On some generalized Fermat equations of the form $x^2 + y^{2n} = z^p$

Philippe Michaud-Jacobs

University of Warwick

Modern Breakthroughs in Diophantine Problems

Banff, Canada

20th June 2022

The Generalized Fermat Conjecture

The equation

$$x^p + y^q + z^r = 0$$

has finitely many (10) solutions (x^p, y^q, z^r) in non-zero coprime integers x, y, and z and $p, q, r \in \mathbb{Z}_{\geq 2}$ satisfying $1/p + 1/q + 1/r < 1$.

We call (p, q, r) the **signature** of the equation.

Many 'solved' cases:

- $(2,3,7)$, $(3,4,5)$, $(5,5,7)$, $\ldots$
- $\underbrace{(\ell,\ell,\ell)}_{\text{FLT}}$, $(\ell,\ell,2)$, $(4,2\ell,3)$, $\ldots$

Aim: Study

$$x^2 + y^{2\ell} = z^p,$$

where p is a fixed prime and ℓ varies + highlight the role played by modular curves.

The modular method

Suppose $x^\ell + 19y^\ell + z^\ell = 0$.

Frey curve	$E_{x,y,z,\ell} = E : Y^2 = (X - x^\ell)(X + 19y^\ell)$
Modularity $\overline{\rho}_{E,\ell}$ must be modular	All elliptic curves $/\mathbb{Q}$ are modular
Irreducibility $\overline{\rho}_{E,\ell}$ must be irreducible	$\overline{\rho}_{E,\ell}$ is irreducible by Mazur's theorem on ℓ-isogenies of elliptic curves $/\mathbb{Q}$
Level-lower $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$, a newform f $\lambda \mid \ell$ a prime of $\mathbb{Q}_f$	$\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f_1,\ell}$ or $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f_2,\ell}$ f_1, f_2 newforms at level 38
Eliminate Compare traces of Frobenius	$\mathrm{tr}(\overline{\rho}_{E,\ell}(\sigma_3)) \equiv \mathrm{tr}(\overline{\rho}_{f_i,\ell}(\sigma_3)) \pmod{\ell}$ $\Rightarrow \ell \leq 5$

Over totally real fields

Frey curve - Modularity - Irreducibility - Level-lower - Eliminate

Over a totally real field K, the same strategy works.

- Need to prove **modularity**
- Need to prove **irreducibility**
- Newforms $\rightsquigarrow$ **Hilbert** newforms

Descent

$$x^2 + y^{2\ell} = z^p$$

- Factor LHS over $\mathbb{Q}(i)$: $\quad (y^\ell + xi)(y^\ell - xi) = z^p$.
- So $y^\ell + xi = (a + bi)^p$ for some $a, b \in \mathbb{Z}$.
- Compare real and imaginary parts and factor over $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$:

$$y^\ell = \frac{(a+bi)^p + (a-bi)^p}{2}$$

$$y^\ell = a \cdot \prod_{j=1}^{(p-1)/2} \underbrace{\left((\zeta_p^j + \zeta_p^{-j} + 2)a^2 + (\zeta_p^j + \zeta_p^{-j} - 2)b^2\right)}_{\beta_j \in K}$$

- Suppose $p \nmid y$ and $\ell \neq p$. Each term on the RHS is an ℓth power.

Frey curves

We have $y^\ell = a \cdot \prod_{j=1}^{(p-1)/2} \beta_j$.

- For $p > 3$ and each β_j, β_k, there is a relation:

$$R \cdot \underbrace{\beta_j}_{\ell\text{th power}} + S \cdot \underbrace{\beta_k}_{\ell\text{th power}} + T \cdot \underbrace{a^2}_{\ell\text{th power}} = 0$$

$$R = 1, \quad S = -\frac{\zeta_p^j - \zeta_p^{-j} - 2}{\zeta_p^k - \zeta_p^{-k} - 2}, \quad T = 4\frac{\zeta_p^j + \zeta_p^{-j} + \zeta_p^k + \zeta_p^{-k}}{\zeta_p^k - \zeta_p^{-k} - 2} \in K$$

- This is an equation of signature (ℓ, ℓ, ℓ). We define a Frey curve over K:

$$E_{x,y,z,\ell} = E : \quad Y^2 = X(X - S \cdot \beta_k)(X + T \cdot a^2).$$

- If $p = 3$, we define a Frey curve over $\mathbb{Q}$:

$$E_{x,y,z,\ell} = E : \quad Y^2 = X^3 + 6b^2X^2 + 3(a^2 - 3b^2)X.$$

Suppose $\overline{\rho}_{E,\ell}$ is modular and irreducible.

$$\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}, \text{ where } \begin{cases} f \text{ is a newform at level } 288 & \text{if } p = 3, \\ f \text{ is a Hilbert newform at level } 2^3 \cdot \mathcal{O}_K & \text{if } p > 3. \end{cases}$$

Problem: We have the trivial solution $(x, y, z, \ell) = (0, \pm 1, 1, \ell)$ and

$$\overline{\rho}_{E_{\mathrm{triv}},\ell} \sim \overline{\rho}_{f_*,\ell}.$$

Consequence: We cannot eliminate the isomorphism $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f_*,\ell}$.
Solution I: Consider $x^{2\ell} + y^{2\ell} = z^p$ instead.

Theorem (B, A–S, B–C–D–D–F, M)

Let $\ell \geq 2$ and $p \in \{3, 5, 7, 11, 13, 17\}$. The equation

$$x^{2\ell} + y^{2\ell} = z^p$$

has no solutions in non-zero coprime integers x, y, and z.

