The modular approach for solving $x^r + y^r = z^p$ over totally real fields

Diana Mocanu

THE UNIVERSITY OF WARWICK

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}. \tag{1}$$

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}. \tag{1}$$

Conjecture(Fermat-Catalan)

Over all choices of prime exponents p, q, r satisfying $1/p + 1/q + 1/r < 1$ the equation (1) admits only finitely many integer solutions (a, b, c) which are non-trivial (i.e. $abc \neq 0$) coprime (i.e. $\gcd(a, b, c) = 1$). (Here solutions like $2^3 + 1^q = 3^2$ are counted only once.)

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

Theorem(Darmon-Granville 1995)

If we fix the prime exponents p, q, r such that $1/p + 1/q + 1/r < 1$, then there are only finitely many coprime solutions to the above equation.

The Theorem can be extended easily to coprime solutions in any fixed number field.

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

We call (p, q, r) **the signature** of the equation.

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

We call (p, q, r) **the signature** of the equation.
Some families of signatures that have been solved:

- $(n, n, n), n \geq 3$ Wiles, Taylor–Wiles 1995;
- $(n, n, 2), n \geq 4$ and $(n, n, 3), n \geq 3$ Darmon–Merel, Poonen 1998;
- $(3j, 3k, n), j, k \geq 2, n \geq 3$ Kraus 1998;
- $(2n, 2n, 5), n \geq 2$ Bennett 2006;
- $(2l, 2m, p), p = 3, 5, 7, 11, l, m \geq 5$, Anni-Siksek 2016;

Modular Forms

Let $\mathbb{H} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$. This is **the upper half plane**.

Modular Forms

Let $\mathbb{H} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$. This is **the upper half plane**.

Definition

A level N modular form of weight 2 is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying:

1. for $z \in \mathbb{H}$,
$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$
whenever $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$ and $N|c$.
2. f is required to be bounded as $z \to i\infty$

Modular Forms

Let $\mathbb{H} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$. This is **the upper half plane**.

Definition

A level N modular form of weight 2 is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying:

1. for $z \in \mathbb{H}$,
$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$
whenever $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$ and $N|c$.
2. f is required to be bounded as $z \to i\infty$

Note that f has a Fourier (or q-expansion):

$$f = \sum_{n=0}^{\infty} c_n q^n,$$

where $c_n \in \mathbb{C}, q = e^{\frac{2\pi i}{z}}$.

Hilbert Modular Forms

- A **Hilbert Modular Form** is a generalization of modular forms in higher dimensions.

Hilbert Modular Forms

- A **Hilbert Modular Form** is a generalization of modular forms in higher dimensions.
- Let K be a totally real number field and $\mathcal{O}_K$ its ring of integers and $\sigma_1, \dots \sigma_m$ the real embeddings of K.

Hilbert Modular Forms

- A **Hilbert Modular Form** is a generalization of modular forms in higher dimensions.
- Let K be a totally real number field and $\mathcal{O}_K$ its ring of integers and $\sigma_1, \dots \sigma_m$ the real embeddings of K.

Definition

A level $\mathcal{N}$ Hilbert modular form of parallel weight $(2, \cdots, 2)$ is an analytic function $f\colon \mathbb{H}^m \to \mathbb{C}$ satisfying for $z = (z_1, \cdot, z_m) \in \mathbb{H}^m$:

$$f\left(\frac{\sigma_1(a)z_1 + \sigma_1(b)}{\sigma_1(c)z_1 + \sigma_1(d)}, \cdots, \frac{\sigma_m(a)z_m + \sigma_m(b)}{\sigma_m(c)z_m + \sigma_m(d)}\right) = \prod_{i=1}^{m} \frac{(\sigma_i(c)z_1 + \sigma_i(d))^2}{\sigma_i(a)\sigma_i(c) - \sigma_i(b)\sigma_i(d)} f(z)$$

whenever $a, b, c, d \in \mathcal{O}_K^+$ with $ad - bc \in \mathcal{O}_K^{*+}$ and $\mathcal{N}|c$.

