On Darmon's program for the generalized Fermat equation of signature (r, r, p)

with Imin Chen, Luis Dieulefait, and Nuno Freitas

Nicolas Billerey

Laboratoire de Mathématiques Blaise Pascal
Université Clermont Auvergne

Rational Points on Modular Curves (ICTS, Bengaluru)
September 22, 2023

Table of contents

Table of contents

Main steps in the proof of Fermat's last theorem

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

[STEP 1/5 – CONSTRUCTION] (Hellegouarch, Frey)

- Consider
$$E : y^2 = x(x - a^p)(x + b^p).$$
The discriminant $\Delta = 2^4(abc)^{2p}$ of this model is non-zero, and hence it defines an elliptic curve over $\mathbf{Q}$ (with full 2-torsion).
- There is a 2-dimensional mod p representation attached to E
$$\overline{\rho}_{E,p} : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p)$$
given by the action of $G_{\mathbf{Q}}$ on the group of p-torsion points on E.
- The representation $\overline{\rho}_{E,p}$ is unramified away from $\{2, p\}$ (Tate).

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

[STEP 2/5 – MODULARITY] (Wiles)

- Without loss of generality, assume from now on that

$$a^p \equiv -1 \pmod 4 \quad \text{and} \quad b^p \equiv 0 \pmod{16}.$$

  Hence the curve E is semistable (at 2).
- Since $E/\mathbf{Q}$ is semistable, the elliptic curve $E/\mathbf{Q}$ is **modular**.
- Moreover, $\overline{\rho}_{E,p}$ has weight 2 in the sense of Edixhoven (or Serre) and Serre's conductor $N(\overline{\rho}_{E,p}) = 2$.

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

[STEP 3/5 – IRREDUCIBILITY] (Mazur)

- Since E has full 2-torsion over $\mathbf{Q}$ and is semistable, the representation

$$\overline{\rho}_{E,p} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$$

is **(absolutely) irreducible**.

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

[STEP 3/5 – IRREDUCIBILITY] (Mazur)

- Since E has full 2-torsion over $\mathbf{Q}$ and is semistable, the representation
$$\overline{\rho}_{E,p} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$$
is **(absolutely) irreducible**.

Sketch of proof. Assume for a contradiction that $\overline{\rho}_{E,p}$ is reducible.

- Write D for a rational subgroup of order p and $\chi : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$ for the corresponding isogeny character.
- Since E is semistable, either $\chi = \chi_p$ (mod p cyc.) or χ is trivial (Serre).
- In the latter case, the curve E has a rational point of order p, and hence $\#E(\mathbf{Q})_{\text{tors}} \geq 4p \geq 20$, contradicting Mazur's theorem on torsion.
- In the former case, the elliptic curve $E' = E/D$ has a rational point of order p and we conclude as before.

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

[STEP 4/5 – LEVEL LOWERING] (Ribet)

- Since $E/\mathbf{Q}$ is modular and the representation $\overline{\rho}_{E,p}$ is absolutely irreducible, it **arises from** a newform of weight 2 and level $N(\overline{\rho}_{E,p}) = 2$ (with trivial character).

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

[Step 4/5 – Level lowering] (Ribet)

- Since $E/\mathbf{Q}$ is modular and the representation $\overline{\rho}_{E,p}$ is absolutely irreducible, it **arises from** a newform of weight 2 and level $N(\overline{\rho}_{E,p}) = 2$ (with trivial character).

Definition ('arises from')

We say that $\overline{\rho}_{E,p}$ arises from a newform f (of weight 2 and level N) if

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

where $\overline{\rho}_{f,p}$ is the mod p Galois representation associated with f.

Main steps in the proof of Fermat's last theorem

Let $p \geq 5$ be a prime. Assume for a contradiction that there exist non-zero coprime integers a, b, c such that $a^p + b^p = c^p$.

[Step 5/5 – Contradiction]

- For every newform g of weight 2 and level 2, the representation $\overline{\rho}_{E,p}$ does **not** arise from g.

The five steps in the modular method

1. Construction
2. Modularity
3. Irreducibility
4. Level lowering
5. Contradiction

The five steps in the modular method

1. Construction
2. Modularity
3. Irreducibility
4. Level lowering
5. Contradiction

The five steps in the modular method

1. Construction
2. Modularity
3. Irreducibility
4. Level lowering
5. Contradiction

Table of contents

Our Diophantine problem

We wish to extend the modular method to deal with generalized Fermat equations

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

where A, B, C are fixed non-zero coprime integers and p, q, r are non-negative integers.

In this talk, we restrict ourselves to the case of

$$x^r + y^r = Cz^p$$

where $r \geq 3$ is a **fixed prime**, C is a fixed positive integer and p is a prime which is allowed to vary.

