Fermat-type equations via computation of elliptic curves with prescribed trace of Frobenius

Nuno Freitas

Instituto de Ciencias Matemáticas
CSIC-ICMAT

June 2023

Joint work with Benjamin Matschke

The origin of everything

Fermat's Last Theorem

The only solutions (a, b, c) to the equation

$$x^n + y^n + z^n = 0, \qquad a, b, c \in \mathbb{Z}, \qquad n \geq 3$$

satisfy $abc = 0$.

Theorem (Wiles, Taylor–Wiles)

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

Can the modular method be applied to other equations?

Can the modular method be applied to other 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 $\gcd(a, b, c) = 1$.

The modular method

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

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).

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

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

The obstruction arising from solutions

The equation $x^p + y^p = z^p$ has solutions $(0, \pm 1, \pm 1)$ and $(1, -1, 0)$

$$E_{a,b} : Y^2 = X(X - a^p)(X + b^p) \quad \Delta = 2^4 \cdot (abc)^{2p}.$$

The equation $x^3 + y^3 = z^p$ also has solutions $(2, 1, \pm 3)$ for $p = 2$

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

The equation $x^2 + y^3 = z^p$ also has solutions $(\pm 3, 2, 1)$ for all p

$$E_{a,b} : Y^2 = X^3 + 3bX + 2a \quad \Delta = 2^6 3^3 c^p.$$

Therefore, after modularity and level lowering, we can have

$$\overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{E_{\mathrm{sol}},p}$$

Theorem (Kraus, Darmon–Merel, Chen–Siksek, F.)

The equation $x^3 + y^3 = z^p$ has no non-trivial primitive solutions for a ser of prime exponents with density ~ 0.844.

The multi-Frey approach to $x^r + y^r = Cz^p$

To avoid solutions we consider equations of the form

$$x^r + y^r = Cz^p \qquad \text{where} \qquad C \geq 3$$

Fix $r \geq 5$ be a prime and $\zeta = \zeta_r$ a fixed primitive r-th root of unity.
Let $K = \mathbb{Q}(\zeta_r)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_r)$.
For an integer k we define the polynomial

$$f_k(x, y) := x^2 + \omega_k xy + y^2 \quad \text{where} \quad \omega_k = \zeta^k + \zeta^{-k}.$$

We have the following elementary factorization over K

$$x^r + y^r = (x + y)\Phi(x, y) = (x + y)f_1(x, y)f_2(x, y) \cdots f_{\frac{r-1}{2}}(x, y).$$

Let $(k_1, k_2, k_3) \in \mathbb{Z}^3$ satisfy $0 \leq k_1 < k_2 < k_3 \leq (r - 1)/2$, and set

$$\alpha = \omega_{k_3} - \omega_{k_2}, \quad \beta = \omega_{k_1} - \omega_{k_3}, \quad \gamma = \omega_{k_2} - \omega_{k_1}.$$

The multi-Frey approach to $x^r + y^r = Cz^p$

Let (a, b, c) be a primitive solution to $x^r + y^r = Cz^p$. Set

$$A_{a,b} = \alpha f_{k_1}(a, b), \quad B_{a,b} = \beta f_{k_2}(a, b), \quad C_{a,b} = \gamma f_{k_3}(a, b)$$

satisfying $A_{a,b} + B_{a,b} + C_{a,b} = 0$.
We can consider the elliptic curve over K given by

$$Z_{a,b}^{(k_1,k_2,k_3)} \ : \ Y^2 = X(X - A_{a,b})(X + B_{a,b}).$$

having standard invariants:

$$\begin{aligned} c_4(Z_{a,b}) &= 2^4(A_{a,b}^2 - B_{a,b}C_{a,b}) \\ c_6(Z_{a,b}) &= -2^5(A_{a,b} - B_{a,b})(B_{a,b} - C_{a,b})(C_{a,b} - A_{a,b}) \\ \Delta(Z_{a,b}) &= 2^4\left(A_{a,b}B_{a,b}C_{a,b}\right)^2. \end{aligned}$$

The discriminant is a constant times a p-th power !

The multi-Frey approach to $x^r + y^r = Cz^p$

Let $(k_1, k_2, k_3) \in \mathbb{Z}^3$ be as above with $k_1 \neq 0$.

The following is a consequence of Tate's Algorithm

Proposition

Let N_E denote the conductor of $E = E_{a,b} = Z_{a,b}^{(k_1,k_2,k_3)}$. We have

1. For all primes $\mathfrak{q} \mid C$ above $q \not\equiv 1 \pmod{r}$ the curve E has good reduction at $\mathfrak{q}$.
2. If $r \mid a + b$ then E has good reduction at $\mathfrak{q}_r$.
3. If $r \nmid a + b$ then E has potentially good reduction at $\mathfrak{q}_r$ and $v_{\mathfrak{q}_r}(N_E) = 2$.
4. For all primes $\mathfrak{q}_2 \mid 2$, we have $v_{\mathfrak{q}_2}(N_E) \in \{2, 3, 4\}$.
5. the Serre level of $\overline{\rho}_{E,p}$ is given by

$$N(\overline{\rho}_{E,p}) = \prod_{\mathfrak{q}_2 \mid 2} \mathfrak{q}_2^{\upsilon_{\mathfrak{q}_2}(N_E)} \mathfrak{q}_r^{\upsilon_{\mathfrak{q}_r}(N_E)}$$

The multi-Frey approach to $x^r + y^r = Cz^p$

Let $(k_1, k_2, k_3) \in \mathbb{Z}^3$ be as above with $k_1 = 0$.