- For a Hilbert newform $\mathfrak{f}$ over K, we let $\mathbb{Q}_\mathfrak{f}$ denote the field generated by its eigenvalues and $\rho_{\mathfrak{f},\mathfrak{p}}$ its associated Galois representation, where $\mathfrak{p}|p$ in $\mathbb{Q}_\mathfrak{f}$.

Elliptic curves

From now on let K be a totally real number field. Let E/K be an elliptic curve.

- We write $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for the group of p-torsion points of E;

Elliptic curves

From now on let K be a totally real number field. Let E/K be an elliptic curve.

- We write $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for the group of p-torsion points of E;
- There is a natural action of the absolute Galois group $G_K := \mathrm{Gal}(\bar{K}/K)$ on $E[p]$:

$$\sigma \cdot (x_P, y_P) = (x_P^\sigma, y_P^\sigma)$$

for all $\sigma \in G_K$ and $P = (x_P, y_P) \in E[p]$.

Elliptic curves

From now on let K be a totally real number field. Let E/K be an elliptic curve.

- We write $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for the group of p-torsion points of E;
- There is a natural action of the absolute Galois group $G_K := \mathsf{Gal}(\bar{K}/K)$ on $E[p]$:

$$\sigma \cdot (x_P, y_P) = (x_P^\sigma, y_P^\sigma)$$

  for all $\sigma \in G_K$ and $P = (x_P, y_P) \in E[p]$.
- We write

$$\overline{\rho}_{E,p} : G_K \to \mathsf{Aut}(E[p]) \simeq \mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

  for the representation of G_K on the p-torsion of E.

Modular Method - Sketch

Let K be a totally real number field. We say the **asymptotic Fermat Last Theorem** holds for $x^p + y^p = z^p$ if there is some bound B_K such that for all $p > B_K$, the equation has no non-trivial (i.e. $abc \neq 0$) and coprime (i.e. $a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K = \mathcal{O}_K$) solutions.

Modular Method - Sketch

Let K be a totally real number field. We say the **asymptotic Fermat Last Theorem** holds for $x^p + y^p = z^p$ if there is some bound B_K such that for all $p > B_K$, the equation has no non-trivial (i.e. $abc \neq 0$) and coprime (i.e. $a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K = \mathcal{O}_K$) solutions.

Theorem (Freitas-Siksek, 2014)

Let $d \geq 2$ be squarefree such that $d \equiv 3 \mod 8$. Then the effective asymptotic Fermat's Last Theorem holds over $K = \mathbb{Q}(\sqrt{d})$.

Modular Method - Sketch

Let K be a totally real number field. We say the **asymptotic Fermat Last Theorem** holds for $x^p + y^p = z^p$ if there is some bound B_K such that for all $p > B_K$, the equation has no non-trivial (i.e. $abc \neq 0$) and coprime (i.e. $a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K = \mathcal{O}_K$) solutions.

Theorem (Freitas-Siksek, 2014)

Let $d \geq 2$ be squarefree such that $d \equiv 3 \mod 8$. Then the effective asymptotic Fermat's Last Theorem holds over $K = \mathbb{Q}(\sqrt{d})$.

We divide the modular method into 5 steps.

Modular Method - Sketch

Step 1: Selecting a Frey curve.
Let (a, b, c) be a solution. The Frey curve $E_{a,b,c}/K$ has the property that the Artin conductor of $\overline{\rho}_{E,p}$ is bounded independently of the putative solution.

Modular Method - Sketch

Step 1: Selecting a Frey curve.
Let (a, b, c) be a solution. The Frey curve $E_{a,b,c}/K$ has the property that the Artin conductor of $\overline{\rho}_{E,p}$ is bounded independently of the putative solution.

