The Fermat-type equations $x^5 + y^5 = 2z^p$ or $3z^p$ solved through $\mathbb{Q}$-curves

Nuno Freitas

Universitat de Barcelona

January 2012

The equation $x^5 + y^5 = dz^p$

Theorem (Billerey and Billerey, Dieulefait)

Let $d = 2^\alpha 3^\beta 5^\gamma$ where $\alpha \geq 2$, $\beta, \gamma, \geq 0$, or $d = 7, 13$. Then, for $p > 19$ the equation $x^5 + y^5 = dz^p$ has no non-trivial primitive solution.

Let γ be an integer divisible only by primes $l \not\equiv 1 \pmod 5$.

Theorem (Dieulefait, F)

For any $p > 13$ such that $p \equiv 1 \bmod 4$ or $p \equiv \pm 1 \bmod 5$, the equation $x^5 + y^5 = 2\gamma z^p$ has no non-trivial primitive solutions.

Theorem (Dieulefait, F)

For any $p > 73$ such that $p \equiv 1 \bmod 4$ or $p \equiv \pm 1 \bmod 5$, the equation $x^5 + y^5 = 3\gamma z^p$ has no non-trivial primitive solutions.

The equation $x^5 + y^5 = dz^p$

Theorem (Billerey and Billerey, Dieulefait)

Let $d = 2^\alpha 3^\beta 5^\gamma$ where $\alpha \geq 2$, $\beta, \gamma, \geq 0$, or $d = 7, 13$. Then, for $p > 19$ the equation $x^5 + y^5 = dz^p$ has no non-trivial primitive solution.

Let γ be an integer divisible only by primes $l \not\equiv 1 \pmod 5$.

Theorem (Dieulefait, F)

For any $p > 13$ such that $p \equiv 1 \bmod 4$ or $p \equiv \pm 1 \bmod 5$, the equation $x^5 + y^5 = 2\gamma z^p$ has no non-trivial primitive solutions.

Theorem (Dieulefait, F)

For any $p > 73$ such that $p \equiv 1 \bmod 4$ or $p \equiv \pm 1 \bmod 5$, the equation $x^5 + y^5 = 3\gamma z^p$ has no non-trivial primitive solutions.

Relating two equations

Key factorization:
$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4)$

Let $\phi(x, y) = (x^4 - x^3y + x^2y^2 - xy^3 + y^4)$

Proposition

If $(a, b) = 1$ then the integers $a + b$ and $\phi(a, b)$ are coprime outside 5. Moreover, $5 \mid a + b \iff \upsilon_5(\phi(a, b)) = 1$

Proposition

Let $l \not\equiv 1 \pmod 5$ be a prime number dividing $a^5 + b^5$. If $(a, b) = 1$ then l divides $a + b$.

Relating two equations

Key factorization:
$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4)$

Let $\phi(x, y) = (x^4 - x^3y + x^2y^2 - xy^3 + y^4)$

Proposition

If $(a, b) = 1$ then the integers $a + b$ and $\phi(a, b)$ are coprime outside 5. Moreover, $5 \mid a + b \iff \upsilon_5(\phi(a, b)) = 1$

Proposition

Let $l \not\equiv 1 \pmod 5$ be a prime number dividing $a^5 + b^5$. If $(a, b) = 1$ then l divides $a + b$.

Relating two equations

Let (a, b, c) be a primitive solution to $x^5 + y^5 = d\gamma z^p$.

- $a^5 + b^5 = (a + b)\phi(a, b) = d\gamma c^p$ $(d = 2, 3)$
- Since $d\gamma$ is divisible only by primes $l \not\equiv 1 \pmod 5$ we have $d\gamma \mid a + b$
- If $5 \nmid a + b$ then $\phi(a, b) = c_0^p$
- If $5 \mid a + b$ then $\phi(a, b) = 5c_0^p$
- $c_0 \mid c$ is only divisible by primes $l \equiv 1 \pmod 5$.

Hence we need to prove that $\phi(x, y) = rz^p$ where $r = 1, 5$ has no non-trivial primitive solutions if $d\gamma \mid a + b$. Actually, we can suppose that $\gamma = 1$.

The Frey $\mathbb{Q}$-curve

Observe that over $\mathbb{Q}(\sqrt{5})$

- $\phi(x,y) = \phi_1(x,y)\phi_2(x,y)$, where
- $\phi_1(x,y) = x^2 + \omega xy + y^2$ and $\phi_2(x,y) = x^2 + \bar{\omega}xy + y^2$, with
- $\omega = \frac{-1+\sqrt{5}}{2}$, $\bar{\omega} = \frac{-1-\sqrt{5}}{2}$
- Moreover, if $(a,b) = 1$ then $\phi_1(a,b), \phi_2(a,b)$ are coprime outside the prime above 5.

Definition

Given a triple (a,b,c) define the Frey-curve over $\mathbb{Q}(\sqrt{5})$

$$E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 - \bar{\omega}\phi_1(a,b)x$$

with discriminant $\Delta(E) = 2^6\bar{\omega}\phi\phi_1$.

There are representations $\rho_{E,l} : G_{\mathbb{Q}(\sqrt{5})} \to \mathrm{GL}_2(\mathbb{Q}_l)$ with residual representations $\bar{\rho}_{E,l} : G_{\mathbb{Q}(\sqrt{5})} \to \mathrm{GL}_2(\mathbb{F}_l)$

Serre Conjecture (Khare, Wintenberger)

Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ be odd and irreducible. Then $\bar{\rho}$ is modular of type $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$.

We need to extend $\bar{\rho}_{E,p}$!!!

