Some Generalized Fermat-type Equations via $\mathbb{Q}$-curves and Modularity.

Nuno Freitas

Universitat de Barcelona

22 October 2012

Advisor: Luis Dieulefait

Outline

1. Introduction to the modular approach.
2. Multi-Frey technique to equations of signature $(5, 5, p)$
3. Frey curves for equations of signature (r, r, p) for $r \geq 7$
4. Modularity and Irreducibility of Galois representations attached to certain elliptic curves.
5. Applications to $r = 13$ and $r = 7$
6. Conclusions and Contributions

1) Introduction to the modular approach.

Everything started in the 17th century in a small margin...saying

Theorem (Fermat's Last Theorem)

Let $n > 2$ be an integer. Then, the equation $x^n + y^n = z^n$ has no solutions (a, b, c) such that $abc \neq 0$.

Brief story of the Proof: Assume (a, b, c) is such that $abc \neq 0$ and $a^p + b^p = c^p$ for a prime $p \geq 5$.

- In 1984 Frey considered the elliptic curve over $\mathbb{Q}$

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

- In the following years Frey, Hellegouarch, Serre, Mazur and Ribet proved that E has unusual properties.

Introduction

Everything started in the 17th century in a small margin...saying

Theorem (Fermat's Last Theorem)

Let $n > 2$ be an integer. Then, the equation $x^n + y^n = z^n$ has no solutions (a, b, c) such that $abc \neq 0$.

Brief story of the Proof: Assume (a, b, c) is such that $abc \neq 0$ and $a^p + b^p = c^p$ for a prime $p \geq 5$.

- In 1984 Frey considered the elliptic curve over $\mathbb{Q}$

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

- In the following years Frey, Hellegouarch, Serre, Mazur and Ribet proved that E has unusual properties.

Introduction

Everything started in the 17th century in a small margin...saying

Theorem (Fermat's Last Theorem)

Let $n > 2$ be an integer. Then, the equation $x^n + y^n = z^n$ has no solutions (a, b, c) such that $abc \neq 0$.

Brief story of the Proof: Assume (a, b, c) is such that $abc \neq 0$ and $a^p + b^p = c^p$ for a prime $p \geq 5$.

- In 1984 Frey considered the elliptic curve over $\mathbb{Q}$

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

- In the following years Frey, Hellegouarch, Serre, Mazur and Ribet proved that E has unusual properties.

Introduction

- In 1994 Wiles' proved another property: E is modular.
- Conclusion: E has so many remarkable properties that does not exist.
- Thus (a, b, c) does not exist.

This strategy (that I will make more precise in a moment!) is now baptized as **the modular approach to Diophantine equations** and it has been extended by several mathematicians to attack other equations.

Introduction

- In 1994 Wiles' proved another property: E is modular.
- Conclusion: E has so many remarkable properties that does not exist.
- Thus (a, b, c) does not exist.

This strategy (that I will make more precise in a moment!) is now baptized as **the modular approach to Diophantine equations** and it has been extended by several mathematicians to attack other equations.

Introduction

- In 1994 Wiles' proved another property: E is modular.
- Conclusion: E has so many remarkable properties that does not exist.
- Thus (a, b, c) does not exist.

This strategy (that I will make more precise in a moment!) is now baptized as **the modular approach to Diophantine equations** and it has been extended by several mathematicians to attack other equations.

Introduction

Some generalizations of the Frey curves for Fermat-type equations:

(1) **Darmon-Merel (1997):**
$x^p + y^p = z^2 \quad and \quad x^p + y^p = z^3$ for $p \geq 3$
Non semistable Frey curves over $\mathbb{Q}$.

(2) **Ellenberg (2004):** $x^2 + y^4 = z^p$ for $p \geq 211$
Frey curves over number fields that are $\mathbb{Q}$-curves.

(3) **Jarvis-Meekin (2004):**
$x^p + y^p = z^p$ for $p > 3$ over $\mathbb{Q}(\sqrt{2})$
Semistable Frey curves over a totally real field

(4) **Bennett-Chen (2011):**
$x^2 + y^6 = z^p$ for $p \geq 3$
Siksek multi-Frey technique with one Frey curve over $\mathbb{Q}$ and one Frey $\mathbb{Q}$-curve.

Broadly speaking, the modular approach to Diophantine equations is divided into the following steps:

(1) **Construction of a Frey curve:** Attach an elliptic curve E over a number field K to a putative solution of the equation.

(2) **Modularity/Level Lowering:** Prove modularity of E and irreducibility of $\bar{\rho}_{E,p}$ in order to conclude via level lowering results, that the representation $\bar{\rho}_{E,p}$ corresponds to a (Hilbert) newform whose level is almost independent of the choice of the solution;

(3) **Contradiction:** Contradict the previous step by showing that among the (Hilbert) newforms on the predicted spaces, none of them corresponds to $\bar{\rho}_{E,p}$.

Broadly speaking, the modular approach to Diophantine equations is divided into the following steps:

(1) **Construction of a Frey curve:** Attach an elliptic curve E over a number field K to a putative solution of the equation.

(2) **Modularity/Level Lowering:** Prove modularity of E and irreducibility of $\bar{\rho}_{E,p}$ in order to conclude via level lowering results, that the representation $\bar{\rho}_{E,p}$ corresponds to a (Hilbert) newform whose level is almost independent of the choice of the solution;

(3) **Contradiction:** Contradict the previous step by showing that among the (Hilbert) newforms on the predicted spaces, none of them corresponds to $\bar{\rho}_{E,p}$.

Introduction

Broadly speaking, the modular approach to Diophantine equations is divided into the following steps:

(1) **Construction of a Frey curve:** Attach an elliptic curve E over a number field K to a putative solution of the equation.