Example

We take the Frey elliptic curve $E_{a,b,c} : Y^2 = X(X - a^p)(X - b^p)$ over K. It has Artin conductor $\mathcal{N}_p = \prod_{\mathfrak{P}|2} \mathfrak{P}^{r_\mathfrak{P}}$ where $0 \leq r_\mathfrak{P} \leq 6v_\mathfrak{P}(2)$.

Modular Method - Sketch

Step 2: Modularity.
E/K is modular if there exists a Hilbert newform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that the Hasse–Weil L-function of E is equal to the Hecke L-function of $\mathfrak{f}$.

Modular Method - Sketch

Step 2: Modularity.
E/K is modular if there exists a Hilbert newform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that the Hasse–Weil L-function of E is equal to the Hecke L-function of $\mathfrak{f}$.

Theorem (Freitas, Hung and Siksek)

Let K be a totally real field. There are at most finitely many $\bar{K}$- isomorphism classes of non-modular elliptic curves E over K. Moreover, if K is real quadratic, then all elliptic curves over K are modular.

Modular Method - Sketch

Step 2: Modularity.
E/K is modular if there exists a Hilbert newform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that the Hasse–Weil L-function of E is equal to the Hecke L-function of $\mathfrak{f}$.

Theorem (Freitas, Hung and Siksek)

Let K be a totally real field. There are at most finitely many $\bar{K}$- isomorphism classes of non-modular elliptic curves E over K. Moreover, if K is real quadratic, then all elliptic curves over K are modular.

Example

We find a Hilbert newform $\mathfrak{f}$ over K of parallel weight 2 which 'corresponds' to $E_{a,b,c}$.

Modular Method - Sketch

Step 3: Irreducibility.
Freitas and Siksek (2015) proved irreducibility of $\overline{\rho}_{E,p}$ for elliptic curves E/K that are semistable at all $\mathfrak{p}|p$, when p is taken to be large enough.

Modular Method - Sketch

Step 3: Irreducibility.
Freitas and Siksek (2015) proved irreducibility of $\overline{\rho}_{E,p}$ for elliptic curves E/K that are semistable at all $\mathfrak{p}|p$, when p is taken to be large enough.

Example

After possibly enlarging p we get that $\overline{\rho}_{E,p}$ is irreducible.

Modular Method - Sketch

Step 4: Level lowering.
Use level lowering theorems (e.g. Freitas and Siksek 2014), which require irreducibility of $\overline{\rho}_{E,p}$, to conclude that

$$\overline{\rho}_{E,p} \simeq \overline{\rho}_{\mathfrak{f},\pi}$$

where $\mathfrak{f}$ is a Hilbert newform over K of parallel weight 2 with level equal to the Artin conductor of E, where π is a prime in $\mathbb{Q}_{\mathfrak{f}}$ with $\pi | p$.
Note: After possibly enlarging p we can assume $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$ so $\pi = p$.

Modular Method - Sketch

Step 4: Level lowering.
Use level lowering theorems (e.g. Freitas and Siksek 2014), which require irreducibility of $\overline{\rho}_{E,p}$, to conclude that

$$\overline{\rho}_{E,p} \simeq \overline{\rho}_{\mathfrak{f},\pi}$$

where $\mathfrak{f}$ is a Hilbert newform over K of parallel weight 2 with level equal to the Artin conductor of E, where π is a prime in $\mathbb{Q}_{\mathfrak{f}}$ with $\pi | p$.
Note: After possibly enlarging p we can assume $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$ so $\pi = p$.

Example

We find a Hilbert newform over K of parallel weight 2 with level equal to $\mathcal{N}_p$ such that

$$\overline{\rho}_{E_{a,b,c},p} \simeq \overline{\rho}_{\mathfrak{f},\varpi}.$$

Modular Method - Sketch

Step 5: Eliminate. Not easy in general.

Modular Method - Sketch

Step 5: Eliminate. Not easy in general.

Example

A solution due to Freitas and Siksek (2014) involves:

1. an 'Eichler-Shimura'-type result;
2. image of inertia comparison arguments;
3. the study of certain S-unit equations;

to get a contradiction.

