Un abordaje multi-Frey al programa de Darmon para la ecuación de Fermat generalizada

Nuno Freitas

Universitat de Barcelona

diciembre 2020

colaboración con Billerey, Chen and Dieulefait

Motivation – Fermat type equations

Let $A, B, C \in \mathbb{Z}$ pairwise coprime. The equation

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

where $r, q, p \geq 2$ are exponents satisfying

$$1/r + 1/q + 1/p < 1$$

is called **the Generalized Fermat Equation.**

Definition

Let (a, b, c) be a solution to the GFE.

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

We say (a, b, c) is **primitive** if $\gcd(a, b, c) = 1$.

Motivation – Fermat type equations

Let $A = B = C = 1$. The GFE becomes

$$x^p + y^q = z^r, \qquad 1/r + 1/q + 1/p < 1.$$

There is a finite list of known solutions, including

$$2^7 + 17^3 = 31^2, \quad 17^7 + 76271^3 = 21063928^2$$

$$1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7$$

and the Catalan solution

$$1^p + 2^3 = 3^2.$$

Conjecture

- The known list is complete.
- **(Zagier-Tijdman, 'Beal Prize' Conjecture)** If $p, q, r \in \mathbb{Z}_{\geq 3}$ then there are only trivial solutions, i.e. $xyz = 0$.

Motivation – Fermat type equations

Theorem (Darmon–Granville)

Fix $A, B, C \in \mathbb{Z}$ pairwise coprime and prime exponents p, q, r satisfying $1/r + 1/q + 1/p < 1$. Then

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

has only finitely many non-trivial primitive solutions.

Fermat's Last Theorem

All solutions (a, b, c) to the equation

$$x^n + y^n + z^n = 0, \qquad n \geq 3$$

satisfy $abc = 0$.

Theorem (Wiles, Breuil–Conrad–Diamond–Taylor)

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

Sketch of proof of FLT

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

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

Consider the following curve, known as the **Frey curve**,

$$E : y^2 = x(x - a^p)(x + b^p),$$
$$\Delta_E = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16(abc)^{2p} \neq 0.$$

Remark: Trivial solutions DO NOT give rise elliptic curves.

WLOG we can assume $a \equiv -1 \pmod 4$ y $2 \mid b$;

Tate's algorithm gives that E is semistable of conductor

$$N_E = 2 \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

Sketch of proof of FLT

- Let $\overline{\rho}_{E,p}$ be the mod p representation attached to E;
- $\overline{\rho}_{E,p}$ is **irreducible** by Mazur's work on isogenies;
- By Wiles E is **modular**, then $\bar{\rho}_{E,p}$ is modular of level N_E.
- Since E is semistable and $\Delta_E = 16(abc)^{2p}$ we obtain the Serre level $N(\overline{\rho}_{E,p}) = 2$;
- Thus $\overline{\rho}_{E,p}$ arises in an eigenform of level $N(\overline{\rho}_{E,p}) = 2$, weight 2 and trivial character, by Ribet's **level lowering**.
- There are no eigenforms of weight 2 and level 2!! $\square$

Question: Can we solve the GFE with this strategy?

This question was already present in Serre's Duke paper from 1987, where a few equations of the form $x^p + y^p + Lz^p = 0$ with $p > 11$ were solved assuming Serre's conjecture.