Our Diophantine problem

We wish to extend the modular method to deal with generalized Fermat equations

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

where A, B, C are fixed non-zero coprime integers and p, q, r are non-negative integers.

In this talk, we restrict ourselves to the case of

$$x^r + y^r = Cz^p$$

where $r \geq 3$ is a **fixed prime**, C is a fixed positive integer and p is a prime which is allowed to vary.

Notation

$r \geq 3$ prime number

ζ_r primitive r-th root of unity

$\omega_i = \zeta_r^i + \zeta_r^{-i}$, for every $i \geq 0$

$$h(X) = \prod_{i=1}^{(r-1)/2} (X - \omega_i) \in \mathbf{Z}[X]$$

$K = \mathbf{Q}(\zeta_r)^+ = \mathbf{Q}(\omega_1)$ maximal totally real subfield of $\mathbf{Q}(\zeta_r)$

$\mathcal{O}_K$ integer ring of K

$\mathfrak{p}_r$ unique prime ideal above r in $\mathcal{O}_K$ (totally ramified)

Step 1 – Kraus' Frey hyperelliptic curve

Let a, b be non-zero coprime integers such that $a^r + b^r \neq 0$.

$$C_r(a,b) : y^2 = (ab)^{\frac{r-1}{2}} xh\left(\frac{x^2}{2} + ab\right) + b^r - a^r.$$

The discriminant of this model is

$$\Delta_r(a,b) = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r (a^r + b^r)^{r-1}.$$

In particular, it defines a hyperelliptic curve of genus $\frac{r-1}{2}$.

Examples

$$r = 3 : \quad y^2 = x^3 + 3abx + b^3 - a^3$$
$$r = 5 : \quad y^2 = x^5 + 5abx^3 + 5a^2b^2x + b^5 - a^5$$
$$r = 7 : \quad y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7.$$

Step 1 – Kraus' Frey hyperelliptic curve

Let a, b be non-zero coprime integers such that $a^r + b^r \neq 0$.

$$C_r(a,b) : y^2 = (ab)^{\frac{r-1}{2}} x h\left(\frac{x^2}{2} + ab\right) + b^r - a^r.$$

The discriminant of this model is

$$\Delta_r(a,b) = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r (a^r + b^r)^{r-1}.$$

In particular, it defines a hyperelliptic curve of genus $\frac{r-1}{2}$.

Examples

$$r = 3 : \quad y^2 = x^3 + 3abx + b^3 - a^3$$
$$r = 5 : \quad y^2 = x^5 + 5abx^3 + 5a^2b^2x + b^5 - a^5$$
$$r = 7 : \quad y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7.$$

Step 1 – Kraus' Frey hyperelliptic curve

Let a, b be non-zero coprime integers such that $a^r + b^r \neq 0$.

$$C_r(a,b) : y^2 = (ab)^{\frac{r-1}{2}} xh\left(\frac{x^2}{2} + ab\right) + b^r - a^r.$$

The discriminant of this model is

$$\Delta_r(a,b) = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r (a^r + b^r)^{r-1}.$$

In particular, it defines a hyperelliptic curve of genus $\frac{r-1}{2}$.

Examples

$$r = 3: \quad y^2 = x^3 + 3abx + b^3 - a^3$$
$$r = 5: \quad y^2 = x^5 + 5abx^3 + 5a^2b^2x + b^5 - a^5$$
$$r = 7: \quad y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7.$$

Step 1 – Frey representations

For a field M of characteristic 0, write $G_M = \mathrm{Gal}(\overline{M}/M)$ for its absolute Galois group.

Definition (Darmon)

A **Frey representation** of signature $(r, q, p) \in (\mathbf{Z}_{>0})^3$ over a number field L in characteristic $\ell > 0$ is a Galois representation

$$\overline{\rho} = \overline{\rho}(t) : G_{L(t)} \to \mathrm{GL}_2(\mathbf{F})$$

where $\mathbf{F}$ finite field of characteristic ℓ such that the following conditions hold.

1. The restriction of $\overline{\rho}$ to $G_{\overline{L}(t)}$ has trivial determinant and is irreducible.
2. The projectivization $\overline{\rho}^{\mathrm{geom}} : G_{\overline{L}(t)} \to \mathrm{PSL}_2(\mathbf{F})$ of this representation is unramified outside $\{0, 1, \infty\}$.
3. It maps the inertia groups at 0, 1, and ∞ to subgroups of $\mathrm{PSL}_2(\mathbf{F})$ of order r, q, and p respectively.

Step 1 – Frey representations

For a field M of characteristic 0, write $G_M = \mathrm{Gal}(\overline{M}/M)$ for its absolute Galois group.