(2) **Modularity/Level Lowering:** Prove modularity of E and irreducibility of $\bar{\rho}_{E,p}$ in order to conclude via level lowering results, that the representation $\bar{\rho}_{E,p}$ corresponds to a (Hilbert) newform whose level is almost independent of the choice of the solution;

(3) **Contradiction:** Contradict the previous step by showing that among the (Hilbert) newforms on the predicted spaces, none of them corresponds to $\bar{\rho}_{E,p}$.

Introduction

Broadly speaking, the modular approach to Diophantine equations is divided into the following steps:

(1) **Construction of a Frey curve:** Attach an elliptic curve E over a number field K to a putative solution of the equation.

(2) **Modularity/Level Lowering:** Prove modularity of E and irreducibility of $\bar{\rho}_{E,p}$ in order to conclude via level lowering results, that the representation $\bar{\rho}_{E,p}$ corresponds to a (Hilbert) newform whose level is almost independent of the choice of the solution;

(3) **Contradiction:** Contradict the previous step by showing that among the (Hilbert) newforms on the predicted spaces, none of them corresponds to $\bar{\rho}_{E,p}$.

Introduction

We are interested in **the Generalized Fermat equation:**

$$Ax^p + By^q = Cz^r,$$

where

- A, B, C pairwise coprime integers and $ABC \neq 0$
- $1/p + 1/q + 1/r < 1$

The triple (p, q, r) is called the **signature** of the equation.

Theorem (Darmon-Granville)

Let $A, B, C \in \mathbb{Z}$ be pairwise coprime. Fix (p, q, r) such that $1/p + 1/q + 1/r < 1$. Then $Aa^p + Bb^q = Cc^r$ has only a finite number of solutions satisfying $\gcd(a, b, c) = 1$.

We are interested in **the Generalized Fermat equation:**

$$Ax^p + By^q = Cz^r,$$

where

- A, B, C pairwise coprime integers and $ABC \neq 0$
- $1/p + 1/q + 1/r < 1$

The triple (p, q, r) is called the **signature** of the equation.

Theorem (Darmon-Granville)

Let $A, B, C \in \mathbb{Z}$ be pairwise coprime. Fix (p, q, r) such that $1/p + 1/q + 1/r < 1$. Then $Aa^p + Bb^q = Cc^r$ has only a finite number of solutions satisfying $\gcd(a, b, c) = 1$.

But more is conjectured

Conjecture

Let $A, B, C \in \mathbb{Z}$ be fixed and pairwise coprime. There is only a finite number of sextuples (a, b, c, p, q, r) satisfying:

- $p, q, r \in \mathbb{Z}$ primes such that $1/p + 1/q + 1/r < 1$,
- $(a, b, c) \in (\mathbb{Z} \setminus \{0\})^3$ and $\gcd(a, b, c) = 1$,
- $Aa^p + Bb^q = Cc^r$.

Rmk: Solutions like $1^p + 2^3 = 3^2$ are counted only once.

Regarding this conjecture, in what follows we will:

- Provide more evidence to the conjecture for signatures $(5, 5, p)$, $(7, 7, p)$, $(13, 13, p)$.
- Describe a general method to attack some equations of signature (r, r, p) for all primes $r \geq 7$.

But more is conjectured

Conjecture

Let $A, B, C \in \mathbb{Z}$ be fixed and pairwise coprime. There is only a finite number of sextuples (a, b, c, p, q, r) satisfying:

- $p, q, r \in \mathbb{Z}$ primes such that $1/p + 1/q + 1/r < 1$,
- $(a, b, c) \in (\mathbb{Z} \setminus \{0\})^3$ and $\gcd(a, b, c) = 1$,
- $Aa^p + Bb^q = Cc^r$.

Rmk: Solutions like $1^p + 2^3 = 3^2$ are counted only once.

Regarding this conjecture, in what follows we will:

- Provide more evidence to the conjecture for signatures $(5, 5, p)$, $(7, 7, p)$, $(13, 13, p)$.
- Describe a general method to attack some equations of signature (r, r, p) for all primes $r \geq 7$.

2) Multi-Frey technique to equations of signature $(5, 5, p)$

Equations of signature $(5, 5, p)$

Theorem (Chap. 2)

Let β be an integer divisible only by primes $\ell \not\equiv 1 \pmod 5$. Suppose that $p \equiv 1 \pmod 4$ or $p \equiv \pm 1 \pmod 5$. Then,

(*A*) If $p > 13$, the equation $x^5 + y^5 = 2\beta z^p$ has no solutions (a, b, c) such that $|abc| > 1$ and $(a, b) = 1$.

(*B*) If $p > 73$, the equation $x^5 + y^5 = 3\beta z^p$ has no solutions (a, b, c) such that $|abc| > 1$ and $(a, b) = 1$.

Note that over $\mathbb{Q}(\sqrt{5})$ we have

$$x^5 + y^5 = (x + y)\phi(x, y) = (x + y)\phi_1(x, y)\phi_2(x, y),$$

where

$$\phi_1(x, y) = x^2 + \omega xy + y^2, \quad \text{and} \quad \phi_2(x, y) = x^2 + \bar{\omega} xy + y^2$$

$$\omega = \frac{-1 + \sqrt{5}}{2} \quad \text{and } \bar{\omega} = \frac{-1 - \sqrt{5}}{2}.$$

Equations of signature $(5, 5, p)$

Theorem (Chap. 2)

Let β be an integer divisible only by primes $\ell \not\equiv 1 \pmod 5$. Suppose that $p \equiv 1 \pmod 4$ or $p \equiv \pm 1 \pmod 5$. Then,

(A) If $p > 13$, the equation $x^5 + y^5 = 2\beta z^p$ has no solutions (a, b, c) such that $|abc| > 1$ and $(a, b) = 1$.

(B) If $p > 73$, the equation $x^5 + y^5 = 3\beta z^p$ has no solutions (a, b, c) such that $|abc| > 1$ and $(a, b) = 1$.