Modular Method Recap

Select a Frey Curve - **M**odularity - **I**rreducibility - **L**evel lowering - **E**liminate

Examples signatures $(p, p, 2)$ and $(p, p, 3)$

Theorem (M.,2021)

Let $d \geq 5$ be a rational prime satisfying $d \equiv 5 \mod 8$. Write $K = \mathbb{Q}(\sqrt{d})$. Then, there is a constant B_K such that for each rational prime $p > B_K$, the equation $x^p + y^p = z^2$ has no coprime, non-trivial solutions $(a, b, c) \in \mathcal{O}_K^3$ with $2|b$.

Examples signatures $(p, p, 2)$ and $(p, p, 3)$

Theorem (M.,2021)

Let $d \geq 5$ be a rational prime satisfying $d \equiv 5 \mod 8$. Write $K = \mathbb{Q}(\sqrt{d})$. Then, there is a constant B_K such that for each rational prime $p > B_K$, the equation $x^p + y^p = z^2$ has no coprime, non-trivial solutions $(a, b, c) \in \mathcal{O}_K^3$ with $2|b$.

Theorem (M.,2021)

Let d a positive, square-free satisfying $d \equiv 2 \mod 3$. Write $K = \mathbb{Q}(\sqrt{d})$ and suppose $3 \nmid h_{K(\omega)}$, $3 \nmid h_K$. Then, there is a constant B_K such that for each prime $p > B_K$, the equation $x^p + y^p = z^3$ has no coprime, non-trivial solutions $(a, b, c) \in \mathcal{O}_K^3$ with $3|b$.

Signature (r, r, p)

Fix $r \geq 5$ a rational prime.

$$x^r + y^r = dz^p, \quad p \geq 2.$$

Signature (r, r, p)

Fix $r \geq 5$ a rational prime.

$$x^r + y^r = dz^p, \quad p \geq 2.$$

Some instances that have been partially solved over $\mathbb{Q}$:

- $(7, 7, p)$ with $d = 3$ Freitas 2013;
- $(5, 5, 7), (5, 5, 19)$, and $(7, 7, 5)$ Dahmen, Siksek 2014;
- $(5, 5, n)$ with $d = 1^*, 2^*, 3$, $(13, 13, n)$ with $d = 3$ Billerey, Chen, Dembélé, Dieulefait and Freitas 2022;
- $(11, 11, p)$ with $d = 1^*$ Billerey, Chen, Dieulefait, Freitas and Najman.
- (r, r, p) with $d \neq 1^*$, d has only primes $q \not\equiv 1 \mod r$ for a positive density of primes p, Freitas and Najman 2022.

Asymptotic (r, r, p)

Theorem (1)

Fix $r \geq 5$ such that $r \not\equiv 1 \mod 8$. Let $\mathbb{Q}^+ := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, suppose that 2 is inert in $\mathbb{Q}^+$ and $2 \nmid h^+_{\mathbb{Q}^+}$. Then, there is a constant B_r (depending only on r) such that for each rational prime $p > B_r$, the equation $x^r + y^r = z^p$ has no integer solutions with $2|z$.

Asymptotic (r, r, p)

Theorem (1)

Fix $r \geq 5$ such that $r \not\equiv 1 \mod 8$. Let $\mathbb{Q}^+ := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, suppose that 2 is inert in $\mathbb{Q}^+$ and $2 \nmid h^+_{\mathbb{Q}^+}$. Then, there is a constant B_r (depending only on r) such that for each rational prime $p > B_r$, the equation $x^r + y^r = z^p$ has no integer solutions with $2|z$.