Definition

Let C be an elliptic curve over $\bar{\mathbb{Q}}$. We say that C is a $\mathbb{Q}$**-curve** if it is isogenous to all its Galois conjugates ${}^{\sigma}C$ for $\sigma \in G_{\mathbb{Q}}$

Proposition

Then $E_{(a,b)}$ is a $\mathbb{Q}$-curve

Proof: The curve $E_{(a,b)}$ has the non-trivial Galois

$$ {}^{\sigma}E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 - \omega\phi_2(a,b)x, $$

Serre Conjecture (Khare, Wintenberger)

Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ be odd and irreducible. Then $\bar{\rho}$ is modular of type $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$.

We need to extend $\bar{\rho}_{E,p}$!!!

Definition

Let C be an elliptic curve over $\bar{\mathbb{Q}}$. We say that C is a **$\mathbb{Q}$-curve** if it is isogenous to all its Galois conjugates ${}^{\sigma}C$ for $\sigma \in G_{\mathbb{Q}}$

Proposition

Then $E_{(a,b)}$ is a $\mathbb{Q}$-curve

Proof: The curve $E_{(a,b)}$ has the non-trivial Galois

$${}^{\sigma}E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 - \omega\phi_2(a,b)x,$$

The Frey $\mathbb{Q}$-curve

Serre Conjecture (Khare, Wintenberger)

Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ be odd and irreducible. Then $\bar{\rho}$ is modular of type $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$.

We need to extend $\bar{\rho}_{E,p}$!!!

Definition

Let C be an elliptic curve over $\bar{\mathbb{Q}}$. We say that C is a **$\mathbb{Q}$-curve** if it is isogenous to all its Galois conjugates ${}^{\sigma}C$ for $\sigma \in G_{\mathbb{Q}}$

Proposition

Then $E_{(a,b)}$ is a $\mathbb{Q}$-curve

Proof: The curve $E_{(a,b)}$ has the non-trivial Galois

$${}^{\sigma}E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 - \omega\phi_2(a,b)x,$$

The Frey $\mathbb{Q}$-curve

and there exists a 2-isogeny $\mu : {}^{\sigma}E \to E$ given by

$$(x, y) \mapsto \left(-\frac{y^2}{2x^2}, \frac{\sqrt{-2}}{4}\frac{y}{x^2}(\omega\phi_2 + x^2)\right).$$

Theorem

Let $K = \mathbb{Q}(\theta)$ where $\theta = \sqrt{\frac{1}{2}(5+\sqrt{5})}$. Put $\gamma = 2\theta^2 - \theta - 5$ and consider the twist of $E_{(a,b)}$ by γ defined over K by

$$E_\gamma : y^2 = x^3 + 2\gamma(a+b)x^2 - \gamma^2\bar{\omega}\phi_1(a,b)x.$$

The Weil restriction $B = \mathrm{Res}_{K/\mathbb{Q}}(E_\gamma/K) \sim S_1 \times S_2$ where S_i are two non-isogenous abelian surfaces of GL_2-type defined over $\mathbb{Q}$. Each S_i has its $\mathbb{Q}$-endomorphism algebra iso to $\mathbb{Q}(i)$.

and there exists a 2-isogeny $\mu : {}^{\sigma}E \to E$ given by

$$(x, y) \mapsto \left(-\frac{y^2}{2x^2}, \frac{\sqrt{-2}}{4}\frac{y}{x^2}(\omega\phi_2 + x^2)\right).$$

Theorem

Let $K = \mathbb{Q}(\theta)$ where $\theta = \sqrt{\frac{1}{2}(5+\sqrt{5})}$. Put $\gamma = 2\theta^2 - \theta - 5$ and consider the twist of $E_{(a,b)}$ by γ defined over K by

$$E_\gamma : y^2 = x^3 + 2\gamma(a+b)x^2 - \gamma^2\bar{\omega}\phi_1(a,b)x.$$

The Weil restriction $B = \mathrm{Res}_{K/\mathbb{Q}}(E_\gamma/K) \sim S_1 \times S_2$ where S_i are two non-isogenous abelian surfaces of GL_2-type defined over $\mathbb{Q}$. Each S_i has its $\mathbb{Q}$-endomorphism algebra iso to $\mathbb{Q}(i)$.

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

- For $\lambda \in \mathbb{Q}(i)$ then $G_{\mathbb{Q}}$ acts on $T_l S_i$ and induces $\rho_l = \rho_{S_i,\lambda} \oplus \rho^{\sigma}_{S_i,\lambda}$.
- To compute $N(\bar{\rho}_{S_i,\lambda})$ we need the level of $\rho_{S_i,\lambda}$ first.

From Tate's Algorithm we compute N_{E_γ} and with

Milne's Formula: $N_B = \mathrm{Nm}_{K/\mathbb{Q}}(N_{E_\gamma})\mathrm{Disc}(K/\mathbb{Q})^2$

we obtain the conductor of B

Proposition

- $N_B = 2^t 5^{6+s} \mathrm{rad}(c)^4$
- $s = 0$ or 2 if $5 \mid a+b$ or $5 \nmid a+b$, respectively
- if $2 \mid a+b \Rightarrow t = 24, 8, 16$ if $2 \parallel a+b, 4 \parallel a+b, 8 \mid a+b$
- if $2 \nmid a+b$ then $t = 24$ or 20 if $4 \nmid a$ or $4 \mid a$, respectively.

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

- For $\lambda \in \mathbb{Q}(i)$ then $G_{\mathbb{Q}}$ acts on $T_l S_i$ and induces $\rho_l = \rho_{S_i,\lambda} \oplus \rho_{S_i,\lambda}^{\sigma}$.
- To compute $N(\bar{\rho}_{S_i,\lambda})$ we need the level of $\rho_{S_i,\lambda}$ first.