Note that over $\mathbb{Q}(\sqrt{5})$ we have

$$x^5 + y^5 = (x + y)\phi(x, y) = (x + y)\phi_1(x, y)\phi_2(x, y),$$

where

$$\phi_1(x, y) = x^2 + \omega xy + y^2, \quad \text{and} \quad \phi_2(x, y) = x^2 + \bar{\omega}xy + y^2$$

$$\omega = \frac{-1 + \sqrt{5}}{2} \quad \text{and } \bar{\omega} = \frac{-1 - \sqrt{5}}{2}.$$

Let (a, b, c) be a solution to $x^5 + y^5 = dz^p$ such that $(a, b) = 1$. Hence

- $\phi(a, b) = c_0^p$ and $\phi_1(a, b) = c_1^p$ and $d \mid a + b$ or,
- $\phi(a, b) = 5c_0^p$ and $\phi_1(a, b) = \sqrt{5}c_1^p$ and $d \mid a + b$

where $c_0 \mid c$ and c_1 divide c in $\mathbb{Q}(\sqrt{5})$.

Definition

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

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

Its discriminant is

$$\Delta(E) = 2^6\bar{\omega}\phi\phi_1 = \begin{cases} 2^6\bar{\omega}(c_0c_1)^p & \text{if } 5 \nmid a + b, \\ 2^6\bar{\omega}5\sqrt{5}(c_0c_1)^p & \text{if } 5 \mid a + b. \end{cases}$$

Let (a,b,c) be a solution to $x^5+y^5=dz^p$ such that $(a,b)=1$. Hence

- $\phi(a,b)=c_0^p$ and $\phi_1(a,b)=c_1^p$ and $d \mid a+b$ or,
- $\phi(a,b)=5c_0^p$ and $\phi_1(a,b)=\sqrt{5}c_1^p$ and $d \mid a+b$

where $c_0 \mid c$ and c_1 divide c in $\mathbb{Q}(\sqrt{5})$.

Definition

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

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

Its discriminant is

$$\Delta(E) = 2^6\bar{\omega}\phi\phi_1 = \begin{cases} 2^6\bar{\omega}(c_0c_1)^p & \text{if } 5 \nmid a+b, \\ 2^6\bar{\omega}5\sqrt{5}(c_0c_1)^p & \text{if } 5 \mid a+b. \end{cases}$$

Equations of signature $(5, 5, p)$

Theorem (Chap. 2)

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 endomorphism algebra isomorphic to $\mathbb{Q}(i)$.

Let ϵ be a charecter fixing K. In particular, it follows that

- There are 4 Galois representations of $G_\mathbb{Q}$ extending $\rho_{E_\gamma,p}$ and they satisfy

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

Theorem (Chap. 2)

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 endomorphism algebra isomorphic to $\mathbb{Q}(i)$.

Let ϵ be a charecter fixing K. In particular, it follows that

- There are 4 Galois representations of $G_\mathbb{Q}$ extending $\rho_{E_\gamma,p}$ and they satisfy

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

Equations of signature $(5, 5, p)$

Let p be the prime in $x^5 + y^5 = Cz^p$. We let $\bar{\rho} := \bar{\rho}_{S_1,\lambda}$, $\lambda \mid p$ and we want to apply Serre's conjecture to it.

Serre Conjecture (Khare, Wintenberger)

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

Theorem (Frey-Hellegouarch)

Let E/K be an elliptic curve and $\ell \nmid 2, p$ unramified in K. If ℓ is semistable for E and $p | \nu_\ell(\Delta_m(E))$ then $\bar{\rho}_{E,p}$ is unramified at ℓ. Moreover, if $\ell \mid p$ then $\bar{\rho}_{E,p}$ is finite at ℓ.

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 $\bar{\rho} \sim \bar{\rho}_{f,\mathfrak{P}}$

Equations of signature $(5, 5, p)$

Let p be the prime in $x^5 + y^5 = Cz^p$. We let $\bar{\rho} := \bar{\rho}_{S_1,\lambda}$, $\lambda \mid p$ and we want to apply Serre's conjecture to it.

Serre Conjecture (Khare, Wintenberger)

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

Theorem (Frey-Hellegouarch)

Let E/K be an elliptic curve and $\ell \nmid 2, p$ unramified in K. If ℓ is semistable for E and $p | \nu_\ell(\Delta_m(E))$ then $\bar{\rho}_{E,p}$ is unramified at ℓ. Moreover, if $\ell \mid p$ then $\bar{\rho}_{E,p}$ is finite at ℓ.

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 $\bar{\rho} \sim \bar{\rho}_{f,\mathfrak{P}}$

Equations of signature $(5, 5, p)$

Given a primitive solution (a, b, c) we consider also the Frey curve

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

- $F_{(a,b)}$ are also $\mathbb{Q}$-curves.
- We can apply to it everything that we have done with $E_{(a,b)}$.
- With two Frey curves we can apply Siksek's multi-Frey technique.

In particular, we have a double isomorphism

$$(\bar{\rho}_{E_\gamma,p}, \bar{\rho}_{F_\gamma,p}) \sim (\bar{\rho}_{f,\mathfrak{P}}|G_K, \bar{\rho}_{g,\mathfrak{P}'}|G_K)$$

where $f \in S_2(M_f, \bar{\epsilon})$ and $g \in S_2(M_g, \bar{\epsilon})$ where the pair of levels (M_f, M_g) may be $(400, 100)$, $(100, 400)$, $(1600, 1600)$ or $(800, 800)$.

Equations of signature $(5, 5, p)$

For each of the finite possible pairs (f, g) we show that the previous isomorphism never holds!!

For example, let (f, g) be such that f has no CM, level 1600 and $\mathbb{Q}_f = \mathbb{Q}(i)$. Let χ be the character of $\mathbb{Q}(\sqrt{2})$.

