S\text{-unit equation has no relevant solutions in } \mathbb{Q}(\sqrt{d})\}$$
$$\mathcal{D} = \{d \in \mathcal{C} \;:\; d \not\equiv 5 \pmod 8\}.$$

Theorem

Let $\mathcal{C}$ and $\mathcal{D}$ be as above. Then

$$\delta_{\mathrm{rel}}(\mathcal{C}) = 1, \qquad \delta_{\mathrm{rel}}(\mathcal{D}) = \frac{5}{6}. \tag{4}$$

Furthermore, if $d \in \mathcal{D}$ and $K = \mathbb{Q}(\sqrt{d})$, then there is some effectively computable B_K such that for $p > B_K$ the Fermat equation has no non-trivial solutions with exponent p. The same conclusion holds for $d \in \mathcal{C}$ if we assume **(ES)**.

The End!