From Tate's Algorithm we compute N_{E_γ} and with

Milne's Formula: $N_B = \mathrm{Nm}_{K/\mathbb{Q}}(N_{E_\gamma})\mathrm{Disc}(K/\mathbb{Q})^2$

we obtain the conductor of B

Proposition

- $N_B = 2^t 5^{6+s} \mathrm{rad}(c)^4$
- $s = 0$ or 2 if $5 \mid a+b$ or $5 \nmid a+b$, respectively
- if $2 \mid a+b \Rightarrow t = 24, 8, 16$ if $2 \parallel a+b, 4 \parallel a+b, 8 \mid a+b$
- if $2 \nmid a+b$ then $t = 24$ or 20 if $4 \nmid a$ or $4 \mid a$, respectively.

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

Let ϵ be the character of K then ϵ^2 is the character of $\mathbb{Q}(\sqrt{5})$.

- E_γ has no CM $\Rightarrow \rho_{E_\gamma,l}$ absolutely irreducible
- Extensions of abs. irr. rep. are unique up to twists
- There are four 2-dimensional rep. of $G_\mathbb{Q}$ extending $\rho_{E_\gamma,l}$

$$\rho_{S_1,\lambda} \otimes \epsilon = \rho^\sigma_{S_1,\lambda}, \quad \rho_{S_1,\lambda} \otimes \epsilon^2 = \rho_{S_2,\lambda}, \quad \rho_{S_1,\lambda} \otimes \epsilon^3 = \rho^\sigma_{S_2,\lambda}$$

- $B \simeq S_1 \times S_2 \Rightarrow N_B = N_{S_1} N_{S_2}$
- $N_{S_i} = \text{cond}(\rho_{S_i,\lambda})\text{cond}(\rho^\sigma_{S_i,\lambda}) = \text{cond}(\rho_{S_i,\lambda})^2$
- The difference between $\text{cond}(\rho_{S_1,\lambda})$ and $\text{cond}(\rho_{S_2,\lambda})$ is at 5
- $\text{cond}_5(\rho_{S_1,\lambda} \otimes \epsilon^2) \leq \text{lcm}(\text{cond}_5(\rho_{S_1,\lambda}), \text{cond}(\epsilon^2)^2 = 5^2)$

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

Let ϵ be the character of K then ϵ^2 is the character of $\mathbb{Q}(\sqrt{5})$.

- E_γ has no CM $\Rightarrow \rho_{E_\gamma, l}$ absolutely irreducible
- Extensions of abs. irr. rep. are unique up to twists
- There are four 2-dimensional rep. of $G_\mathbb{Q}$ extending $\rho_{E_\gamma, l}$

$$\rho_{S_1,\lambda} \otimes \epsilon = \rho^\sigma_{S_1,\lambda}, \quad \rho_{S_1,\lambda} \otimes \epsilon^2 = \rho_{S_2,\lambda}, \quad \rho_{S_1,\lambda} \otimes \epsilon^3 = \rho^\sigma_{S_2,\lambda}$$

- $B \simeq S_1 \times S_2 \Rightarrow N_B = N_{S_1} N_{S_2}$
- $N_{S_i} = \text{cond}(\rho_{S_i,\lambda})\text{cond}(\rho^\sigma_{S_i,\lambda}) = \text{cond}(\rho_{S_i,\lambda})^2$
- The difference between $\text{cond}(\rho_{S_1,\lambda})$ and $\text{cond}(\rho_{S_2,\lambda})$ is at 5
- $\text{cond}_5(\rho_{S_1,\lambda} \otimes \epsilon^2) \leq \text{lcm}(\text{cond}_5(\rho_{S_1,\lambda}), \text{cond}(\epsilon^2)^2 = 5^2)$

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

Let ϵ be the character of K then ϵ^2 is the character of $\mathbb{Q}(\sqrt{5})$.

- E_γ has no CM $\Rightarrow \rho_{E_\gamma, l}$ absolutely irreducible
- Extensions of abs. irr. rep. are unique up to twists
- There are four 2-dimensional rep. of $G_\mathbb{Q}$ extending $\rho_{E_\gamma, l}$

$$\rho_{S_1,\lambda} \otimes \epsilon = \rho^\sigma_{S_1,\lambda}, \quad \rho_{S_1,\lambda} \otimes \epsilon^2 = \rho_{S_2,\lambda}, \quad \rho_{S_1,\lambda} \otimes \epsilon^3 = \rho^\sigma_{S_2,\lambda}$$

- $B \simeq S_1 \times S_2 \Rightarrow N_B = N_{S_1} N_{S_2}$
- $N_{S_i} = \mathrm{cond}(\rho_{S_i,\lambda})\mathrm{cond}(\rho^\sigma_{S_i,\lambda}) = \mathrm{cond}(\rho_{S_i,\lambda})^2$
- The difference between $\mathrm{cond}(\rho_{S_1,\lambda})$ and $\mathrm{cond}(\rho_{S_2,\lambda})$ is at 5
- $\mathrm{cond}_5(\rho_{S_1,\lambda} \otimes \epsilon^2) \leq \mathrm{lcm}(\mathrm{cond}_5(\rho_{S_1,\lambda}), \mathrm{cond}(\epsilon^2)^2 = 5^2)$