- With SAGE we computed the coefficients of $f \otimes \chi$ to find that $f \otimes \chi$ are all of level of level 800.
- Let $E_{\gamma,2}$ the twist of E_γ by 2. The representation $\rho_1 := \rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_{\gamma,2},p}$.
- $\bar{\rho}_1$ is modular of type $(M_1, 2, \bar{\epsilon})$ with $M = 100$ or 400
- $\bar{\rho}_1 = \overline{\rho_{S_1,\lambda} \otimes \chi} \sim \bar{\rho} \otimes \bar{\chi} \sim \bar{\rho}_{f,p} \otimes \bar{\chi} \sim \bar{\rho}_{f \otimes \chi, p} \sim \bar{\rho}_{f',p}$,
- We know that f' has level 800
- Contradiction, since this kind of level lowering can not happen (by Carayol)!

Equations of signature $(5, 5, p)$

For each of the finite possible pairs (f, g) we show that the previous isomorphism never holds!!

For example, let (f, g) be such that f has no CM, level 1600 and $\mathbb{Q}_f = \mathbb{Q}(i)$. Let χ be the character of $\mathbb{Q}(\sqrt{2})$.

- With SAGE we computed the coefficients of $f \otimes \chi$ to find that $f \otimes \chi$ are all of level of level 800.
- Let $E_{\gamma,2}$ the twist of E_γ by 2. The representation $\rho_1 := \rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_{\gamma,2},p}$.
- $\bar{\rho}_1$ is modular of type $(M_1, 2, \bar{\epsilon})$ with $M = 100$ or 400
- $\bar{\rho}_1 = \overline{\rho_{S_1,\lambda} \otimes \chi} \sim \bar{\rho} \otimes \bar{\chi} \sim \bar{\rho}_{f,p} \otimes \bar{\chi} \sim \bar{\rho}_{f \otimes \chi, p} \sim \bar{\rho}_{f',p}$,
- We know that f' has level 800
- Contradiction, since this kind of level lowering can not happen (by Carayol)!

Equations of signature $(5, 5, p)$

For each of the finite possible pairs (f, g) we show that the previous isomorphism never holds!!

For example, let (f, g) be such that f has no CM, level 1600 and $\mathbb{Q}_f = \mathbb{Q}(i)$. Let χ be the character of $\mathbb{Q}(\sqrt{2})$.

- With SAGE we computed the coefficients of $f \otimes \chi$ to find that $f \otimes \chi$ are all of level of level 800.
- Let $E_{\gamma,2}$ the twist of E_γ by 2. The representation $\rho_1 := \rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_{\gamma,2},p}$.
- $\bar{\rho}_1$ is modular of type $(M_1, 2, \bar{\epsilon})$ with $M = 100$ or 400
- $\bar{\rho}_1 = \overline{\rho_{S_1,\lambda} \otimes \chi} \sim \bar{\rho} \otimes \bar{\chi} \sim \bar{\rho}_{f,p} \otimes \bar{\chi} \sim \bar{\rho}_{f\otimes\chi,p} \sim \bar{\rho}_{f',p}$,
- We know that f' has level 800
- Contradiction, since this kind of level lowering can not happen (by Carayol)!

Equations of signature $(5, 5, p)$

For each of the finite possible pairs (f, g) we show that the previous isomorphism never holds!!

For example, let (f, g) be such that f has no CM, level 1600 and $\mathbb{Q}_f = \mathbb{Q}(i)$. Let χ be the character of $\mathbb{Q}(\sqrt{2})$.

- With SAGE we computed the coefficients of $f \otimes \chi$ to find that $f \otimes \chi$ are all of level of level 800.
- Let $E_{\gamma,2}$ the twist of E_γ by 2. The representation $\rho_1 := \rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_{\gamma,2},p}$.
- $\bar{\rho}_1$ is modular of type $(M_1, 2, \bar{\epsilon})$ with $M = 100$ or 400
- $\bar{\rho}_1 = \overline{\rho_{S_1,\lambda} \otimes \chi} \sim \bar{\rho} \otimes \bar{\chi} \sim \bar{\rho}_{f,p} \otimes \bar{\chi} \sim \bar{\rho}_{f\otimes\chi,p} \sim \bar{\rho}_{f',p}$,
- We know that f' has level 800
- Contradiction, since this kind of level lowering can not happen (by Carayol)!

3) Frey curves for equations of signature (r, r, p) for $r \geq 7$

Equations of signature (r, r, p) for $r \geq 7$

- Let $r \geq 7$ be a fixed prime and K^+ be the maximal totally real subfield of $\mathbb{Q}(\zeta_r)$.
- Let h_r^+ be the class number of K^+.
- For $r = 6k + 1$ we denote by K_0 the subfield of K^+ of degree k.

Theorem (Chap. 3 and 5)

Let $C \in \mathbb{Z} \backslash \{0\}$ be divisible only by primes $q \not\equiv 1, 0 \pmod{r}$. Then,

1. There are Frey curves over K^+ attached to the equations $x^r + y^r = Cz^p$
2. If $r = 6k + 1$ there are Frey curves defined over K_0.
3. If $r = 4m + 1$ there are two more Frey curves.

From now on we suppose that C is as in the statement.

Equations of signature (r, r, p) for $r \geq 7$

Let $\zeta = \zeta_r$ and observe that

$$x^r + y^r = (x + y)\phi_r(x, y)$$

and that over $\mathbb{Q}(\zeta)$ we have

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

Since $r - 1 \geq 6$ is even we choose three different factors f_i of ϕ_r with coefficients in K^+ of the form

$$f_i = (x + \zeta^{k_i} y)(x + \zeta^{r-k_i} y).$$

From now on we will be considering triples (k_1, k_2, k_3) $(1 \leq k_i \leq r - 1)$ such that the corresponding three polynomials f_1, f_2, f_3 are different.