Darmon's Frey curves over $\mathbb{Q}$ in 1997

(p,q,r)	Frey curve for $a^p+b^q=c^r$	Δ
$(2,3,p)$	$y^2=x^3+3bx+2a$	$-2^6 3^3 c^p$
$(3,3,p)$	$y^2=x^3+3(a-b)x^2+3(a^2-ab+b^2)x$	$-2^4 3^3 c^{2p}$
$(4,p,4)$	$y^2=x^3+4acx^2-(a^2-c^2)^2x$	$2^6(a^2-c^2)^2b^{2p}$
$(5,5,p)$	$y^2=x^3-5(a^2+b^2)x^2+5\frac{a^5+b^5}{a+b}x$	$2^4 5^3(a+b)^2c^{2p}$
$(7,7,p)$	$y^2=x^3+(a^2+ab+b^2)x^2$ $-(2a^4-3a^3b+6a^2b^2-3ab^3+2b^4)x$ $-(a^6-4a^5b+6a^4b^2-7a^3b^3+6a^2b^4-4ab^5+b^6)$	$2^4 7^2(\frac{a^7+b^7}{a+b})^2$
$(p,p,2)$	$y^2=x^3+2cx^2+a^px$	$2^6(a^2b)^p$
$(p,p,3)$	$y^2+cxy=x^3-c^2x^2-\frac{3}{2}cb^px+b^p(a^p+\frac{5}{4}b^p)$	$3^3(a^3b)^p$
(p,p,p)	$y^2=x(x-a^p)(x+b^p)$	$2^4(abc)^{2p}$

> *"Can one refine the existing techniques based on elliptic curves, modular forms, and Galois representations to prove the generalized Fermat conjecture for all the exponent listed in this table?"*

In a great Crelle paper Darmon and Loïc Merel solved the cases $(p,p,2)$, $(p,p,3)$ and $(4,p,4)$ but the other cases are still open!

Main steps of the modular method

1) Constructing the Frey curve. Attach a Frey elliptic curve E/K to a Diophantine equation, where K is a totally real;

2) Modularity. Prove modularity of E/K;

3) Irreducibility. Prove irreducibility of $\overline{\rho}_{E,p}$

4) Level lowering. Conclude via level lowering that $\overline{\rho}_{E,p} \simeq \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$ where $\mathfrak{f}$ is Hilbert eigenform over K with parallel weight 2, trivial character and level among finitely many explicit possibilities N_i;

5) Contradiction.
5a) Compute all the Hilbert newforms $\mathfrak{f}$ predicted in step 4;
5b) Show that $\overline{\rho}_{E,p} \not\simeq \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$ for all $\mathfrak{f}$ computed in **5a)** that is, we need to distinguish Galois representations.

Obstructions arising from solutions

Consider the the Fermat-type equation

$$x^3 + y^3 = z^p$$

which has associaed Frey curve

$$E_{a,b} : Y^2 = X^3 + 3abX + b^3 - a^3, \quad \Delta = -2^4 \cdot 3^3 \cdot c^{2p}.$$

It has the solutions

$$0^3 + (\pm 1)^3 = (\pm 1)^p \quad \text{and} \quad 2^3 + 1^3 = (\pm 3)^2$$

which give rise to elliptic curves since $c \neq 0$. In particular, after modularity, irreducibility and level lowering, we can have

$$\overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{E_{1,0},p}, \quad \text{or} \quad \overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{E_{2,1},p},$$

where

$$E_{1,0} : y^2 = x^3 + 1 \quad \text{or} \quad E_{2,1} : y^2 = x^3 + 6x - 7.$$

Obstructions arising from solutions

Sometimes the situation can be (partially) saved.

Recall that $0^3 + (\pm 1)^3 = (\pm 1)^p$ and suppose

$$\overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{E_{1,0},p}, \qquad \text{with} \qquad E_{1,0} : y^2 = x^3 + 1$$

- $E_{1,0}$ has CM by $\mathbb{Q}(\sqrt{-3})$
- If $p \equiv 1 \pmod 3$ then $\overline{\rho}_{E_{1,0},p}$ has image in the normalizer of a split Cartan, so $\overline{\rho}_{E_{a,b},p}$ also;
- From a result of Bilu–Parent–Reboledo conclude that $E_{a,b}$ is CM, thus $j = \frac{2^8 3^3 (ab)^3}{c^{2p}} \in \mathbb{Z}$, hence $c = \pm 1$
- If $p \equiv 2 \pmod 3$ then $\overline{\rho}_{E_{a,b},p}$ has image in the normalizer of a non-split Cartan; note $E_{a,b}$ has the two torsion point $(a - b, 0)$
- From a result of Darmon–Merel we get that $j \in \mathbb{Z}[\frac{1}{p}]$, hence $c = \pm 1$

Obstructions arising from solutions

Recall the solution $2^3 + 1^3 = (\pm 3)^2$ and assume

$$\overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{E_{2,1},p}, \quad \text{with} \quad E_{2,1} : y^2 = x^3 + 6x - 7.$$

The curve $E_{2,1}$ has no CM.