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

Equation	$\nu_2(a+b)$	$\rho_{S_1,\lambda}$	$\rho^{\sigma}_{S_1,\lambda}$	$\rho_{S_2,\lambda}$	$\rho^{\sigma}_{S_2,\lambda}$
$r=1$	0	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$
$r=1$	0	$2^5 5^2 c_0$	$2^5 5^2 c_0$	$2^5 5^2 c_0$	$2^5 5^2 c_0$
$r=1$	1	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$
$r=1$	2	$2^2 5^2 c_0$	$2^2 5^2 c_0$	$2^2 5^2 c_0$	$2^2 5^2 c_0$
$r=1$	≥ 3	$2^4 5^2 c_0$	$2^4 5^2 c_0$	$2^4 5^2 c_0$	$2^4 5^2 c_0$
$r=5$	0	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5 c_0$	$2^6 5 c_0$
$r=5$	0	$2^5 5^2 c_0$	$2^5 5^2 c_0$	$2^5 5 c_0$	$2^5 5 c_0$
$r=5$	1	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5 c_0$	$2^6 5 c_0$
$r=5$	2	$2^2 5^2 c_0$	$2^2 5^2 c_0$	$2^2 5 c_0$	$2^2 5 c_0$
$r=5$	≥ 3	$2^4 5^2 c_0$	$2^4 5^2 c_0$	$2^4 5 c_0$	$2^4 5 c_0$

Table: Values of conductors, where $c_0 = \mathrm{rad}(c)$

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

Let λ in $\mathbb{Q}(i)$ be above p and define $\rho := \rho_{S_1,\lambda}$ and $\bar{\rho} := \bar{\rho}_{S_1,\lambda}$.

- (Hellegouarch) $\bar{\rho}|K = \bar{\rho}_{E_\gamma,p}$ is unramified at $c_0 = \mathrm{rad}(c)$.
- $\mathrm{Disc}(K/\mathbb{Q}) = 2^4 5^3$ then $\bar{\rho}$ can not ramify outside 2 and 5
- (Carayol) Wild ramification implies conductor does not decrease when reducing mod p
- Then $N(\bar{\rho})$ is equal to the first column in the previous table without c_0
- (Pyle) ρ has character ϵ^{-1} then $\epsilon(\bar{\rho}) = \epsilon^{-1}$ since $p > 2$
- If $p \nmid c$ S_1 has good reduction; if $p \mid c$, since $p \mid \upsilon_{\mathfrak{P}(\Delta)}$ then $\bar{\rho}$ is finite. In both cases $k(\bar{\rho}) = 2$
- (Ellenberg) $\bar{\rho}$ is absolutely irreducible for $p > 13$ if (a, b, c) is such that $|c| > 1$.

From Serre conjecture there is a newform f of type $(M, 2, \bar{\epsilon})$ with $M = 1600, 800, 400$ or 100 and a prime $\mathfrak{P}$ in $\mathbb{Q}_f$ above p such that $\bar{\rho} \equiv \bar{\rho}_{f,\mathfrak{P}} (\mathrm{mod}\ \mathfrak{P})$

Computing $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$

Let λ in $\mathbb{Q}(i)$ be above p and define $\rho := \rho_{S_1,\lambda}$ and $\bar{\rho} := \bar{\rho}_{S_1,\lambda}$.

- (Hellegouarch) $\bar{\rho}|K = \bar{\rho}_{E_\gamma,p}$ is unramified at $c_0 = \mathrm{rad}(c)$.
- $\mathrm{Disc}(K/\mathbb{Q}) = 2^4 5^3$ then $\bar{\rho}$ can not ramify outside 2 and 5
- (Carayol) Wild ramification implies conductor does not decrease when reducing mod p
- Then $N(\bar{\rho})$ is equal to the first column in the previous table without c_0
- (Pyle) ρ has character ϵ^{-1} then $\epsilon(\bar{\rho}) = \epsilon^{-1}$ since $p > 2$
- If $p \nmid c$ S_1 has good reduction; if $p \mid c$, since $p \mid \upsilon_{\mathfrak{P}(\Delta)}$ then $\bar{\rho}$ is finite. In both cases $k(\bar{\rho}) = 2$
- (Ellenberg) $\bar{\rho}$ is absolutely irreducible for $p > 13$ if (a, b, c) is such that $|c| > 1$.

From Serre conjecture there is a newform f of type $(M, 2, \bar{\epsilon})$ with $M = 1600, 800, 400$ or 100 and a prime $\mathfrak{P}$ in $\mathbb{Q}_f$ above p such that $\bar{\rho} \equiv \bar{\rho}_{f,\mathfrak{P}} (\mathrm{mod}\ \mathfrak{P})$

Computing $(N(\bar\rho), k(\bar\rho), \epsilon(\bar\rho))$

Let λ in $\mathbb{Q}(i)$ be above p and define $\rho := \rho_{S_1,\lambda}$ and $\bar\rho := \bar\rho_{S_1,\lambda}$.

- (Hellegouarch) $\bar\rho|K = \bar\rho_{E_\gamma,p}$ is unramified at $c_0 = \mathrm{rad}(c)$.
- $\mathrm{Disc}(K/\mathbb{Q}) = 2^4 5^3$ then $\bar\rho$ can not ramify outside 2 and 5
- (Carayol) Wild ramification implies conductor does not decrease when reducing mod p
- Then $N(\bar\rho)$ is equal to the first column in the previous table without c_0
- (Pyle) ρ has character ϵ^{-1} then $\epsilon(\bar\rho) = \epsilon^{-1}$ since $p > 2$
- If $p \nmid c$ S_1 has good reduction; if $p \mid c$, since $p \mid \upsilon_{\mathfrak{P}(\Delta)}$ then $\bar\rho$ is finite. In both cases $k(\bar\rho) = 2$
- (Ellenberg) $\bar\rho$ is absolutely irreducible for $p > 13$ if (a, b, c) is such that $|c| > 1$.