Lemma

Let $r \geq 7$ and (k_1, k_2, k_3) be fixed. Let $p \nmid h_r^+$ be a prime. Suppose there is a solution (a, b, c') to $x^r + y^r = Cz^p$ such that $|abc'| > 1$ and $(a, b) = 1$. Then, there exists a unit $\mu \in \mathcal{O}_{K^+}^\times$ and a solution (a, b, c) in $\mathbb{Z}^2 \times \mathcal{O}_{K^+}$ such that $|Norm_{K^+/\mathbb{Q}}(c)| > 1$ (non-trivial) to

$$f_1(x, y)f_2(x, y)f_3(x, y) = \mu z^p \quad \text{or} \tag{1}$$

$$f_1(x, y)f_2(x, y)f_3(x, y) = \mu \pi_r^3 z^p, \tag{2}$$

which satisfies $r \nmid a + b$ in case (1) and $r \mid a + b$ in case (2). Moreover:

- *if $d \mid C$, then $d \mid a + b$;*
- *the primes in K^+ divisors of c are all above rational primes congruent to $1 \pmod{r}$. In particular, neither the primes above 2 nor the primes above r divide c.*

Equations of signature (r, r, p) for $r \geq 7$

Fix $r \geq 7$ and (k_1, k_2, k_3). Recall that

$$\begin{cases} f_1(x,y) = x^2 + (\zeta^{k_1} + \zeta^{r-k_1})xy + y^2, \\ f_2(x,y) = x^2 + (\zeta^{k_2} + \zeta^{r-k_2})xy + y^2, \\ f_3(x,y) = x^2 + (\zeta^{k_3} + \zeta^{r-k_3})xy + y^2. \end{cases}$$

We are interested in finding a triple (α, β, γ) such that

$$\alpha f_1 + \beta f_2 + \gamma f_3 = 0.$$

We see from the form of the f_i that finding (α, β, γ) is always possible, because it is a solution of a linear system with two equations in three variables. In particular, we choose the solution

$$\begin{cases} \alpha = -(\zeta^{k_2} + \zeta^{r-k_2} - \zeta^{k_3} - \zeta^{r-k_3}), \\ \beta = \zeta^{k_1} + \zeta^{r-k_1} - \zeta^{k_3} - \zeta^{r-k_3}, \\ \gamma = -\zeta^{k_1} - \zeta^{r-k_1} + \zeta^{k_2} + \zeta^{r-k_2}. \end{cases}$$

Equations of signature (r, r, p) for $r \geq 7$

Suppose now that $(a, b, c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ is a primitive solution to equation (1) or (2) and let

$$A(a,b) = \alpha f_1(a,b), \quad B(a,b) = \beta f_2(a,b), \quad C(a,b) = \gamma f_3(a,b).$$

Observe that $A + B + C = 0$.

We define the Frey curve over K^+

$$E_{(a,b)} : y^2 = x(x - A(a,b))(x + B(a,b))$$

satisfying

$$\Delta = 2^4(AB(A+B))^2 = \begin{cases} \mu^2 2^4 (\alpha\beta\gamma)^2 c^{2p} & \text{if } r \nmid a+b, \\ \mu^2 2^4 (\alpha\beta\gamma)^2 \pi_r^6 c^{2p} & \text{if } r \mid a+b. \end{cases}$$

Equations of signature (r, r, p) for $r \geq 7$

Suppose now that $(a, b, c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ is a primitive solution to equation (1) or (2) and let

$$A(a,b) = \alpha f_1(a,b), \quad B(a,b) = \beta f_2(a,b), \quad C(a,b) = \gamma f_3(a,b).$$

Observe that $A + B + C = 0$.

We define the Frey curve over K^+

$$E_{(a,b)} : y^2 = x(x - A(a,b))(x + B(a,b))$$

satisfying

$$\Delta = 2^4(AB(A+B))^2 = \begin{cases} \mu^2 2^4 (\alpha\beta\gamma)^2 c^{2p} & \text{if } r \nmid a+b, \\ \mu^2 2^4 (\alpha\beta\gamma)^2 \pi_r^6 c^{2p} & \text{if } r \mid a+b. \end{cases}$$

Equations of signature (r, r, p) for $r \geq 7$

Let $r = 6k + 1$ and σ a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$. Denote by K_0 the totally real subfield of K^+ with degree k.

Theorem (Chap. 3)

Fix $(k_1, k_2, k_3) = (1, n_2, n_3)$, where $\zeta_r^{n_2} = \sigma^{2k}(\zeta_r)$ and $\zeta_r^{n_3} = \sigma^{4k}(\zeta_r)$. Suppose that (a, b, c) is a primitive solution of (1) or (2). Then the Frey curves $E_{(a,b)}/K^+$ have a model over K_0.

Proof: We have $\sigma^{2k}(A) = B, \sigma^{2k}(B) = C, \sigma^{2k}(C) = A$. Moreover, the short Weierstrass form satisfies

$$\begin{aligned} a_4 &= -432(AB + BC + CA) = \sigma^{2k}(a_4) \\ a_6 &= -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3) \\ &= -1728(2(-B - C)^3 + 3(-B - C)^2B - 3(-B - C)B^2 - 2B^3) \\ &= -1728(2B^3 + 3B^2C - 3BC^2 - 2C^3) = \sigma^{2k}(a_6) \end{aligned}$$

Equations of signature (r, r, p) for $r \geq 7$

Let $r = 6k + 1$ and σ a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$. Denote by K_0 the totally real subfield of K^+ with degree k.