Definition (Darmon)

A **Frey representation** of signature $(r, q, p) \in (\mathbf{Z}_{>0})^3$ over a number field L in characteristic $\ell > 0$ is a Galois representation

$$\overline{\rho} = \overline{\rho}(t) : G_{L(t)} \to \mathrm{GL}_2(\mathbf{F})$$

where $\mathbf{F}$ finite field of characteristic ℓ such that the following conditions hold.

1. The restriction of $\overline{\rho}$ to $G_{\overline{L}(t)}$ has trivial determinant and is irreducible.
2. The projectivization $\overline{\rho}^{\mathrm{geom}} : G_{\overline{L}(t)} \to \mathrm{PSL}_2(\mathbf{F})$ of this representation is unramified outside $\{0, 1, \infty\}$.
3. It maps the inertia groups at 0, 1, and ∞ to subgroups of $\mathrm{PSL}_2(\mathbf{F})$ of order r, q, and p respectively.

Step 1 – Hecke–Darmon's classification theorem

Let p be a prime number.

Theorem (Hecke–Darmon)

Up to equivalence, there is only one Frey representation of signature (p, p, p). It occurs over $\mathbf{Q}$ in characteristic p and is associated with the Legendre family

$$L(t) : y^2 = x(x-1)(x-t).$$

The classical Frey–Hellegouarch curve

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

is obtained from $L(t)$ after **specialization** at $t_0 = \frac{a^p}{a^p+b^p}$ and **quadratic twist** by $-(a^p + b^p)$.

Step 1 – Hecke–Darmon's classification theorem

Let p be a prime number.

Theorem (Hecke–Darmon)

Up to equivalence, there is only one Frey representation of signature (p, p, p). It occurs over $\mathbf{Q}$ in characteristic p and is associated with the Legendre family

$$L(t) : y^2 = x(x-1)(x-t).$$

The classical Frey–Hellegouarch curve

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

is obtained from $L(t)$ after **specialization** at $t_0 = \frac{a^p}{a^p+b^p}$ and **quadratic twist** by $-(a^p+b^p)$.

Step 1 – Abelian varieties of GL_2-type

Definition

Let A be an abelian variety over a field L of characteristic 0. We say that A/L is of GL_2-type (or $\mathrm{GL}_2(F)$-type) if there is an embedding $F \hookrightarrow \mathrm{End}_L(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ where F is a number field with $[F : \mathbf{Q}] = \dim A$.

Let A/L be an abelian variety of $\mathrm{GL}_2(F)$-type.

- For each prime ideal $\lambda \mid \ell$ in F, there is a linear action of G_L on $V_\lambda(A) := V_\ell(A) \otimes_{F \otimes \mathbf{Q}_\ell} F_\lambda$ which gives rise to a λ-adic representation

$$\rho_{A,\lambda} : G_L \longrightarrow \mathrm{Aut}_{F_\lambda}(V_\lambda(A)) \simeq \mathrm{GL}_2(F_\lambda).$$

- The representations $\{\rho_{A,\lambda}\}_\lambda$ form a strictly compatible system of F-integral representations.
- For each prime ideal $\lambda \mid \ell$ in F, we have a residual representation

$$\overline{\rho}_{A,\lambda} : G_L \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda),$$

with values in the residue field $\mathbf{F}_\lambda$ of F_λ.

Step 1 – Abelian varieties of GL_2-type

Definition

Let A be an abelian variety over a field L of characteristic 0. We say that A/L is of GL_2-type (or $\mathrm{GL}_2(F)$-type) if there is an embedding $F \hookrightarrow \mathrm{End}_L(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ where F is a number field with $[F : \mathbf{Q}] = \dim A$.

Let A/L be an abelian variety of $\mathrm{GL}_2(F)$-type.

- For each prime ideal $\lambda \mid \ell$ in F, there is a linear action of G_L on $V_\lambda(A) := V_\ell(A) \otimes_{F \otimes \mathbf{Q}_\ell} F_\lambda$ which gives rise to a λ-adic representation

$$\rho_{A,\lambda} : G_L \longrightarrow \mathrm{Aut}_{F_\lambda}(V_\lambda(A)) \simeq \mathrm{GL}_2(F_\lambda).$$

- The representations $\{\rho_{A,\lambda}\}_\lambda$ form a strictly compatible system of F-integral representations.
- For each prime ideal $\lambda \mid \ell$ in F, we have a residual representation

$$\overline{\rho}_{A,\lambda} : G_L \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda),$$

with values in the residue field $\mathbf{F}_\lambda$ of F_λ.

Step 1 – Abelian varieties of GL_2-type

Definition

Let A be an abelian variety over a field L of characteristic 0. We say that A/L is of GL_2-type (or $\mathrm{GL}_2(F)$-type) if there is an embedding $F \hookrightarrow \mathrm{End}_L(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ where F is a number field with $[F : \mathbf{Q}] = \dim A$.