Example

This implies that there are no integer solutions (x, y, z) with $2|z$ for p large enough for signatures:

$$(5,5,p), (7,7,p), (11,11,p), (13,13,p), (19,19,p), (23,23,p), (37,37,p), (43,43,p), \cdots$$

Asymptotic (r, r, p)

Theorem (2)

Fix $r \geq 5$ such that $r \not\equiv 1 \mod 8$. Let $K := \mathbb{Q}(\sqrt{d})$ with d square-free and $d \not\equiv 1 \mod 8$. Assume that r is inert in K. Let $K^+ := K(\zeta_r + \zeta_r^{-1})$, suppose that 2 is inert in $\mathbb{Q}^+$ and $2 \nmid h^+_{K^+}$. Moreover

1. *if $d \equiv 5 \mod 8$ we assume $r \not\equiv 1 \mod 8$;*
2. *if $d \equiv 2, 3 \mod 4$ we assume $r \not\equiv 1, d \mod 8$.*

In the first case, 2 is inert in K and in the second case, it is totally ramified. Either way, we denote the unique prime above 2 by $\mathfrak{P}$. Then, there is a constant $B_{K,r}$ (depending only on r and K) such that for each rational prime $p > B_{K,r}$, the equation $x^r + y^r = z^p$ has no integer solutions with $\mathfrak{P} | z$.

Proof of Theorem 1

Fix $r \geq 5$ a rational prime. Suppose we have an integer solution (x, y, z) with $2|z$ to the equation

$$x^r + y^r = z^p, \quad p \geq 2, \text{ rational prime.}$$

Proof of Theorem 1

Fix $r \geq 5$ a rational prime. Suppose we have an integer solution (x, y, z) with $2|z$ to the equation

$$x^r + y^r = z^p, \quad p \geq 2, \text{ rational prime.}$$

We will show we get a contradiction when:

- $r \not\equiv 1 \mod 8$;
- 2 is inert in $\mathbb{Q}^+$;
- $2 \nmid h^+_{\mathbb{Q}^+}$.

where $\mathbb{Q}^+ := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$. We will denote by $\mathfrak{P}_r$ the unique prime above r.

Relating diophantine equations

We write

$$\phi_r(x,y) := \frac{x^r + y^r}{x+y} = \sum_{i=1}^{r-1} (-1)^i x^{r-1-i} y^i. \tag{2}$$

Over the field $L := \mathbb{Q}(\zeta_r)$ one gets the factorization

$$\phi_r(x,y) = \prod_{i=1}^{r-1} (x + \zeta_r^i y). \tag{3}$$

Relating diophantine equations

Over the totally real field $\mathbb{Q}^+$, ϕ_r factors into degree two factors of the form

$$f_k(x,y) := x^2 + (\zeta_r^k + \zeta_r^{-k})xy + y^2, \quad 1 \leq k \leq \frac{r-1}{2}. \tag{4}$$

Moreover, we denote $f_0(x,y) = (x+y)^2$.

Relating diophantine equations

Over the totally real field $\mathbb{Q}^+$, ϕ_r factors into degree two factors of the form

$$f_k(x,y) := x^2 + (\zeta_r^k + \zeta_r^{-k})xy + y^2, \quad 1 \leq k \leq \frac{r-1}{2}. \tag{4}$$

Moreover, we denote $f_0(x,y) = (x+y)^2$. From the fact that

$$(x+y)\prod_{k=1}^{(r-1)/2} f_k(x,y) = z^p$$

we deduce there is precisely one k_1 such that $2|f_{k_1}$. Since $\frac{r-1}{2} \geq 2$ we can fix two more distinct subscripts $0 \leq k_2, k_3 \leq \frac{r-1}{2}$.