The following is a consequence of Tate's Algorithm

Proposition

Let N_F denote the conductor of $F = F_{a,b} = Z_{a,b}^{(0,k_2,k_3)}$.

1. A prime $\mathfrak{q} \nmid 2r$ is of bad reduction for F if and only if it divides $(a+b)f_{k_2}(a,b)f_{k_3}(a,b)$. In such case, F has bad multiplicative reduction at $\mathfrak{q}$
2. If $\mathfrak{q} \mid C$ and $\mathfrak{q} \nmid 2r$ then $v_{\mathfrak{q}}(N_F) = 1$.
3. We have $v_{\mathfrak{q}_2}(N_F) \in \{1, 2, 3, 4\}$
4. the Serre level of $\overline{\rho}_{F,p}$ is given by

$$N(\overline{\rho}_{F,p}) = \prod_{\mathfrak{q}_2 \mid 2} \mathfrak{q}_2^{\upsilon_{\mathfrak{q}_2}(N_F)} \cdot \mathfrak{q}_r^{\upsilon_{\mathfrak{q}_r}(N_F)} \cdot \prod_{\mathfrak{q} \mid C} \mathfrak{q}$$

The equation $x^{19} + y^{19} = 5z^p$

Let $K_0 = \mathbb{Q}(z)$ where $z^3 + z^2 - 6z - 7 = 0$.

Note that 2 and 5 are inert in K_0 and K

We have $[K : \mathbb{Q}] = 9$ and $[K : K_0] = 3$.

There is a generator σ of $\mathrm{Gal}(K/K_0)$ satisfying

$$\sigma(\omega_1) = \omega_7, \quad \sigma(\omega_7) = \omega_8, \quad \sigma(\omega_8) = \omega_1,$$

hence the Frey curve $E_{a,b} = Z_{a,b}^{(1,7,8)}$ admits a model E_0/K_0.

Since $[K_0 : \mathbb{Q}]$ is odd, the Eichler-Shimura conjecture holds over K_0. Therefore, by modularity and level lowering, for large enough p, we have

$$\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{f,\mathfrak{p}} \simeq \overline{\rho}_{W,p}$$

where W is an elliptic curve over K_0 with full 2-torsion over K, no 2-torsion points over K_0 and conductor equal to $N(\overline{\rho}_{E_0,p})$.

The equation $x^{19} + y^{19} = 5z^p$

We know that $\upsilon_{\mathfrak{q}_2}(N_{E_0}) \in \{2, 3, 4\}$, and the exact valuations are determined by $a, b \pmod{2^5}$. Using `Magma` to run through all the congruence classes yields

$$N(\overline{\rho}_{E_0,p}) = \begin{cases} \mathfrak{q}_2^4 \mathfrak{q}_r^2 & \text{if } a+b \text{ is odd and } ab \equiv 2 \pmod 4, \\ \mathfrak{q}_2^3 \mathfrak{q}_r^2 & \text{otherwise,} \end{cases} \tag{1}$$

Moreover, if $a + b$ is odd and $ab \equiv 2 \pmod 4$, we have

$$N(\overline{\rho}_{E_0^{\delta_1},p}) = \mathfrak{q}_2^2 \mathfrak{q}_r^2 \tag{2}$$

where $E_0^{\delta_1}$ is the quadratic twist of E_0 by the unit $\delta_1 = -z^2 + 5$.

The equation $x^{19} + y^{19} = 5z^p$

When $19 \mid a + b$, the curve $E_{a,b}/K$ has good reduction at $\mathfrak{q}_r$.

If $19 \nmid a + b$, then $E_{a,b}^{\delta_2}/K$ has good reduction at $\mathfrak{q}_r$ where $\delta_2 = -z^2 - 3z - 3$.

The curve $E_{a,b}/K$ has good reduction at $\mathfrak{q}_5$.