Let A/L be an abelian variety of $\mathrm{GL}_2(F)$-type.

- For each prime ideal $\lambda \mid \ell$ in F, there is a linear action of G_L on $V_\lambda(A) := V_\ell(A) \otimes_{F \otimes \mathbf{Q}_\ell} F_\lambda$ which gives rise to a λ-adic representation

$$\rho_{A,\lambda} : G_L \longrightarrow \mathrm{Aut}_{F_\lambda}(V_\lambda(A)) \simeq \mathrm{GL}_2(F_\lambda).$$

- The representations $\{\rho_{A,\lambda}\}_\lambda$ form a strictly compatible system of F-integral representations.
- For each prime ideal $\lambda \mid \ell$ in F, we have a residual representation

$$\overline{\rho}_{A,\lambda} : G_L \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda),$$

with values in the residue field $\mathbf{F}_\lambda$ of F_λ.

Step 1 – Abelian varieties of GL_2-type

Definition

Let A be an abelian variety over a field L of characteristic 0. We say that A/L is of GL_2-type (or $\mathrm{GL}_2(F)$-type) if there is an embedding $F \hookrightarrow \mathrm{End}_L(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ where F is a number field with $[F : \mathbf{Q}] = \dim A$.

Let A/L be an abelian variety of $\mathrm{GL}_2(F)$-type.

- For each prime ideal $\lambda \mid \ell$ in F, there is a linear action of G_L on $V_\lambda(A) := V_\ell(A) \otimes_{F \otimes \mathbf{Q}_\ell} F_\lambda$ which gives rise to a λ-adic representation

$$\rho_{A,\lambda} : G_L \longrightarrow \mathrm{Aut}_{F_\lambda}(V_\lambda(A)) \simeq \mathrm{GL}_2(F_\lambda).$$

- The representations $\{\rho_{A,\lambda}\}_\lambda$ form a strictly compatible system of F-integral representations.
- For each prime ideal $\lambda \mid \ell$ in F, we have a residual representation

$$\overline{\rho}_{A,\lambda} : G_L \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda),$$

with values in the residue field $\mathbf{F}_\lambda$ of F_λ.

Step 1 – Frey representations in signature (r, r, p)

Theorem

There exists a hyperelliptic curve $C'_r(t)$ over $K(t)$ of genus $\frac{r-1}{2}$ such that $J'_r(t) = \mathrm{Jac}(C'_r(t))$ satisfies:

1. It is of $\mathrm{GL}_2(K)$-type, i.e. $K \hookrightarrow \mathrm{End}_{K(t)}(J'_r(t)) \otimes \mathbf{Q}$
2. For every $t_0 \in K$, the embedding $K \hookrightarrow \mathrm{End}_K(J'_r(t_0)) \otimes \mathbf{Q}$ is well-defined;
3. For every prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ above a rational prime p,

$$\overline{\rho}_{J'_r(t),\mathfrak{p}} : G_{K(t)} \to \mathrm{GL}_2(\mathcal{O}_K/\mathfrak{p})$$

   is a Frey representation of signature (r, r, p).

Moreover, $C_r(a,b)/K$ is obtained from $C'_r(t)$ after **specialization** at $t_0 = \frac{a^r}{a^r+b^r}$ and **quadratic twist** by $-\frac{(ab)^{\frac{r-1}{2}}}{a^r+b^r}$.

➥ The proof uses Darmon's construction of Frey representations of signature (p, p, r).

Step 1 – Frey representations in signature (r, r, p)

Theorem

There exists a hyperelliptic curve $C'_r(t)$ over $K(t)$ of genus $\frac{r-1}{2}$ such that $J'_r(t) = \mathrm{Jac}(C'_r(t))$ satisfies:

1. It is of $\mathrm{GL}_2(K)$-type, i.e. $K \hookrightarrow \mathrm{End}_{K(t)}(J'_r(t)) \otimes \mathbf{Q}$
2. For every $t_0 \in K$, the embedding $K \hookrightarrow \mathrm{End}_K(J'_r(t_0)) \otimes \mathbf{Q}$ is well-defined;
3. For every prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ above a rational prime p,

$$\overline{\rho}_{J'_r(t),\mathfrak{p}} : G_{K(t)} \to \mathrm{GL}_2(\mathcal{O}_K/\mathfrak{p})$$

   is a Frey representation of signature (r, r, p).

Moreover, $C_r(a, b)/K$ is obtained from $C'_r(t)$ after **specialization** at $t_0 = \frac{a^r}{a^r+b^r}$ and **quadratic twist** by $-\frac{(ab)^{\frac{r-1}{2}}}{a^r+b^r}$.

➥ The proof uses Darmon's construction of Frey representations of signature (p, p, r).