There exists a $G_{\mathbb{Q}}$-modules isomorphism $\phi : \ E_{a,b}[p] \to E_{2,1}[p]$.

We can study wether ϕ preserves the Weil pairing.

Theorem (F. 2016)

Let $p \geq 3$ be a prime such that $p \equiv 2 \pmod 3$. Then the equation

$$x^3 + y^3 = z^p$$

has no non-trivial primitive solutions.

Remark: Together with a result of Chen–Siksek this equation is solved for a set of prime exponents p with density ~ 0.81.

Obstructions arising from solutions

Consider the the Fermat-type equation

$$x^2 + y^3 = z^p$$

which has associaed Frey curve

$$E_{a,b} \; : y^2 = x^3 + 3bx + 2a, \qquad \Delta = -2^6 3^3 c^p.$$

- $(\pm 1, -1, 0)$ give rise to singular Frey curves since $c = 0$;
- $(\pm 1, 0, 1)$ and $\pm(0, 1, 1)$ give rise to CM curves;
- The Catalan solution $3^2 + (-2)^3 = 1^p$, givess the non-CM curve $E_{3,-2} \; : y^2 = x^3 - 6x + 6$.

In particular, after level lowering, we can have

$$\overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{E_{3,-2},p}, \quad \overline{\rho}_{E_{1,0},p}, \quad \overline{\rho}_{E_{0,1},p}$$

Note that $E_{a,b}$ has no 2 or 3 torsion points.

Obstructions arising from solutions

By determining rational points on the several modular curves $X_E(p)$, including $E = E_{3,-2}, E_{1,0}, E_{0,1}$, we have

Theorem (Poonen–Schaefer–Stoll 2007)

For $p = 7$ all solutions to $x^2 + y^3 = z^p$ are known.

Theorem (F.–Naskręcki–Stoll 2019)

For $p = 11$, assuming GRH, all solutions to $x^2 + y^3 = z^p$ are trivial.

To deal with all kinds of solutions, the ideal tool is

Frey–Mazur Conjecture

There exists a constant $C \geq 17$ such that for any elliptic curves E, E' over $\mathbb{Q}$ and $p > C$ we have

$$E[p] \simeq E'[p] \Rightarrow E \text{ is isogenous to } E'$$

Major difficulties of the modular method

(1) There are not enough Frey curves.

Theorem (F. 2015)

Let $r \geq 5$ be a prime.
There are several explicit Frey curves attached to the equation $x^r + y^r = Cz^p$ defined over totally real subfields of $\mathbb{Q}(\zeta_r)$.

(2) We need to deal with obstructions arising from solutions.

In a Duke paper from 2000, Henri Darmon described a remarkable program to attack the GFE that **conjecturally** deals with these problems **in general!**

Darmon's Frey representations

Let K be a number field and $K(t)$ the function field with variable t.

Definition

Let p, q, r be primes with $p \neq 2$. A **Frey representation** (in characteristic p) of signature (p, q, r) over K is a representation

$$\overline{\rho} : G_{K(t)} \to \mathrm{GL}_2(\mathbb{F}) \qquad \text{where } [\mathbb{F} : \mathbb{F}_p] \text{ is finite,}$$

with projectivization $\mathbb{P}(\overline{\rho}) : G_{K(t)} \to \mathrm{PGL}_2(\mathbb{F})$ and such that

1. $\overline{\rho}\,|_{G_{\bar{K}(t)}}$ has trivial determinant and is irreducible.
2. $\mathbb{P}(\overline{\rho})|_{G_{\bar{K}(t)}}$ is unramified outside $0, 1, \infty$.
3. $\mathbb{P}(\overline{\rho})|_{G_{\bar{K}(t)}}$ maps the inertia subgroups at 0, 1 and ∞ to subgroups of $\mathrm{PSL}_2(\mathbb{F})$ of order p, q and r, respectively.