From Serre conjecture there is a newform f of type $(M, 2, \bar\epsilon)$ with $M = 1600, 800, 400$ or 100 and a prime $\mathfrak{P}$ in $\mathbb{Q}_f$ above p such that $\bar\rho \equiv \bar\rho_{f,\mathfrak{P}} (\mathrm{mod}\ \mathfrak{P})$

Computing $(N(\bar\rho), k(\bar\rho), \epsilon(\bar\rho))$

Let λ in $\mathbb{Q}(i)$ be above p and define $\rho := \rho_{S_1,\lambda}$ and $\bar\rho := \bar\rho_{S_1,\lambda}$.

- (Hellegouarch) $\bar\rho|K = \bar\rho_{E_\gamma,p}$ is unramified at $c_0 = \mathrm{rad}(c)$.
- $\mathrm{Disc}(K/\mathbb{Q}) = 2^4 5^3$ then $\bar\rho$ can not ramify outside 2 and 5
- (Carayol) Wild ramification implies conductor does not decrease when reducing mod p
- Then $N(\bar\rho)$ is equal to the first column in the previous table without c_0
- (Pyle) ρ has character ϵ^{-1} then $\epsilon(\bar\rho) = \epsilon^{-1}$ since $p > 2$
- If $p \nmid c$ S_1 has good reduction; if $p \mid c$, since $p \mid \upsilon_{\mathfrak{P}(\Delta)}$ then $\bar\rho$ is finite. In both cases $k(\bar\rho) = 2$
- (Ellenberg) $\bar\rho$ is absolutely irreducible for $p > 13$ if (a, b, c) is such that $|c| > 1$.

From Serre conjecture there is a newform f of type $(M, 2, \bar\epsilon)$ with $M = 1600, 800, 400$ or 100 and a prime $\mathfrak{P}$ in $\mathbb{Q}_f$ above p such that $\bar\rho \equiv \bar\rho_{f,\mathfrak{P}} (\mathrm{mod}\ \mathfrak{P})$

Eliminating Newforms

For each possible newform we will contradict the congruence $\bar{\rho} \equiv \bar{\rho}_{f,p}$.

- Compute with SAGE the newforms in $\mathcal{S}_2(M, \epsilon^{-1})$
- The newforms corresponding to the trivial solutions $(\pm 1, 0)$, $(0, \pm 1)$, $(1, 1)$, $(-1, -1)$ and $(1, -1)$, $(-1, 1)$ exist.
- $E_{(\pm 1,0)}$, $E_{(0,\pm 1)}$ is not a problem for $d = 2$
- $E_{(-1,1)}$, $E_{(1,-1)}$, $E_{(1,1)}$ and $E_{(-1,-1)}$ have Complex Multiplication

Observe that $\mathbb{Q}(i) = \mathbb{Q}(\epsilon) \subseteq \mathbb{Q}_f$ and define the sets:

S1: Newforms with CM (Complex Multiplication),

S2: Newforms without CM and field of coefficients strictly containing $\mathbb{Q}(i)$,

S3: Newforms without CM and field of coefficients $\mathbb{Q}(i)$

Eliminating Newforms

For each possible newform we will contradict the congruence $\bar{\rho} \equiv \bar{\rho}_{f,p}$.

- Compute with SAGE the newforms in $\mathcal{S}_2(M, \epsilon^{-1})$
- The newforms corresponding to the trivial solutions $(\pm 1, 0)$, $(0, \pm 1)$, $(1, 1)$, $(-1, -1)$ and $(1, -1)$, $(-1, 1)$ exist.
- $E_{(\pm 1,0)}$, $E_{(0,\pm 1)}$ is not a problem for $d = 2$
- $E_{(-1,1)}$, $E_{(1,-1)}$, $E_{(1,1)}$ and $E_{(-1,-1)}$ have Complex Multiplication

Observe that $\mathbb{Q}(i) = \mathbb{Q}(\epsilon) \subseteq \mathbb{Q}_f$ and define the sets:

S1: Newforms with CM (Complex Multiplication),

S2: Newforms without CM and field of coefficients strictly containing $\mathbb{Q}(i)$,

S3: Newforms without CM and field of coefficients $\mathbb{Q}(i)$

d=2: Newforms in S1

Recall that $2 \mid a + b$ then 800 is not a possible level.

- There are four with CM by $\mathbb{Q}(i)$ and four by $\mathbb{Q}(\sqrt{-5})$.
- If (a, b, c) is non-trivial there exists a prime ≥ 5 of multiplicative reduction.
- (Ellenberg) If $p > 13$ the image of $\bar{\rho}$ will not lie in the normalizer of a split Cartan subgroup.
- For an f with CM if p is a square on the field of CM then the image of $\bar{\rho}_{f,p}$ will be in a normalizer of a split Cartan subgroup.
- Then $p \equiv 1 \bmod 4$ and $p \equiv \pm 1 \bmod 5 \Rightarrow \bar{\rho} \not\equiv \bar{\rho}_{f,p}$

d=2: Newforms in S2

- There are 12 newforms (modulo conjugation) in S2.
- For q of good reduction for S_1, $a_q = \bar{a}_q \epsilon^{-1}(q)$.
- 3 is of good reduction and $a_3 = t - ti$ with $t \in \mathbb{Z}$.
- Weil bound $|a_3| \leq 2\sqrt{3} \Rightarrow |t| \leq 2$
- If $f = q + \sum_{n=2} a_n(f)q^n$ then $a_3(\bar{\rho}) \equiv a_3(f) \pmod{\mathfrak{P}}$
- There is f in S2 of level 400 with $a_3(f)$ having minimal polynomial $x^2 + 10i$
- Then $a_3(f) \equiv t - it \pmod{\mathfrak{P}}$ implies $100 \equiv 4t^4 \pmod{\mathfrak{P}}$, substituting for $t = 0, \pm 1, \pm 2$ we reach a contradiction if $p > 5$.
- Do the same with $a_3(f)$ for all other f and conlude a contradiction for $p > 7$.

d=2: Newforms in S3

Let χ be the character of $\mathbb{Q}(\sqrt{2})$ and $E_{\gamma,2}$ the twist by 2 of E_γ.