Step 1 – Frey representations in signature (r, r, p)

Theorem

There exists a hyperelliptic curve $C'_r(t)$ over $K(t)$ of genus $\frac{r-1}{2}$ such that $J'_r(t) = \mathrm{Jac}(C'_r(t))$ satisfies:

1. It is of $\mathrm{GL}_2(K)$-type, i.e. $K \hookrightarrow \mathrm{End}_{K(t)}(J'_r(t)) \otimes \mathbf{Q}$
2. For every $t_0 \in K$, the embedding $K \hookrightarrow \mathrm{End}_K(J'_r(t_0)) \otimes \mathbf{Q}$ is well-defined;
3. For every prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ above a rational prime p,

$$\overline{\rho}_{J'_r(t),\mathfrak{p}} : G_{K(t)} \to \mathrm{GL}_2(\mathcal{O}_K/\mathfrak{p})$$

   is a Frey representation of signature (r, r, p).

Moreover, $C_r(a, b)/K$ is obtained from $C'_r(t)$ after **specialization** at $t_0 = \frac{a^r}{a^r+b^r}$ and **quadratic twist** by $-\frac{(ab)^{\frac{r-1}{2}}}{a^r+b^r}$.

➥ The proof uses Darmon's construction of Frey representations of signature (p, p, r).

Step 1 – Two-dimensional $\mathfrak{p}$-adic and mod $\mathfrak{p}$ representations

Write $J_r = \mathrm{Jac}(C_r(a,b))/K$ for the Jacobian of $C_r(a,b)$ base changed to K.

- There is a compatible system of K-rational Galois representations

$$\rho_{J_r,\mathfrak{p}} : G_K \to \mathrm{GL}_2(K_\mathfrak{p})$$

  indexed by the prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ associated with J_r.
- For $\mathfrak{p} = \mathfrak{p}_r$, the residual representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$ arises after **specialization** and **twisting** from a Frey representation of signature (r,r,r).

Step 1 – Two-dimensional $\mathfrak{p}$-adic and mod $\mathfrak{p}$ representations

Write $J_r = \mathrm{Jac}(C_r(a,b))/K$ for the Jacobian of $C_r(a,b)$ base changed to K.

- There is a compatible system of K-rational Galois representations

$$\rho_{J_r,\mathfrak{p}} : G_K \to \mathrm{GL}_2(K_\mathfrak{p})$$

  indexed by the prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ associated with J_r.
- For $\mathfrak{p} = \mathfrak{p}_r$, the residual representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$ arises after **specialization** and **twisting** from a Frey representation of signature (r,r,r).

Step 1 – Two-dimensional $\mathfrak{p}$-adic and mod $\mathfrak{p}$ representations

Write $J_r = \mathrm{Jac}(C_r(a,b))/K$ for the Jacobian of $C_r(a,b)$ base changed to K.

- There is a compatible system of K-rational Galois representations

$$\rho_{J_r,\mathfrak{p}} : G_K \to \mathrm{GL}_2(K_\mathfrak{p})$$

  indexed by the prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ associated with J_r.
- For $\mathfrak{p} = \mathfrak{p}_r$, the residual representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$ arises after **specialization** and **twisting** from a Frey representation of signature (r,r,r).

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x - a^r)(x + b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^{\times}$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x - a^r)(x + b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x-a^r)(x+b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x - a^r)(x + b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x - a^r)(x + b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x-a^r)(x+b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x-a^r)(x+b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x - a^r)(x + b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – The representation $\overline{\rho}_{J_r,\mathfrak{p}_r}$

Theorem

Assume $r \geq 5$. The representation $\overline{\rho}_{J_r,\mathfrak{p}_r} : G_K \to \mathrm{GL}_2(\mathbf{F}_r)$ is absolutely irreducible when restricted to $G_{\mathbf{Q}(\zeta_r)}$.

Sketch of proof. For simplicity, assume $r = 11$ or $r \geq 17$.

- By Hecke–Darmon's classification theorem we have $\overline{\rho}_{J_r,\mathfrak{p}_r} \simeq \overline{\rho}_{L,r} \otimes \chi$ where $\chi : G_K \to \overline{\mathbf{F}}_r^\times$ and $L = L(t_0)$, with $t_0 = \frac{a^r}{a^r+b^r}$.
- Since $\det \overline{\rho}_{L,r} = \chi_r$, we have $\overline{\rho}_{L,r}(G_{\mathbf{Q}(\zeta_r)}) = \overline{\rho}_{L,r}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{F}_r)$.
- The elliptic curve L is a quadratic twist of $L' : y^2 = x(x - a^r)(x + b^r)$ which has semistable reduction at r.
- If $\overline{\rho}_{L',r}(G_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{F}_r)$, then $\overline{\rho}_{L',r}(G_{\mathbf{Q}})$ is either contained in a Borel subgroup or in the normalizer of a Cartan subgroup (Serre).
- In the former case, we get a rational point on $Y_0(2r)$ and a contradiction (Mazur, Kenku).
- In the latter case, it follows from results of Mazur, Momose, Merel (split Cartan case) and Darmon, Merel, Lemos (non split Cartan case) that $j(L) = j(L') \in \mathbf{Z}$ and we conclude from this.