We say that two Frey representations $\overline{\rho}_1$, $\overline{\rho}_2$ of signature (p, q, r) are **equivalent** when $\mathbb{P}(\overline{\rho}_1)$, $\mathbb{P}(\overline{\rho}_2)$ are conjugate in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$.

Darmon's Frey representations

One should think of a Frey representation of signature (p, q, r)

$$\overline{\rho} : G_{K(t)} \to \mathrm{GL}_2(\mathbb{F})$$

as a one-parameter family $\overline{\rho} = \overline{\rho}(t)$ of representations of G_K.

Proposition (Darmon's motivation)

There exists a finite set of primes S of K depending on $\overline{\rho}$ in an explicit way, such that, for all primitive solutions (a, b, c) to $Aa^p + Bb^q = Cc^r$, the representation $\overline{\rho}(Aa^p/Cc^r)$ has a quadratic twist which is unramified outside S.

Frey representations of signature (p, p, p)

The Legendre family $L(t)\ :\ y^2 = x(x-1)(x-t)$ gives Frey representations of signature (p, p, p). Suppose $a^p + b^p = c^p$. Then $L(a^p/c^p)$ is a quadratic twist of $y^2 = x(x - a^p)(x + b^p)$ whose mod p representation is unramified outside 2.

Darmon's Frey representations

Frey representations of signature (p, p, r)

Let $r \geq 3$ be prime. Let $K = \mathbb{Q}(\zeta_r)^+$ with ring of integers $\mathcal{O}_K$. Set $\omega_j = \zeta_r^j + \zeta_r^{-j}$ and $g(x) = \prod_j (x + \omega_j)$. Consider the hyperelliptic curve over $\mathbb{Q}(t)$

$$C_r^-(t) \, : \, y^2 = xg(x^2 - 2) + 2 - 4t$$

Theorem (Darmon)

The Jacobian $J = J_r^-(t)$ of $C_r^-(t)$ become of GL_2-type over $K(t)$ with real multiplications by $\mathcal{O}_K$ and its mod $\mathfrak{p}$ representations $\overline{\rho}_{J/K,\mathfrak{p}} : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ are Frey representations of type (p, p, r).

Other Frey representations

Darmon also shows there are Frey representations of signatures (r, r, p) and (p, q, r) arising on certain Frey abelian varieties but these are not explicit and impractical to work with.

Advantages of the Darmon program

(1) There are not enough Frey curves.

For (a, b, c) a solution to $x^p + y^p = z^r$ with $r = 5, 7$ considers the Jacobian J_r of the curves:

$$\begin{aligned} r = 5 &\ :\ y^2 = x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p), \\ r = 7 &\ :\ y^2 = x^7 - 7c^2x^5 + 14c^4x^3 - 7c^6x - 2(a^p - b^p). \end{aligned}$$

A recipe is given for all r and the discriminant is

$$\Delta = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r (ab)^{\frac{r-1}{2}p}.$$

Over the maximal totally real subfield K of $\mathbb{Q}(\zeta_r)$, we have that J_r acquires real multiplications by K, hence it becomes of GL_2-type. **Conjecturally** the 2-dimensional p-torsion representation of J_r/K arises in a Hilbert modular form over K with 'small' conductor.

Advantages of the Darmon program

(2) We need to deal with obstructions arising from solutions.

Recall the 'Beal Prize' Conjecture

If $p, q, r \in \mathbb{Z}_{\geq 3}$ then there are only trivial solutions to $x^p + y^q = z^r$

Proposition (Darmon)

The Frey abelian varieties attached to trivial solutions of $x^p + y^p = z^r$ have CM.