- There are 10 "bad" newforms in S3 all with level 1600 $(2 \parallel a+b)$.
- Since $1600 = 2^6 5^2$ and $\mathrm{cond}(\chi)^2 = 8^2 = 2^6$ the conductor of $f \otimes \chi$ may decrease.
- With SAGE we compute the coefficients of $f \otimes \chi$ to find that $f \otimes \chi$ are of level 800 for all f in S3
- $(\rho_{S_1,\lambda} \otimes \chi)_{|K} = (\rho_{S_1,\lambda})_{|K} \otimes \chi_{|K} = \rho_{E_\gamma,p} \otimes \chi_{|K} = \rho_{E_{\gamma,2},p}$
- Then $\rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_{\gamma,2},p}$ and the same holds for $\rho^\sigma_{S_1,\lambda}$, $\rho^\sigma_{S_2,\lambda}$, $\rho_{S_2,\lambda}$
- Therefore $\rho_{B,p} \otimes \chi = (\mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho_{E_\gamma,p}) \otimes \chi = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(\rho_{E_\gamma,p} \otimes \chi_{|K}) = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho_{E_{\gamma,2},p}$ arises from $G_\mathbb{Q}$ acting on the p-adic Tate module of $\mathrm{Res}_{K/\mathbb{Q}}(E_{\gamma,2}/K)$.
- Then we can compute conductor of $\rho_{B,p} \otimes \chi$ via Milne's Formula

d=2: Newforms in S3

Let χ be the character of $\mathbb{Q}(\sqrt{2})$ and $E_{\gamma,2}$ the twist by 2 of E_γ.

- There are 10 “bad” newforms in S3 all with level 1600 ($2 \parallel a+b$).
- Since $1600 = 2^6 5^2$ and $\mathrm{cond}(\chi)^2 = 8^2 = 2^6$ the conductor of $f \otimes \chi$ may decrease.
- With SAGE we compute the coefficients of $f \otimes \chi$ to find that $f \otimes \chi$ are of level 800 for all f in S3
- $(\rho_{S_1,\lambda} \otimes \chi)_{|K} = (\rho_{S_1,\lambda})_{|K} \otimes \chi_{|K} = \rho_{E_\gamma,p} \otimes \chi_{|K} = \rho_{E_{\gamma,2},p}$
- Then $\rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_{\gamma,2},p}$ and the same holds for $\rho^\sigma_{S_1,\lambda}$, $\rho^\sigma_{S_2,\lambda}$, $\rho_{S_2,\lambda}$
- Therefore $\rho_{B,p} \otimes \chi = (\mathrm{Ind}^{G_\mathbb{Q}}_{G_K} \rho_{E_\gamma,p}) \otimes \chi = \mathrm{Ind}^{G_\mathbb{Q}}_{G_K}(\rho_{E_\gamma,p} \otimes \chi_{|K}) = \mathrm{Ind}^{G_\mathbb{Q}}_{G_K} \rho_{E_{\gamma,2},p}$ arises from $G_\mathbb{Q}$ acting on the p-adic Tate module of $\mathrm{Res}_{K/\mathbb{Q}}(E_{\gamma,2}/K)$.
- Then we can compute conductor of $\rho_{B,p} \otimes \chi$ via Milne's Formula

d=2: Newforms in S3

Let χ be the character of $\mathbb{Q}(\sqrt{2})$ and $E_{\gamma,2}$ the twist by 2 of E_γ.

- There are 10 "bad" newforms in S3 all with level 1600 ($2 \parallel a+b$).
- Since $1600 = 2^6 5^2$ and $\mathrm{cond}(\chi)^2 = 8^2 = 2^6$ the conductor of $f \otimes \chi$ may decrease.
- With SAGE we compute the coefficients of $f \otimes \chi$ to find that $f \otimes \chi$ are of level 800 for all f in S3
- $(\rho_{S_1,\lambda} \otimes \chi)_{|K} = (\rho_{S_1,\lambda})_{|K} \otimes \chi_{|K} = \rho_{E_\gamma,p} \otimes \chi_{|K} = \rho_{E_{\gamma,2},p}$
- Then $\rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_{\gamma,2},p}$ and the same holds for $\rho^\sigma_{S_1,\lambda}$, $\rho^\sigma_{S_2,\lambda}$, $\rho_{S_2,\lambda}$
- Therefore $\rho_{B,p} \otimes \chi = (\mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho_{E_\gamma,p}) \otimes \chi = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(\rho_{E_\gamma,p} \otimes \chi_{|K}) = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho_{E_{\gamma,2},p}$ arises from $G_\mathbb{Q}$ acting on the p-adic Tate module of $\mathrm{Res}_{K/\mathbb{Q}}(E_{\gamma,2}/K)$.
- Then we can compute conductor of $\rho_{B,p} \otimes \chi$ via Milne's Formula

d=2: Newforms in S3

$\rho_1 := \rho_{S_1,\lambda} \otimes \chi$ is a 2-dimensional factor of $\rho_{B,p} \otimes \chi$ and extends $\rho_{E_{\gamma,2},p}$. Let $\bar{\rho}_1$ denote its reduction. A similar analysis as for E_γ shows that if $2 \parallel a+b$ then by Serre's conjecture

$\bar{\rho}_1$ is modular of type $(M_1, 2, \bar{\epsilon})$ with $M = 100$ or 400

- $\bar{\rho}_1 \equiv \bar{\rho}_{g,p} \pmod{\mathfrak{P}}$
- $\bar{\rho}_1 = \overline{\rho_{S_1,\lambda} \otimes \chi} = \bar{\rho} \otimes \chi \equiv \bar{\rho}_{f,p} \otimes \chi \equiv \bar{\rho}_{f \otimes \chi,p} = \bar{\rho}_{f',p}$,
- We know that f' has level 800
- This kind of level lowering can not happen (by Carayol)!