Step 2 – Modularity of J_r/K

Serre's modularity conjecture (Khare–Wintenberger, Dieulefait) and a recent modularity lifting theorem (Khare–Thorne) then give the following.

Corollary

The abelian variety J_r/K is modular (for any prime $r \geq 3$).

Step 2 – Modularity of J_r/K

Serre's modularity conjecture (Khare–Wintenberger, Dieulefait) and a recent modularity lifting theorem (Khare–Thorne) then give the following.

Corollary

The abelian variety J_r/K is modular (for any prime $r \geq 3$).

Step 3– Irreducibility

Theorem

Assume a and b satisfy

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 1 \pmod 4.$$

Assume further that $r \nmid \#\mathbf{F}_{\mathfrak{q}_2}^{\times}$ where $\mathfrak{q}_2$ is a prime ideal above 2 in $K = \mathbf{Q}(\zeta_r)^+$.
Then, for all primes $p \neq 2$ and all prime ideals $\mathfrak{p} \mid p$ in K the representation $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible.

- Under these two assumptions the representation $\overline{\rho}_{J_r,\mathfrak{p}}$ is irreducible locally at 2.
- There are several other situations where we can prove irreducibility (e.g, $r = 7$).
- We do not know how to prove it in general though.

Step 3– Irreducibility

Theorem

Assume a and b satisfy

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 1 \pmod 4.$$

Assume further that $r \nmid \#\mathbf{F}_{\mathfrak{q}_2}^{\times}$ where $\mathfrak{q}_2$ is a prime ideal above 2 in $K = \mathbf{Q}(\zeta_r)^+$.
Then, for all primes $p \neq 2$ and all prime ideals $\mathfrak{p} \mid p$ in K the representation $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible.

- Under these two assumptions the representation $\overline{\rho}_{J_r,\mathfrak{p}}$ is irreducible locally at 2.
- There are several other situations where we can prove irreducibility (e.g, $r = 7$).
- We do not know how to prove it in general though.

Step 4 – Refined level lowering

Finally assume that there exists a non-zero integer c such that $a^r + b^r = Cc^p$ for some fixed positive integer C and that we have

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 1 \pmod 4.$$

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ above the rational prime p.

Theorem

Suppose that $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible. Then, there is a Hilbert newform g over K of parallel weight 2, trivial character and level $2^2\mathfrak{p}_r^2\mathfrak{n}'$ such that

$$\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$$

for some prime ideal $\mathfrak{P} \mid p$ in the coefficient field K_g of g.
Here, $\mathfrak{n}'$ denotes the product of prime ideals coprime to $2r$ dividing C.
Moreover, we have $K \subset K_g$.

- Refined level lowering theorem of Breuil–Diamond.
- Precise description of the image of inertia, notably at prime ideals above 2 in K.

Step 4 – Refined level lowering

Finally assume that there exists a non-zero integer c such that $a^r + b^r = Cc^p$ for some fixed positive integer C and that we have

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 1 \pmod 4.$$

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ above the rational prime p.

Theorem

Suppose that $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible. Then, there is a Hilbert newform g over K of parallel weight 2, trivial character and level $2^2\mathfrak{p}_r^2\mathfrak{n}'$ such that

$$\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$$

for some prime ideal $\mathfrak{P} \mid p$ in the coefficient field K_g of g.
Here, $\mathfrak{n}'$ denotes the product of prime ideals coprime to $2r$ dividing C.
Moreover, we have $K \subset K_g$.

- Refined level lowering theorem of Breuil–Diamond.
- Precise description of the image of inertia, notably at prime ideals above 2 in K.

Step 4 – Refined level lowering

Finally assume that there exists a non-zero integer c such that $a^r + b^r = Cc^p$ for some fixed positive integer C and that we have

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 1 \pmod 4.$$

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ above the rational prime p.

Theorem

Suppose that $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible. Then, there is a Hilbert newform g over K of parallel weight 2, trivial character and level $2^2\mathfrak{p}_r^2\mathfrak{n}'$ such that

$$\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$$

for some prime ideal $\mathfrak{P} \mid p$ in the coefficient field K_g of g.
Here, $\mathfrak{n}'$ denotes the product of prime ideals coprime to $2r$ dividing C.
Moreover, we have $K \subset K_g$.

- Refined level lowering theorem of Breuil–Diamond.
- Precise description of the image of inertia, notably at prime ideals above 2 in K.