Step 1: Constructing the Frey Elliptic Curve

We find (α, β, γ) such that

$$\alpha f_{k_1} + \beta f_{k_2} + \gamma f_{k_3} = 0.$$

Write $A = \alpha f_{k_1}, B = \beta f_{k_2}, C = \gamma f_{k_3}$ and define

$$E : Y^2 = X(X - A)(X + B). \tag{5}$$

Note that E is defined over the totally real number field $\mathbb{Q}^+$. The Artin conductor of E is

$$\mathcal{N}_p = 2^{e_2}\mathfrak{P}_r^{e_r}.$$

Step 1: Constructing the Frey Elliptic Curve

We find (α, β, γ) such that

$$\alpha f_{k_1} + \beta f_{k_2} + \gamma f_{k_3} = 0.$$

Write $A = \alpha f_{k_1}, B = \beta f_{k_2}, C = \gamma f_{k_3}$ and define

$$E : Y^2 = X(X - A)(X + B). \tag{5}$$

Note that E is defined over the totally real number field $\mathbb{Q}^+$. The Artin conductor of E is

$$\mathcal{N}_p = 2^{e_2}\mathfrak{P}_r^{e_r}.$$

Note: The choice of A, B, C assures that $2|A$ and A, B, C are pairwise coprime outside $\mathfrak{P}_r$.

Steps 2,3,4: Modularity, Level Lowering, Irreducibility

After possibly enlarging p, $E/\mathbb{Q}^+$ is **modular** and $\overline{\rho}_{E,p}$ **irreducible** allowing us to apply **level lowering** and get a Hilbert newform over K with rational eigenvalues, parallel weight 2 with level equal to $\mathcal{N}_p$ such that

$$\overline{\rho}_{E,p} \simeq \overline{\rho}_{\mathfrak{f},p}.$$

Step 5 - Eliminate

1.Eichler Schimura

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 rational eigenvalues. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

Step 5 - Eliminate

1.Eichler Schimura

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 rational eigenvalues. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

A theorem due to Freitas and Siksek (2014) gives a partial result to this conjecture. In our case, it gives an elliptic curve E'/K such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},p} \sim \overline{\rho}_{E',p}$ and E' has conductor $\mathcal{N}_p$.

Step 5 - Eliminate

What can we say about E'?

Step 5 - Eliminate

What can we say about E'?

- $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$

Step 5 - Eliminate

What can we say about E'?

- $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$
- E' has good reduction outside $S := \{2, \mathfrak{P}_r\}$

Step 5 - Eliminate

What can we say about E'?

- $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$
- E' has good reduction outside $S := \{2, \mathfrak{P}_r\}$
- E' has $\#E'(\mathbb{Q}^+)[2] = 4$ (after possibly enlarging p and replacing E' with an 2-isogenous curve)

Step 5 - Eliminate

What can we say about E'?

- $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$
- E' has good reduction outside $S := \{2, \mathfrak{P}_r\}$
- E' has $\#E'(\mathbb{Q}^+)[2] = 4$ (after possibly enlarging p and replacing E' with an 2-isogenous curve)
- E' has potentially multiplicative reduction at 2 (after possibly enlarging p).

Step 5 - Eliminate

2. Image of inertia comparison: E' has potentially multiplicative reduction at $2 \Leftrightarrow v_2(j_{E'}) < 0$

Lemma

Let E be an elliptic curve over K with j-invariant j_E. Let $p \geq 5$ and let $\mathfrak{q} \nmid p$ be a prime of K. Then $p | \#\overline{\rho}_{E,p}(I_\mathfrak{q})$ if and only if E has potentially multiplicative reduction at $\mathfrak{q}$ (i.e. $v_\mathfrak{q}(j_E) < 0$) and $p \nmid v_\mathfrak{q}(j_E)$.

Step 5 - Eliminate

2. Image of inertia comparison: E' has potentially multiplicative reduction at $2 \Leftrightarrow v_2(j_{E'}) < 0$

Lemma

Let E be an elliptic curve over K with j-invariant j_E. Let $p \geq 5$ and let $\mathfrak{q} \nmid p$ be a prime of K. Then $p | \#\overline{\rho}_{E,p}(I_\mathfrak{q})$ if and only if E has potentially multiplicative reduction at $\mathfrak{q}$ (i.e. $v_\mathfrak{q}(j_E) < 0$) and $p \nmid v_\mathfrak{q}(j_E)$.