Theorem

For any $p > 13$ such that $p \equiv 1 \bmod 4$ and $p \equiv \pm 1 \bmod 5$, the equation $x^5 + y^5 = 2\gamma z^p$ has no non-trivial primitive solutions.

d=2: Newforms in S3

$\rho_1 := \rho_{S_1,\lambda} \otimes \chi$ is a 2-dimensional factor of $\rho_{B,p} \otimes \chi$ and extends $\rho_{E_{\gamma,2},p}$. Let $\bar{\rho}_1$ denote its reduction. A similar analysis as for E_γ shows that if $2 \parallel a + b$ then by Serre's conjecture

$\bar{\rho}_1$ is modular of type $(M_1, 2, \bar{\epsilon})$ with $M = 100$ or 400

- $\bar{\rho}_1 \equiv \bar{\rho}_{g,p} \pmod{\mathfrak{P}}$
- $\bar{\rho}_1 = \overline{\rho_{S_1,\lambda} \otimes \chi} = \bar{\rho} \otimes \chi \equiv \bar{\rho}_{f,p} \otimes \chi \equiv \bar{\rho}_{f \otimes \chi,p} = \bar{\rho}_{f',p}$,
- We know that f' has level 800
- This kind of level lowering can not happen (by Carayol)!

Theorem

For any $p > 13$ such that $p \equiv 1 \bmod 4$ and $p \equiv \pm 1 \bmod 5$, the equation $x^5 + y^5 = 2\gamma z^p$ has no non-trivial primitive solutions.

d=3: a+b odd, level 800

Let $d = 3$. Recall that $3 \mid a + b$ and suppose $a + b$ odd, which means level 800 or 1600.

- In level 800 there are 4 newforms of type S2 and 10 of type S3 and none of type S1. Suppose $\bar{\rho} \equiv \bar{\rho}_{f,p}$.
- For type S2 we do as before. There exists f in S2 with $a_3(f)$ having minimal polynomial $t^2 \pm (2 - 2i)t + i$ then we need $p > 73$ to achieve a contradiction.
- If $f \in S3$, $\bar{\rho}|_{G_K} \equiv \bar{\rho}_{f,p}|_{G_K} \Rightarrow a_{\mathfrak{P}_3}(E_\gamma) \equiv a_{\mathfrak{P}_3}(f) \pmod{p}$
- $3 \mid a + b \Rightarrow a_{\mathfrak{P}_3}(E_\gamma) = -18$ (with SAGE)
- $a_3(f) = \pm(2i - 2)$ or $\pm(i - 1)$ for f in S3
- $a_{\mathfrak{P}_3}(f) = \alpha^4 + \beta^4$, where α, β are roots of the characteristic polynomial of $\rho_{f,p}(\mathrm{Frob}_3)$, i.e. $x^2 - a_3(f)x + \epsilon^{-1}(3)3$
- Then $a_{\mathfrak{P}_3}(f) = 14$ or 2, contradiction for $p > 3$

d=3: a+b odd, level 1600

Now level 1600:

- The forms of type S1 and S2 can be eliminated exactly as for $d = 2$. Since f in S1 with CM by $\mathbb{Q}(\sqrt{-5})$ verify $a_3 = \pm(i - 1)$ we only need the condition $p \equiv 1 \bmod 4$, because $3 \mid a + b$.
- For f in S3 consider $f \otimes \chi$ known to have level $800 = 2^5 5^2$ and twist $E_\gamma(a, b)$ by 2.
- If $\mathrm{cond}_2(E_{\gamma,2}) \neq 2^5$ we have a contradiction by Carayol.
- If $\mathrm{cond}_2(E_{\gamma,2}) = 2^5$ then since $E_{\gamma,2}$ mod $\mathfrak{P}_3$ is equal to $E_\gamma(a, b)$ mod $\mathfrak{P}_3$ we have $a_{\mathfrak{P}_3}(E_{\gamma,2}) = -18$ which gives a contradiction with $a_{\mathfrak{P}_3}(f)$ as before.

d=3: a+b even

Suppose $a + b$ even.

- We eliminate newforms of type S2 and S3 exactly with the same arguments used when $d = 2$.
- For f in S1 we only need to suppose that is $p \equiv 1 \bmod 4$ to get a contradiction since newforms with CM by $\mathbb{Q}(\sqrt{-5})$ verify $a_3 = \pm(i - 1)$.

Theorem

For any $p > 73$ such that $p \equiv 1 \bmod 4$, the equation $x^5 + y^5 = 3\gamma z^p$ has no non-trivial primitive solutions.

d=3: a+b even

Suppose $a+b$ even.

- We eliminate newforms of type S2 and S3 exactly with the same arguments used when $d=2$.
- For f in S1 we only need to suppose that is $p \equiv 1 \bmod 4$ to get a contradiction since newforms with CM by $\mathbb{Q}(\sqrt{-5})$ verify $a_3 = \pm(i-1)$.

Theorem

For any $p > 73$ such that $p \equiv 1 \bmod 4$, the equation $x^5 + y^5 = 3\gamma z^p$ has no non-trivial primitive solutions.