The trace of Frobenius $a_{\mathfrak{q}_5}(E_0) = (5^3 + 1) - \#\tilde{E}_0(\mathbb{F}_{\mathfrak{q}_5})$ depends only on a, b modulo 5. Using that $5 \mid a + b$, we have

$$a_{\mathfrak{q}_5}(E_0) = a_{\mathfrak{q}_5}(E_0^{\delta_1}) = a_{\mathfrak{q}_5}(E_0^{\delta_2}) = a_{\mathfrak{q}_5}(E_{1,-1}/K_0) = -9$$

Therefore, taking twists by δ_i and traces at $\mathfrak{q}_5$ in $\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{W,p}$ together with the Weil bound imply

$$a_{\mathfrak{q}_5}(W) = a_{\mathfrak{q}_5}(W^{\delta_1}) = a_{\mathfrak{q}_5}(W^{\delta_2}) = -9. \tag{3}$$

The equation $x^{19} + y^{19} = 5z^p$

All the above shows that, after twisting both sides of $\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{W,p}$ by δ_1 or δ_2 or $\delta_1\delta_2$ when needed, we can assume that

$$\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{W,p}$$

where W satisfies

1. full 2-torsion over K and trivial 2-torsion over K_0;
2. good reduction away from $\mathfrak{q}_2$ over K;
3. conductor $\mathfrak{q}_2^2\mathfrak{q}_r^2$ or $\mathfrak{q}_2^3\mathfrak{q}_r^2$ over K_0;
4. $a_{\mathfrak{q}_5}(W/K) = \alpha^3 + \beta^3 = 2646$, where α, β are the roots of the characteristic polynomial of Frobenius at $\mathfrak{q}_5$ over K_0, that is $x^2 + 9x + 125$.

Can we compute ONLY these curves?

Matschke tables for elliptic curves

Benjamin Matschke developed a novel S-unit equation solver which he used to efficiently compute sets $M(K, S)$ of elliptic curves over a number field K with good reduction outside S.

For example, over $\mathbb{Q}$, he computed all curves of conductor N such that $\mathrm{Rad}(2N) \leq 1000000$. These include all elliptic curves in Cremonas' database (i.e. $N \leq 500000$) and the largest conductor included is 1727923968836352. Upcoming improvements to the solver will compute particular subsets of $M(S, K)$, where

1. the 2-torsion field of E is given,
2. the places of possible bad reduction of E over the 2-torsion field is further restricted, and
3. some trace of Frobenius is prescribed (up to sign).

Remark: Applying 3. requires extra computations, so it depends on the case wether it will be quicker than applying no restrictions.

The equation $x^{19} + y^{19} = 5z^p$

Using the above algorithms, we computed all elliptic curves satisfying the required properties. Unfortunately there are still unnecessary computations going on.

We found no elliptic curves with conductor $\mathfrak{q}_2^2\mathfrak{q}_r^2$ and 24 elliptic curves with conductor $\mathfrak{q}_2^3\mathfrak{q}_r^2$.

Next, for each computed W, we show that, for large p, the isomorphism $\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{W,p}$ is impossible unless $W = E_{1,-1}$. This is achieved by standard arguments comparing traces of Frobenius at various primes.

We note 13 is inert in K_0, and from $\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{E_{-1,1},p}$ it follows

$$a_{\mathfrak{q}_{13}}(E_{a,b}) = a_{\mathfrak{q}_{13}}(E_{1,-1}) = 67.$$

Since $a_{\mathfrak{q}_{13}}(E_{a,b})$ depends only on a, b modulo 13, a quick computation shows that $a_{\mathfrak{q}_{13}}(E_{a,b}) = 67$ implies $13 \mid a + b$.

The equation $x^{19} + y^{19} = 5z^p$

Finally, we now switch to the Frey curve $F_{a,b}$

Note that F is defined over K and not K_0.

After modularity and level lowering, we have

$$\overline{\rho}_{F_{a,b},p} \simeq \overline{\rho}_{W,p}$$

where W has full 2-torsion over K, conductor $N(\overline{\rho}_{F_{a,b},p})$.
Moreover, F/K It has multiplicative reduction at $\mathfrak{q}_{13}$ and

$$N(\overline{\rho}_{F,p}) = 2^{\upsilon_{\mathfrak{q}_2}(N_F)} \cdot \mathfrak{q}_{19}^{\upsilon_{\mathfrak{q}_r}(N_F)} \cdot 5$$

therefore level lowering occurs at $\mathfrak{q}_{13}$ which requires

$$a_{\mathfrak{q}_{13}}(W) \equiv \pm(\mathrm{Norm}(\mathfrak{q}_{13}) + 1) \pmod{p}.$$

For large p this congruence gives a contradiction with the Weil bound $|a_{\mathfrak{q}}(W)| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}$. $\square$

Concluding Remarks

We have proved

Theorem (F.–Matschke)

The equation $x^{19} + y^{19} = 5z^p$ has non non-trivial primitive integer solutions for large enough p.

Remarks:

- Note that there were **NO** calculation of newforms or elliptic curves required with the Frey curve F.
- The equations $x^r + y^r = 3z^p$ for $r = 11, 17, 19$ seem approachable.
- We have computed all elliptic curves over the degree 8 maximal totally real subfield $K \subset \mathbb{Q}(\zeta_{19})$ with good reduction outside 2, full 2-torsion over K and $a_{\mathfrak{q}_3}(W) = \pm 118$. Took about 6 days, and computing all the curves seems impossible.

THANK YOU !!