Conjecture

Let K be totally real field. There exists a constant C_K such that, for any abelian variety A/K of GL_2-type with

$$\mathrm{End}_K(A) \otimes \mathbb{Q} = \mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q} = K,$$

and all primes $\mathfrak{p}$ of K of norm $> C_K$, we have $\mathrm{SL}_2(\mathbb{F}) \subset \overline{\rho}_{A,\mathfrak{p}}(G_K)$.

So (2) is **conjecturally solved** $x^p + y^p = z^r$.

Problems of the Darmon program

So far Darmon's approach only succeeded when the Frey abelian varieties are elliptic curves.

Otherwise there are issues at every step! More precisely :

- Writing down the Frey varieties of type (r, r, p) and (p, q, r)
- Computing their conductor;
- Proving irreducibility of their mod p representations;
- Proving modularity of their mod p representations;
- Computing Hilbert newforms over large fields is impractical;
- Deal with the obstructions arising from solutions.

So, can we use it ?

We simplify the problem and consider the subfamily $x^r + y^r = 3z^p$ of the GFE which has only the trivial solution $(1, -1, 0)$.

The Fermat equation $x^r + y^r = 3z^p$

The equation $x^r + y^r = 3z^p$ has been stuedied in various works using the modular method with elliptic curves. In particular, using the **multi-Frey** approach, i.e., using **several** Frey curves over totally real fields we proved :

Theorem (Billerey–Chen–Dieulefait–F., 2019)

For all primes p there are no non-trivial primitive solutions to

$$x^5 + y^5 = 3z^p \quad \text{and} \quad x^{13} + y^{13} = 3z^p.$$

where for the second equation we assume also $p \neq 7$.

Theorem (Billerey–Chen–Dembélé–Dieulefait–F., preprint)

There are no non-trivial primitive solutions to the equation

$$x^{13} + y^{13} = 3z^7.$$

The Fermat equation $x^r + y^r = 3z^p$

Theorem (F. 2015)

There is a constant C such that, for all primes $p > C$,

$$x^7 + y^7 = 3z^p$$

has no non-trivial primitive solutions.

Question: Can we optimize this constant?

To do that requires to compute Hilbert newforms over $\mathbb{Q}(\zeta_7)^+$ in spaces of dimensions 12289 and 10753, which is impractical.

Using a Frey curve over $\mathbb{Q}$ and another over $\mathbb{Q}(\zeta_7)^+$ we get

Theorem (Billerey–Chen–Dieulefait–F.)

For all primes p there are no non-trivial primitive solutions to

$$x^7 + y^7 = 3z^p \qquad \text{with} \qquad 2 \mid x + y.$$

Kraus Frey hyperelliptic curve

Set $\omega_j = \zeta_7^j + \zeta_7^{-j}$ and $g(x) = \prod_j (x - \omega_j)$. Consider

$$C(s) \ : \ y^2 = xg(x^2 + 2) + s$$

defined over $\mathbb{Q}(s)$.

Proposition

Let $K = \mathbb{Q}(\zeta_7)^+$. The Jacobian $J(s)$ of $C(s)$ becomes of GL_2-type over $K(s)$ with multiplicatons by $\mathcal{O}_K$. Moreover, its mod $\mathfrak{p}$ representations are 'like' a Frey representation of type $(p, p, 7)$ but with ramification at $\{\pm 2i, \infty\}$.

Given a solution to $a^7 + b^7 = 3c^p$, $ab \neq 0$, set $s_0 = \frac{(b^7 - a^7)}{(\sqrt{ab})^7}$.
A quadratic twist of $C(s_0)$ gives Kraus hyperelliptic Frey curve

$$C(a, b, c) \ : \ y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7,$$

$$\Delta = -2^{12} \cdot 7^7 \cdot (a^7 + b^7)^6 = -2^{12} \cdot 7^7 \cdot 3^6 \cdot c^{6p}.$$

The residual representation modulo $\mathfrak{p}_7$

Let (a, b, c) satisfy $a^7 + b^7 = 3c^p$ and $\gcd(a, b, c) = 1$.
Set $J = J(C(a, b, c))$ and $t_0 = \frac{a^7}{3c^p}$.