Theorem (Chap. 3)

Fix $(k_1, k_2, k_3) = (1, n_2, n_3)$, where $\zeta_r^{n_2} = \sigma^{2k}(\zeta_r)$ and $\zeta_r^{n_3} = \sigma^{4k}(\zeta_r)$. Suppose that (a, b, c) is a primitive solution of (1) or (2). Then the Frey curves $E_{(a,b)}/K^+$ have a model over K_0.

Proof: We have $\sigma^{2k}(A) = B, \sigma^{2k}(B) = C, \sigma^{2k}(C) = A$. Moreover, the short Weierstrass form satisfies

$$
\begin{aligned}
a_4 &= -432(AB + BC + CA) = \sigma^{2k}(a_4) \\
a_6 &= -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3) \\
&= -1728(2(-B - C)^3 + 3(-B - C)^2B - 3(-B - C)B^2 - 2B^3) \\
&= -1728(2B^3 + 3B^2C - 3BC^2 - 2C^3) = \sigma^{2k}(a_6)
\end{aligned}
$$

4) Modularity and Irreducibility of Galois representations attached to certain elliptic curves.

Modularity and Irreducibility

Theorem (Chap. 3)

Let F be a totally real abelian number field and C and elliptic curve defined over F. Suppose that 3 splits completely in F and C has good reduction at the primes above 3. Then C is modular.

Idea of proof: First prove that, when irreducible, $\bar{\rho}_{C,3}$ is modular via Langlands-Tunnel theorem. Then we divide into three cases

1. Assume $\bar{\rho}_{C,3}$ and $\bar{\rho}_{C,3}|G_{F(\sqrt{-3})}$ both abs. irred.
2. Assume $\bar{\rho}_{C,3}$ abs. irr. and $\bar{\rho}_{C,3}|G_{F(\sqrt{-3})}$ both reducible.
3. Assume $\bar{\rho}_{C,3}$ abs. reducible.

and we show that in each case a modularity lifting theorem applies.

Modularity and Irreducibility

1. Kisin's modularity lifting theorem for potentially Barsotti-Tate representations.
2. Skinner-Wiles for residually modular nearly ordinary reps.
3. Skinner-Wiles for residually reducible ordinary reps.

Theorem (Chap. 3)

Let F be a totally real number field and C/F be an elliptic curve with conductor N_E. Let A be the factor of N_E corresponding to the additive primes. Suppose further that $\mathfrak{q} \nmid N_C$ is a fixed prime of good reduction. Then, there exist an explicit constant $M(F, A, \mathfrak{q})$ such that, if

1) p is odd and unramified in F,
2) all primes $\mathfrak{p} \mid p$ are of semistable reduction for C,
3) $p > M(F, A, \mathfrak{q})$,

then, the representation $\bar{\rho}_{C,p}$ is absolutely irreducible.

Modularity and Irreducibility

1. Kisin's modularity lifting theorem for potentially Barsotti-Tate representations.
2. Skinner-Wiles for residually modular nearly ordinary reps.
3. Skinner-Wiles for residually reducible ordinary reps.

Theorem (Chap. 3)

Let F be a totally real number field and C/F be an elliptic curve with conductor N_E. Let A be the factor of N_E corresponding to the additive primes. Suppose further that $\mathfrak{q} \nmid N_C$ is a fixed prime of good reduction. Then, there exist an explicit constant $M(F, A, \mathfrak{q})$ such that, if

1) p is odd and unramified in F,
2) all primes $\mathfrak{p} \mid p$ are of semistable reduction for C,
3) $p > M(F, A, \mathfrak{q})$,

then, the representation $\bar{\rho}_{C,p}$ is absolutely irreducible.

4) Applications to the cases $r = 13$ and $r = 7$.

Theorem (Chap. 4)

Let $d = 3, 5, 7$ or 11 and γ be an integer divisible only by primes $\ell \neq 13$ satisfying $\ell \not\equiv 1 \pmod{13}$. Let also $p > 4992539$ be a prime. Then,

(*I*) The equation

$$x^{13} + y^{13} = d\gamma z^p$$

has no solutions (a, b, c) such that $|abc| > 1$ (non-trivial), $\gcd(a, b) = 1$ (primitive) and $13 \nmid c$.

(*II*) The equation

$$x^{26} + y^{26} = 2d\gamma z^p$$

has no non-trivial primitive solutions.

Since $13 = 6 \times 2 + 1$ we have,

$$k = 2, \quad K_0 = \mathbb{Q}(\sqrt{13}) \text{ and } (1, n_2, n_3) = (1, 4, 3)$$

Application to $r = 13$

By the recipe we obtain Frey curves with models given by $E_{(a,b)} : y^2 = x^3 + a_4(a,b)x + a_6(a,b)$, where $w^2 = 13$ and

$$
\begin{aligned}
a_4(a,b) &= (216w - 2808)a^4 + (-1728w + 5616)a^3b \\
&\quad +(1728w - 11232)a^2b^2 + (-1728w + 5616)ab^3 \\
&\quad +(216w - 2808)b^4
\end{aligned}
$$

$$
\begin{aligned}
a_6(a,b) &= (-8640w + 44928)a^6 + (49248w - 235872)a^5b \\
&\quad +(-129600w + 471744)a^4b^2 + (152928w \\
&\quad -662688)a^3b^3 + (-129600w + 471744)a^2b^4 \\
&\quad +(49248w - 235872)ab^5 + \\
&\quad +(-8640w + 44928)b^6 + (50193w + 182520)b^6,
\end{aligned}
$$

Application to $r = 13$

Proposition

The conductor of $E_{(a,b)}$ is given by $N_E = 2^s (w)^2 \mathrm{rad}(c)$, where $w^2 = 13$ and $s = 3, 4$. In particular, E has good red. at all $v \mid 3$.

Theorem

The Frey curves $E_{(a,b)}/\mathbb{Q}(\sqrt{13})$ are modular.