Step 4 – Refined level lowering

Finally assume that there exists a non-zero integer c such that $a^r + b^r = Cc^p$ for some fixed positive integer C and that we have

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 1 \pmod 4.$$

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ above the rational prime p.

Theorem

Suppose that $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible. Then, there is a Hilbert newform g over K of parallel weight 2, trivial character and level $2^2\mathfrak{p}_r^2\mathfrak{n}'$ such that

$$\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$$

for some prime ideal $\mathfrak{P} \mid p$ in the coefficient field K_g of g.
Here, $\mathfrak{n}'$ denotes the product of prime ideals coprime to $2r$ dividing C.
Moreover, we have $K \subset K_g$.

- Refined level lowering theorem of Breuil–Diamond.
- Precise description of the image of inertia, notably at prime ideals above 2 in K.

Step 4 – Refined level lowering

Finally assume that there exists a non-zero integer c such that $a^r + b^r = Cc^p$ for some fixed positive integer C and that we have

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 1 \pmod 4.$$

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ above the rational prime p.

Theorem

Suppose that $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible. Then, there is a Hilbert newform g over K of parallel weight 2, trivial character and level $2^2\mathfrak{p}_r^2\mathfrak{n}'$ such that

$$\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$$

for some prime ideal $\mathfrak{P} \mid p$ in the coefficient field K_g of g.
Here, $\mathfrak{n}'$ denotes the product of prime ideals coprime to $2r$ dividing C.
Moreover, we have $K \subset K_g$.

- Refined level lowering theorem of Breuil–Diamond.
- Precise description of the image of inertia, notably at prime ideals above 2 in K.

Table of contents

Step 5 – Main obstacles

In applying the modular method to Fermat equations of the shape

$$x^r + y^r = Cz^p$$

for specific values of r and C, we find that the **contradiction step** (and, to some extent, the irreducibility step) is the most problematic:

- Newform subspaces may not be accessible to computer softwares (as they are too large or by lack of efficient algorithms, for instance).
- We miss a general method to discard an isomorphism of the shape $\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$.

Step 5 – Main obstacles

In applying the modular method to Fermat equations of the shape

$$x^r + y^r = Cz^p$$

for specific values of r and C, we find that the **contradiction step** (and, to some extent, the irreducibility step) is the most problematic:

- Newform subspaces may not be accessible to computer softwares (as they are too large or by lack of efficient algorithms, for instance).
- We miss a general method to discard an isomorphism of the shape $\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$.

Step 5 – Main obstacles

In applying the modular method to Fermat equations of the shape

$$x^r + y^r = Cz^p$$

for specific values of r and C, we find that the **contradiction step** (and, to some extent, the irreducibility step) is the most problematic:

- Newform subspaces may not be accessible to computer softwares (as they are too large or by lack of efficient algorithms, for instance).
- We miss a general method to discard an isomorphism of the shape $\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{g,\mathfrak{P}}$.

The case $r = 7$ and $C = 3$

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a, b, c) = 1.$$

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a, b, c) = 1.$$

- **Multi-Frey approach** with:

  (Darmon) A Frey curve over $\mathbf{Q}$:

$$E : y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

where

$$\begin{aligned} a_2 &= -(a-b)^2, \\ a_4 &= -2a^4 + a^3 b - 5a^2 b^2 + ab^3 - 2b^4, \\ a_6 &= a^6 - 6a^5 b + 8a^4 b^2 - 13a^3 b^3 + 8a^2 b^4 - 6ab^5 + b^6. \end{aligned}$$

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a,b,c) = 1.$$

- **Multi-Frey approach** with:

  (Freitas) A Frey curve over the totally real cubic field $F/\mathbf{Q}(\zeta_7)^+$ (and its quadratic twists $F^{(d)}$):

$$F : y^2 = x(x-A)(x+B),$$

where

$$\begin{aligned} A &= (\omega_2 - \omega_1)(a+b)^2 \\ B &= (2-\omega_2)(a^2 + \omega_1 ab + b^2) \end{aligned}$$

and $\omega_i = \zeta_7^i + \zeta_7^{-i}, \quad (i = 1, 2).$

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a, b, c) = 1.$$

➥ **Multi-Frey approach** with:

(Kraus) A Frey hyperelliptic curve over $\mathbf{Q}$:

$$C : y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7$$

and its Jacobian $J/\mathbf{Q}(\zeta_7)^+$.

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a, b, c) = 1.$$

➥ **Computations** in (Hilbert) modular form spaces (Magma).