Definition

Let $F_{(a,b)}$ be the elliptic curve defined over $\mathbb{Q}(\sqrt{5})$ given by

$$F_{(a,b)} : y^2 = x^3 + 2(a-b)x^2 + (\frac{3}{10}\sqrt{5} + \frac{1}{2})\phi_1(a,b)x.$$

- $F_{(a,b)}$ is a $\mathbb{Q}$-curve.
- As in the case of E we apply Quer's theory, Milne's Formula and Serre's conjecture.
- We have $\bar{\rho} \equiv \bar{\rho}_{f,p}$ for newforms with level 100, 400 or 1600 if $8 \mid a+b$, $4 \parallel a+b$ or $2 \parallel a+b$, respectively.
- If $2 \nmid a+b$ we can suppose that a is even and we are in level 800 or 1600 if $4 \mid a$ or $4 \nmid a$, respectively.

Definition

Let $F_{(a,b)}$ be the elliptic curve defined over $\mathbb{Q}(\sqrt{5})$ given by

$$F_{(a,b)} : y^2 = x^3 + 2(a-b)x^2 + (\frac{3}{10}\sqrt{5} + \frac{1}{2})\phi_1(a,b)x.$$

- $F_{(a,b)}$ is a $\mathbb{Q}$-curve.
- As in the case of E we apply Quer's theory, Milne's Formula and Serre's conjecture.
- We have $\bar{\rho} \equiv \bar{\rho}_{f,p}$ for newforms with level 100, 400 or 1600 if $8 \mid a+b$, $4 \parallel a+b$ or $2 \parallel a+b$, respectively.
- If $2 \nmid a+b$ we can suppose that a is even and we are in level 800 or 1600 if $4 \mid a$ or $4 \nmid a$, respectively.

Multi-Frey technique

- Suppose that $a^5 + b^5 = dc^p$ and that c is even.
- Then we have a solution (a, b, c_0) to $x^5 + y^5 = d2^p z^p$ and by B-D it is impossible.
- We can suppose c to be odd and we only have to deal with the cases $2 \parallel a + b$ or $2 \nmid a + b$.
- Thus we have to eliminate newforms only on levels 1600 ($d = 2$) or 1600 and 800 ($d = 3$).
- These are the same levels as in the case of $E_{(a,b)}$
- For a solution (a, b, c) we have a double congruence $(\bar{\rho}_E, \bar{\rho}_F) \equiv (\bar{\rho}_{f,p}|K, \bar{\rho}_{g,p}|K) \pmod{\mathfrak{P}}$, where f, g are newforms in $S_2(M, \epsilon^{-1})$ both with level $M = 800$ or $M = 1600$.
- We can apply the multi-Frey technique with E and F!

Multi-Frey technique

Definition

Let $C_{(x,y)}/K$ be $E_{(x,y)}$ or $F_{(x,y)}$. For a prime q of good reduction for C and newform f let

$$C_{(x,y)}(q,f) = a_q(C_{(x,y)}) - a_q(f|K)$$

Theorem (Siksek)

Let (f,g) be a pair of newforms and define

$$A_q(f,g) = \prod_{(x,y)\in\mathbb{F}_q-\{(0,0)\}} \gcd(E_{(x,y)}(q,f)), F_{(x,y)}(q,g)).$$

If (a,b,c) is a primitive solution giving rise to the double congruence $(\bar{\rho}_E, \bar{\rho}_F) \equiv (\bar{\rho}_{f,p}|K, \bar{\rho}_{g,p}|K) \pmod{\mathfrak{P}}$ then $p \mid A_q$.

- We want to improve the conditions on p which comes from CM forms.
- In level 800 there are no newforms with CM
- In level 1600 there are f_1,f_2 by $\mathbb{Q}(i)$ and g_1,g_2 by $\mathbb{Q}(\sqrt{-5})$
- Let SS1 be the set of pairs (f, g) where f has no CM and SS2 the set of those where f has CM.
- We eliminate a pair (f, g) in SS1 by applying the arguments on f explained before.
- Given (f, g) in SS2 we compute $A_q(f, g)$ using the auxiliary primes $q = 3, 7, 13, 17$ to find that $A_q(f, g) = 0$ for all the auxiliary primes only if f, g have CM by distinct fields.
- Remain four pairs: (f_1, g_1), (f_1, g_2), (g_1, f_1) and (g_2, f_2).
- For a prime $p \equiv 1 \pmod 4$ or $p \equiv \pm 1 \pmod 5$ we can eliminate these pairs by applying Ellenberg's theorem to E or F convenientyl to get a contradiction! q.e.d.

- We want to improve the conditions on p which comes from CM forms.
- In level 800 there are no newforms with CM
- In level 1600 there are f_1,f_2 by $\mathbb{Q}(i)$ and g_1,g_2 by $\mathbb{Q}(\sqrt{-5})$
- Let SS1 be the set of pairs (f, g) where f has no CM and SS2 the set of those where f has CM.
- We eliminate a pair (f, g) in SS1 by applying the arguments on f explained before.
- Given (f, g) in SS2 we compute $A_q(f, g)$ using the auxiliary primes $q = 3, 7, 13, 17$ to find that $A_q(f, g) = 0$ for all the auxiliary primes only if f, g have CM by distinct fields.
- Remain four pairs: (f_1, g_1), (f_1, g_2), (g_1, f_1) and (g_2, f_2).
- For a prime $p \equiv 1 \pmod 4$ or $p \equiv \pm 1 \pmod 5$ we can eliminate these pairs by applying Ellenberg's theorem to E or F convenientyl to get a contradiction! q.e.d.