Proof: $\mathbb{Q}(\sqrt{13})$ is a totally real and abelian. 3 splits in $\mathbb{Q}(\sqrt{13})$ and all the primes above 3 are of good reduction.

Theorem

Let $p > 97$ and $(a, b) = 1$. Then, the representations $\bar{\rho}_{E,p} : G_{\mathbb{Q}(\sqrt{13})} \to GL_2(\mathbb{F}_p)$ attached to the Frey curves $E_{(a,b)}$ are abs. irreducible.

Application to $r = 13$

Now let p be the exponent in $x^{13} + y^{13} = Cz^p$.

Theorem (Level Lowering)

There is an Hilbert newform f defined over $\mathbb{Q}(\sqrt{13})$ of level $2^s w^2$ and parallel weight 2 such that $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}$ for some $\mathfrak{P} \mid p$.

Let $L \nmid N_E$ be a prime. From $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}$ it follows that

$$a_L(E) \equiv a_L(f) \pmod{\mathfrak{P}},$$

where $f \in S_2(2^s w^2)$ for $s = 3, 4$.

We want to contradict the previous congruence!!

We divide the newforms into 2 sets:

- S1: Newforms such that $\mathbb{Q}_f = \mathbb{Q}$.
- S2: Newforms such that $\mathbb{Q}_f$ strictly contains $\mathbb{Q}$ ($p > 4992539$).

On one hand, with the help of John Voight we obtained a list of about 170 newforms in S1, as an example:

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
1	1	3	3	1	1	-6	3	3	-13	-21
3	-1	-7	1	-2	-2	7	0	-8	-1	-6
3	-1	7	-1	2	2	-7	0	-8	1	6
-3	-3	-3	-3	-1	-1	6	-1	-1	13	-3
-3	-3	3	3	1	1	-6	-1	-1	-13	3
-3	-1	-7	-7	-3	-1	-6	-7	9	1	9
-3	-1	-7	1	-2	2	-7	0	8	-1	-6
-3	-1	7	-1	2	-2	7	0	8	1	6
-1	-1	-5	7	-5	3	6	-1	-5	-1	3
-1	-1	-3	-7	-7	1	2	3	7	1	-3

On the other hand, we used SAGE to go through all the possible residual elliptic curves for pairs $(a, b) \in \mathbb{F}_\ell \times \mathbb{F}_\ell$ and compute the possible values for $a_L(E)$:

$$\begin{cases} a_{L_3^0} \in \{-3, -1\}, \\ a_{L_3^1} \in \{-3, -1, 1\}, \\ a_{L_5} \in \{-6, -2, 2\}, \\ a_{L_7} \in \{11, -11, -1, -5\}, \\ a_{L_{11}} \in \{-15, 3, 5, -7, 9, -1, 15\}, \\ a_{L_{17}^0} \in \{1, 3, 5, 7, -3, -1\}, \\ a_{L_{17}^1} \in \{3, 5, 7, -7, -5, -3\}, \\ a_{L_{23}^0} \in \{1, 3, 5, 7, -9, -7, -5, -3\}, \\ a_{L_{23}^1} \in \{1, 3, 7, -9, -3, -1\}, \\ a_{L_{29}^0} \in \{1, 3, 5, -9, -7, -5, -3, -1\}, \\ a_{L_{29}^1} \in \{1, 3, 5, 9, -9, -7, -5, -3, -1\} \end{cases}$$

Application to $r = 13$

For example, let f be such that $a_{L_5}(f) = -9$ and recall that

$$a_{L_5}(E) \in \{-6, -2, 2\}.$$

Easily we see that for $p > 11$ we have a contradiction with

$$-9 \equiv -6, -2, 2 \pmod{p}.$$

Going through all the computed newforms and using several primes we eliminate all except 4.

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
-1	1	7	3	1	7	2	-7	-3	-1	3
-1	1	3	7	-7	-1	2	-3	-7	-1	3
-1	-3	-1	-5	5	-9	-6	-3	1	-5	15
-3	-1	1	-3	-3	-9	-2	-7	5	-11	-15

These newforms correspond to $E_{(1,0)}$, $E_{(1,1)}$, $E_{(1,-1)}$ and $E_{(1,1)}$ twisted by -1.

For example, let f be such that $a_{L_5}(f) = -9$ and recall that

$$a_{L_5}(E) \in \{-6, -2, 2\}.$$

Easily we see that for $p > 11$ we have a contradiction with

$$-9 \equiv -6, -2, 2 \pmod{p}.$$

Going through all the computed newforms and using several primes we eliminate all except 4.

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
-1	1	7	3	1	7	2	-7	-3	-1	3
-1	1	3	7	-7	-1	2	-3	-7	-1	3
-1	-3	-1	-5	5	-9	-6	-3	1	-5	15
-3	-1	1	-3	-3	-9	-2	-7	5	-11	-15

These newforms correspond to $E_{(1,0)}$, $E_{(1,1)}$, $E_{(1,-1)}$ and $E_{(1,1)}$ twisted by -1.

Application to $r = 13$

We will now deal with the last 4 newforms. Recall that

$$d\gamma \mid a + b \quad \text{and } d = 3, 5, 7, 11$$

Using SAGE we go through all the possible non-zero pairs $(a, b) \in \mathbb{F}_d \times \mathbb{F}_d$ satisfying $a + b \equiv 0 \pmod{d}$ and we computed the possible values for $a_{L_d}(E)$ to get

$$\begin{aligned}
\text{if } d = 3 \quad & \text{then} \quad a_{L_3^0} = -3 \text{ and } a_{L_3^1} = -1 \\
\text{if } d = 5 \quad & \text{then} \quad a_{L_5} = -2 \\
\text{if } d = 7 \quad & \text{then} \quad a_{L_7} = -11 \\
\text{if } d = 11 \quad & \text{then} \quad a_{L_{11}} = -15
\end{aligned}$$

These conditions allow to eliminate the newforms attached to $E_{(1,0)}$, $E_{(1,1)}$ and $E_{(1,1)}$ twisted by -1.
We are left to eliminate the newform g corresponding to the fourth row.