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a,b,c) = 1.$$

➥ **Three** different proofs:

	$7 \nmid a+b$	$7 \mid a+b$
$2 \nmid ab$	E or $F^{(-7)}$	F
$2 \parallel ab$	E or $F^{(-7\omega_2)}$	$F^{(\omega_2)}$
$4 \mid ab$	$F^{(-7)}$	E or F

	$7 \nmid a+b$	$7 \mid a+b$
$2 \nmid ab$	E or $F^{(-7)}$	F
$2 \parallel ab$	J	J
$4 \mid ab$	J	J

	$7 \nmid a+b$	$7 \mid a+b$
$2 \nmid ab$	E or $F^{(-7)}$	F
$2 \parallel ab$	E or $F^{(-7\omega_2)}$	J
$4 \mid ab$	$F^{(-7)}$	J

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a, b, c) = 1.$$

- **Multi-Frey approach** with **three** different Frey varieties: two elliptic curves $E/\mathbf{Q}$, $F/\mathbf{Q}(\zeta_7)^+$, and a 3-dimensional abelian variety $J/\mathbf{Q}(\zeta_7)^+$.
- **Computations** in (Hilbert) modular form spaces (Magma).
- **Three** different proofs: $(E+)F$ ($\sim$ **41 min.**), $(E+)F + J$ (as much as possible) ($\sim$ **8 min.**), $(E+)F + J$ ($\sim$ **1 min.**).

The case $r = 7$ and $C = 3$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^7 + b^7 = 3c^n, \quad abc \neq 0, \quad \gcd(a, b, c) = 1.$$

- **Multi-Frey approach** with **three** different Frey varieties: two elliptic curves $E/\mathbf{Q}$, $F/\mathbf{Q}(\zeta_7)^+$, and a 3-dimensional abelian variety $J/\mathbf{Q}(\zeta_7)^+$.
- **Computations** in (Hilbert) modular form spaces (Magma).
- **Three** different proofs: $(E+)F$ ($\sim$ **41 min.**), $(E+)F + J$ (as much as possible) ($\sim$ **8 min.**), $(E+)F + J$ ($\sim$ **1 min.**).
- Proofs using the hyperelliptic curve C are **faster**!

A partial answer in the case $r = 11$ and $C = 1$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^{11} + b^{11} = c^n, \quad abc \neq 0, \quad \gcd(a,b,c) = 1, \text{ and } (2 \mid a+b \text{ or } 11 \mid a+b).$$

- **Multi-Frey approach** using a Frey elliptic curve $F/\mathbf{Q}(\zeta_{11})^+$ (Freitas) and the hyperelliptic Frey curve C_{11}.
- Total running time in Magma: 7 hours = 6 hours (**computation** of the relevant Hilbert space) + 1 hour (**elimination**).
- Proving this result using only properties of $F/\mathbf{Q}(\zeta_{11})^+$ requires in particular computations in the space of Hilbert newforms of level $\mathfrak{p}_2^3\mathfrak{p}_{11}$ over $\mathbf{Q}(\zeta_{11})^+$ which has dimension $12,013$ and is **not** currently feasible to compute.

A partial answer in the case $r = 11$ and $C = 1$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^{11}+b^{11} = c^n, \quad abc \neq 0, \quad \gcd(a,b,c) = 1, \text{ and } (2 \mid a+b \text{ or } 11 \mid a+b).$$

- **Multi-Frey approach** using a Frey elliptic curve $F/\mathbf{Q}(\zeta_{11})^+$ (Freitas) and the hyperelliptic Frey curve C_{11}.
- Total running time in Magma: 7 hours = 6 hours (**computation** of the relevant Hilbert space) + 1 hour (**elimination**).
- Proving this result using only properties of $F/\mathbf{Q}(\zeta_{11})^+$ requires in particular computations in the space of Hilbert newforms of level $\mathfrak{p}_2^3\mathfrak{p}_{11}$ over $\mathbf{Q}(\zeta_{11})^+$ which has dimension 12,013 and is **not** currently feasible to compute.

A partial answer in the case $r = 11$ and $C = 1$

Theorem (B.–Chen–Dieulefait–Freitas, 2022)

For every integer $n \geq 2$, there are no integers a, b, c such that

$$a^{11}+b^{11} = c^n, \quad abc \neq 0, \quad \gcd(a,b,c) = 1, \text{ and } (2 \mid a+b \text{ or } 11 \mid a+b).$$

- **Multi-Frey approach** using a Frey elliptic curve $F/\mathbf{Q}(\zeta_{11})^+$ (Freitas) and the hyperelliptic Frey curve C_{11}.
- Total running time in Magma: 7 hours = 6 hours (**computation** of the relevant Hilbert space) + 1 hour (**elimination**).
- Proving this result using only properties of $F/\mathbf{Q}(\zeta_{11})^+$ requires in particular computations in the space of Hilbert newforms of level $\mathfrak{p}_2^3\mathfrak{p}_{11}$ over $\mathbf{Q}(\zeta_{11})^+$ which has dimension $12,013$ and is **not** currently feasible to compute.

Thank you!