Proposition

The representation $\overline{\rho}_{J,\mathfrak{p}_7} : G_K \to \mathrm{GL}_2(\mathbb{F}_7)$ is a quadratic twist of $\overline{\rho}_{L(t_0),7}$, where $L(t)$ is $y^2 = x(x-1)(x-t)$.

Idea of proof:

- There is a quadratic extension $K(s, t)$ of $K(s)$ such that the base change of $C(s)$ to $K(s, t)$ has a model $C'(t)$ defined over $\mathbb{Q}(t)$ with ramification set equal to $\{0, 1, \infty\}$.
- Let $J'(t)$ be the Jacobian of $C'(t)$ and $\mathfrak{p} \mid p$ in K. The representation $\overline{\rho}_{J'(t),\mathfrak{p}} : G_{K(t)} \to \mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$ is a Frey representation of type $(7, 7, p)$.
- In particular, $\overline{\rho}_{J',\mathfrak{p}_7} : G_{K(t)} \to \mathrm{GL}_2(\mathbb{F}_7)$ is a Frey representation of type $(7, 7, 7)$, where $\mathfrak{p}_7$ is the unique prime above 7 in K.

The residual representation modulo $\mathfrak{p}_7$

- In particular, $\overline{\rho}_{J',\mathfrak{p}_7} : G_{K(t)} \to \mathrm{GL}_2(\mathbb{F}_7)$ is a Frey representation of type $(7,7,7)$, where $\mathfrak{p}_7$ is the unique prime above 7 in K.

Theorem (Darmon, Hecke)

There is a unique Frey representation of signature (p,p,p). It arises in the Legendre family $L(t)$.

- Hence as representations of G_K, we have

$$\overline{\rho}_{J'(t_0),\mathfrak{p}_7} \cong \overline{\rho}_{L(t_0),7} \otimes \epsilon$$

  where $\epsilon : G_K \to \overline{\mathbb{F}}^\times$ is a character.
- Since $t_0 \in \mathbb{Q}$ we have $J'(t_0)$ is defined over $\mathbb{Q}$ and since 7 is totally ramified in $\mathcal{O}_K$ it follows that the action of G_K on $J'(t_0)[\mathfrak{p}_7]$ extends to a linear representation $G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_7)$.
- We show that ϵ extends to $G_\mathbb{Q}$ and is quadratic.
- This proves the statement for $\overline{\rho}_{J'(t_0),\mathfrak{p}_7}$ and carefully reversing the relation between $J'(t_0)$ and J gives the result.

The residual representation modulo $\mathfrak{p}_7$

Proposition

The G_K-representation $\overline{\rho}_{J,\mathfrak{p}_7}$ is absolutely irreducibility and its image is not projectively dihedral, unless $(a,b) = \pm(1,1)$.

Proof: We have seen that, as $G_{\mathbb{Q}}$-representations,

$$\overline{\rho}_{L(t_0),7} \simeq \overline{\rho}_{J,\mathfrak{p}_7} \otimes \chi \qquad t_0 = \frac{a^7}{Cc^p},$$

where χ is quadratic and $L(t_0)$ has full 2-torsion.

If $\overline{\rho}_{J,\mathfrak{p}_7}$ is reducible over G_K, we obtain a non-cuspidal K-point in $X_0(28)$, therefore also in $X_0(14)$.

All the K-points on $X_0(14)$ are due to rational elliptic curves with conductor 49 and none of these curves acquires a 4-isogeny over K.

We conclude there are no non-cuspidal K-rational points in $X_0(28)$, hence $\overline{\rho}_{J,\mathfrak{p}_7}$ is absolutely irreducibile.