The Frey Elliptic curve

$$E : Y^2 = X(X - A)(X + B)$$

has

$$j_E = -2^8 \frac{(AB + BC + AC)^3}{(ABC)^2}$$

From Elliptic Curves to S-units

- We have an elliptic curve $E'/\mathbb{Q}^+$ with full 2 torsion over $\mathbb{Q}^+$, hence with a model:

$$E' : Y^2 = (X - e_1)(X - e_2)(X - e_3).$$

Consider $\lambda := (e_3 - e_1)/(e_2 - e_1)$ then

$$j_{E'} = 2^8(\lambda^2 - \lambda + 1)^3\lambda^{-2}(\lambda - 1)^{-2}$$

From Elliptic Curves to S-units

- We have an elliptic curve $E'/\mathbb{Q}^+$ with full 2 torsion over $\mathbb{Q}^+$, hence with a model:

$$E' : Y^2 = (X - e_1)(X - e_2)(X - e_3).$$

Consider $\lambda := (e_3 - e_1)/(e_2 - e_1)$ then

$$j_{E'} = 2^8(\lambda^2 - \lambda + 1)^3\lambda^{-2}(\lambda - 1)^{-2}$$

- Good reduction outside $S \Rightarrow j_{E'} \in \mathcal{O}_S$
- Potentially multiplicative reduction at $2 \Leftrightarrow v_2(j_{E'}) < 0$

Putting this information together we get an S-unit equation

$$\lambda + \mu = 1$$

where $S := \{2, \mathfrak{P}_r\}$ and with $2^5|\lambda$.

Step 5 - Eliminate

3.Finiteness of S-units

Theorem (De Weger's, Siegel, Smart)

Let K be a number field and $S \subset \mathcal{O}_K$ a finite set of prime ideals, and let $a, b \in K^*$. Then, the equation

$$ax + by = 1$$

has only finitely many solutions in $\mathcal{O}_S^*$.

S-unit solver for $a = b = 1$ has been implemented in the free open-source mathematics software, Sage by A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West.

Step 5 - Eliminate

We are going to show that when our assumptions that $r \not\equiv 1 \mod 8$ and $2 \nmid h^+_{\mathbb{Q}^+}$ hold, the S-unit equation

$$\lambda + \mu = 1$$

cannot have $2^5 | \lambda$.

Step 5 - Eliminate

If by contradiction $2^5|\lambda$, then

$$\mu \equiv 1 \mod 32.$$

Step 5 - Eliminate

If by contradiction $2^5|\lambda$, then

$$\mu \equiv 1 \mod 32.$$

Ingredient 1: Class field theory (+assumptions) gives $\mu = \tau_0^2$ with $\tau_0 \in \mathcal{O}_S^*$.
Denote $(\lambda, \mu) = (\lambda_0, \mu_0)$. This gives the possibility to construct a sequence of solutions to our S-unit equation

$$(\lambda_{n+1}, \mu_{n+1}) = \left(\frac{-(1-\tau_n)^2}{4\tau_n}, \frac{(1+\tau_n)^2}{4\tau_n} \right)$$

with $v_2(\lambda_{n+1}) > v_2(\lambda_n)$.

Step 5 - Eliminate

If by contradiction $2^5|\lambda$, then

$$\mu \equiv 1 \mod 32.$$

Ingredient 1: Class field theory (+assumptions) gives $\mu = \tau_0^2$ with $\tau_0 \in \mathcal{O}_S^*$.
Denote $(\lambda, \mu) = (\lambda_0, \mu_0)$. This gives the possibility to construct a sequence of solutions to our S-unit equation

$$(\lambda_{n+1}, \mu_{n+1}) = \left(\frac{-(1-\tau_n)^2}{4\tau_n}, \frac{(1+\tau_n)^2}{4\tau_n} \right)$$

with $v_2(\lambda_{n+1}) > v_2(\lambda_n)$.
Ingredient 2: Finiteness of S-units gives the desired contradiction.

Merci!