Proposition

Let $\mathfrak{P}_{13}$ be the prime in K^+ above 13. The conductor of the curve $E_{(a,b)}/K^+$ satisfies $\upsilon_{\mathfrak{P}_{13}}(N_E) = 0$ or $\upsilon_{\mathfrak{P}_{13}}(N_E) = 2$ if $13 \mid a+b$ or $13 \nmid a+b$, respectively.

- The surviving newform g corresponds to $E_{(1,-1)}$.
- From the proposition the conductor at $\mathfrak{P}_{13}$ of $\rho_{g,p}|G_{K^+}$ is $\mathfrak{P}_{13}^0$
- Assume now that $13 \nmid a+b$ (is equivalent to $13 \nmid c$)
- From the proposition the conductor at $\mathfrak{P}_{13}$ of $\rho_{E,p}|G_{K^+}$ is $\mathfrak{P}_{13}^2$
- The conductors of the reductions modulo p will also have different conductors at $\mathfrak{P}_{13}$ since p is big.
- Thus $\bar{\rho}_{E,p} \sim \bar{\rho}_{g,\mathfrak{P}}$ can not hold.

Application to $r = 13$

Proposition

Let $\mathfrak{P}_{13}$ be the prime in K^+ above 13. The conductor of the curve $E_{(a,b)}/K^+$ satisfies $\upsilon_{\mathfrak{P}_{13}}(N_E) = 0$ or $\upsilon_{\mathfrak{P}_{13}}(N_E) = 2$ if $13 \mid a+b$ or $13 \nmid a+b$, respectively.

- The surviving newform g corresponds to $E_{(1,-1)}$.
- From the proposition the conductor at $\mathfrak{P}_{13}$ of $\rho_{g,p}|G_{K^+}$ is $\mathfrak{P}_{13}^0$
- Assume now that $13 \nmid a+b$ (is equivalent to $13 \nmid c$)
- From the proposition the conductor at $\mathfrak{P}_{13}$ of $\rho_{E,p}|G_{K^+}$ is $\mathfrak{P}_{13}^2$
- The conductors of the reductions modulo p will also have different conductors at $\mathfrak{P}_{13}$ since p is big.
- Thus $\bar{\rho}_{E,p} \sim \bar{\rho}_{g,\mathfrak{P}}$ can not hold.

Application to $r = 13$

Proposition

Let $\mathfrak{P}_{13}$ be the prime in K^+ above 13. The conductor of the curve $E_{(a,b)}/K^+$ satisfies $\upsilon_{\mathfrak{P}_{13}}(N_E) = 0$ or $\upsilon_{\mathfrak{P}_{13}}(N_E) = 2$ if $13 \mid a+b$ or $13 \nmid a+b$, respectively.

- The surviving newform g corresponds to $E_{(1,-1)}$.
- From the proposition the conductor at $\mathfrak{P}_{13}$ of $\rho_{g,p}|G_{K^+}$ is $\mathfrak{P}_{13}^0$
- Assume now that $13 \nmid a+b$ (is equivalent to $13 \nmid c$)
- From the proposition the conductor at $\mathfrak{P}_{13}$ of $\rho_{E,p}|G_{K^+}$ is $\mathfrak{P}_{13}^2$
- The conductors of the reductions modulo p will also have different conductors at $\mathfrak{P}_{13}$ since p is big.
- Thus $\bar{\rho}_{E,p} \sim \bar{\rho}_{g,\mathfrak{P}}$ can not hold.

Application to $r = 7$

Theorem (Chap. 4)

Let $d = 2^{s_0}3^{s_1}5^{s_2}$ and γ be an integer divisible only by primes $\ell \not\equiv 1, 0 \pmod 7$. Then, if $p \geq 17$ we have that

(*A*) The equation $x^7 + y^7 = d\gamma z^p$ has no non-trivial primitive solutions such that $7 \nmid c$ if (s_0, s_1, s_2) satisfies any of the following three conditions $(\geq 2, \geq 0, \geq 0)$, $(= 1, \geq 1, \geq 0)$ or $(= 0, \geq 0, \geq 1)$.

(*B*) The equation $x^{14} + y^{14} = d\gamma z^p$ has no non-trivial primitive solutions if $s_1 > 0$ or $s_2 > 0$ or $s_0 \geq 2$.

Conclusions

In summary, we generalized some aspects of the modular approach and used it to study some equations of signature (r, r, p) for $r \geq 5$. In particular, we

- Solved equations of signature $(5, 5, p)$ via multi-Frey technique using two $\mathbb{Q}$-curves.
- Constructed Frey curves over totally real fields to equations of signature (r, r, p) for all primes $r \geq 7$.
- Used them to apply the modular approach via classic newforms for signature $(7, 7, p)$
- Proved modularity and irreducibility statements for some elliptic curves over totally real abelian number fields.
- Used them to apply the modular approach via Hilbert newforms over $\mathbb{Q}(\sqrt{13})$ for signature $(13, 13, p)$
- Constructed two extra Frey curves when $r = 4m + 1$

Contributions

This thesis resulted in the following papers that can be found at arxiv.org

- N. Freitas: 'Recipes for Fermat-type equations of the form $x^r + y^r = Cz^p$', preprint.
- L. Dieulefait, N. Freitas: 'Fermat-type equations of signature $(13, 13, p)$ via Hilbert cuspforms', submitted.
- L. Dieulefait, N. Freitas: 'The Fermat-type equations $x^5 + y^5 = 2z^p$ or $3z^p$ solved through $\mathbb{Q}$-curves', to appear in Mathematics of Computation.