The residual representation $\overline{\rho}_{J,\mathfrak{p}_7}$

Proof (continued): Recall that $\overline{\rho}_{J,\mathfrak{p}_7} \simeq \overline{\rho}_{L(t_0),7} \otimes \chi$ is irreducible. We are left to show that $\overline{\rho}_{J,\mathfrak{p}_7}$ has image not projectively dihedral.

That is, $\overline{\rho}_{J,\mathfrak{p}_7}(G_K) \subset \mathrm{GL}_2(\mathbb{F}_7)$ is not contained in the normalizer of a Cartan subgroup, equivalently $\overline{\rho}_{L(t_0),7}(G_K)$ is not contained in the normalizer of a Cartan subgroup.

This will follow from $\mathrm{SL}_2(\mathbb{F}_7) \subset \overline{\rho}_{L(t_0),7}(G_{\mathbb{Q}})$.

Since L has full 2-torsion, it is known that, either (a) $L(t_0)$ has CM or (b) $\overline{\rho}_{L(t_0),7}$ is reducible or surjective.

If we are in case (b), then $\overline{\rho}_{L(t_0),7}$ is surjective and we are done.

If $L(t_0)$ has CM, then

$$j(L(t_0)) = 2^8 \cdot \frac{((a^7+b^7)^2 - (ab)^7)^3}{((ab)^7(a^7+b^7))^2} \in \mathbb{Z}$$

Since a, b are coprime, we get that $(ab)^{14}$ divides 2^8 and hence $ab = \pm 1$. From $a^7 + b^7 \neq 0$ it follows that $(a,b) = \pm(1,1)$.

Modularity

Theorem

The Frey variety J/K attached to $a^7 + b^7 = 3c^p$ is modular.

Proof:

- If $(a, b) = \pm(1, 1), \pm(1, 0), \pm(0, 1)$ then J has CM;
- Assume $(a, b) \neq \pm(1, 1)$ and $ab \neq 0$;
- There is an irreducible $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_7)$ such that $\overline{\rho}_{J,\mathfrak{p}_7} \cong \overline{\rho}\,|_{G_K}$, that is, $\overline{\rho}_{J,\mathfrak{p}_7}$ is a base change from $\mathbb{Q}$.
- From Serre's Conjecture $\overline{\rho}$ is modular, so $\overline{\rho}_{J,\mathfrak{p}_7}$ is modular over K by cyclic base change.
- Modularity of J/K now follows from a modularity lifting theorem of Breuil–Diamond, since $\overline{\rho}_{J,\mathfrak{p}_7}$ is absolutely irreducible and its image not projectively dihedral.

Remark: Modularity proof does not use $2 \nmid a + b$ neither $C = 3$.

Irreducibility, Level Lowering and Contradiction

Using $2 \nmid a + b$ we show that J/K is a principal series at $\mathfrak{q}_2$ and by combining this with CFT we can prove.

Proposition

The representation $\overline{\rho}_{J,\mathfrak{p}}$ is irreducible for all $\mathfrak{p} \mid p$ when $p \geq 5$.

Modularity, irreducibility, level lowering and $2 \nmid a + b$ give

$$\overline{\rho}_{J,\mathfrak{p}} \cong \overline{\rho}_{g,\mathfrak{p}'},$$

where g is new of level $N(\overline{\rho}_{J,\mathfrak{p}}) = \mathfrak{q}_2^2 \mathfrak{q}_3 \mathfrak{q}_7^2$ and parallel weight 2.

The dimension of this cuspidal space is 1345, and so it is **possible** to compute the newforms!

To reach a contradiction we need to show that $\overline{\rho}_{J,\mathfrak{p}} \ncong \overline{\rho}_{g,\mathfrak{p}'}$ for all g for each of the 61 newforms. Making this efficiently requires using various arguments some using $2 \nmid a + b$.

GRACIAS!!