Complex multiplication

Solution II: When $p = 3$, the curve $E_{\mathrm{triv}} : Y^2 = X^3 + 3X$ has complex multiplication by $\mathbb{Q}(i)$.
Consequence: If $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f_*,\ell} \sim \overline{\rho}_{E_{\mathrm{triv}},\ell}$ then

$$E \rightsquigarrow P \in \begin{cases} X^+_{\mathrm{split}}(\ell)(\mathbb{Q}) & \text{if } p \equiv 1 \pmod 4 \quad ☺ \\ X^+_{\mathrm{nonsplit}}(\ell)(\mathbb{Q}) & \text{if } p \equiv -1 \pmod 4 \quad ☹ \end{cases}$$

In fact, when $p \equiv -1 \pmod 4$:

$$E \rightsquigarrow P' \in \left(X^+_{\mathrm{nonsplit}}(\ell) \times_{X(1)} X_0(2)\right)(\mathbb{Q}) \quad ☺$$

In each case $j(E) \in \mathbb{Z}[1/\ell]$, forcing $E = E_{\mathrm{triv}}$.

- Same idea works when $\ell = p$ (for any p).

All this was in the case $p \nmid y$.

- If $p = 3$ and $3 \mid y$ we cannot eliminate an isomorphism

$$\overline{\rho}_{W,\ell} \sim \overline{\rho}_{g_*,\ell}$$

for a newform g_* at level 96 for all ℓ.

Theorem (Chen, Dahmen)

Let ℓ be a prime and suppose there exist non-zero coprime integers x, y, and z satisfying

$$x^2 + y^{2\ell} = z^3.$$

Then $3 \mid y$ and $\ell > 10^7$.

$x^2 + y^{2\ell} = z^{3p}$

Assume $p > 5$ is fixed and $p \nmid y$.

- Know $\ell > 10^7$.
- Since $3 \mid y$, the Frey curve $E_{x,y,z,\ell}/K$ has multiplicative reduction at all primes $\mathfrak{q} \mid 3$.

Assume $\overline{\rho}_{E,\ell}$ is modular and irreducible.

$\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$, where f is a Hilbert newform at level $2^3 \cdot \mathcal{O}_K$.

Compare traces of Frobenius at $\sigma_{\mathfrak{q}_3} \in G_{\mathbb{Q}}$:

$$\pm(\mathrm{Norm}(\mathfrak{q}_3) + 1) \equiv a_{\mathfrak{q}_3}(f) \pmod{\lambda}.$$

So

$$\ell \mid B_f := \mathrm{Norm}_{\mathbb{Q}(f)/\mathbb{Q}}(\mathrm{Norm}(\mathfrak{q}_3) + 1 \pm a_{\mathfrak{q}_3}(f))$$

We have

$$\ell \mid B_f := \mathrm{Norm}_{\mathbb{Q}(f)/\mathbb{Q}}\left(\mathrm{Norm}(\mathfrak{q}_3) + 1 \pm a_{\mathfrak{q}_3}(f)\right).$$

When $p = 7$:

- $B_f \in \{20, 24, 28, 32, 36\}$ and so $\ell \leq 7 < 10^7$.

When $p \geq 11$:

- it is (too) hard to compute the values $a_{\mathfrak{q}_3}(f)$...

But

$$|a_{\mathfrak{q}_3}(f)| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q}_3)}.$$

Using this,

$$\begin{aligned}\ell \mid B_f &:= \mathrm{Norm}_{\mathbb{Q}(f)/\mathbb{Q}}\left(\mathrm{Norm}(\mathfrak{q}_3) + 1 \pm a_{\mathfrak{q}_3}(f)\right)\\ &\leq \left(\mathrm{Norm}(\mathfrak{q}_3) + 1 + 2\sqrt{\mathrm{Norm}(\mathfrak{q}_3)}\right)^{[\mathbb{Q}(f):\mathbb{Q}]}\\ &= \left(1 + \sqrt{\mathrm{Norm}(\mathfrak{q}_3)}\right)^{2[\mathbb{Q}(f):\mathbb{Q}]}\\ &\leq \left(1 + \sqrt{\mathrm{Norm}(\mathfrak{q}_3)}\right)^{2d},\end{aligned}$$

where d is the dimension of the space of Hilbert newforms at level $2^3 \cdot \mathcal{O}_K$.

Example. Let $p = 17$. Then $d = 41883752$ and $\ell \leq 10^{160315410}$.

Modularity

Theorem (Freitas)

Let K be an abelian totally real number field where 3 is unramified. Let C/K be an elliptic curve semistable at all primes $\mathfrak{q}|3$. Then, C is modular.

Consequence: $\overline{\rho}_{E,\ell}$ is modular for all ℓ.

Irreducibility

Suppose $\overline{\rho}_{E,\ell}$ is reducible so that $E \rightsquigarrow P \in X_0(\ell)(K)$.

- We can bound ℓ:

$$\ell \mid \mathrm{Norm}_{K/\mathbb{Q}}(\epsilon^{12} - 1) \textbf{ or } \underbrace{\ell \leq (1 + 3^{3(p-1)h_K/2})^2}_{\text{from studying } X_1(\ell)},$$

  for ϵ a fundamental unit of K.

- When $p = 7$, we have

$$\ell \mid 15369 \textbf{ or } \ell \leq (1 + 3^9)^2 > 10^7 \ldots$$

  We have $P \equiv \text{cusp} \pmod{3 \cdot \mathcal{O}_K} \implies \ell < 65 \cdot 6^6 < 10^7$.

An asymptotic result

Theorem (M)

Let p be a prime. There exists a constant $C(p)$ such that for $\ell > C(p)$, the equation

$$x^2 + y^{2\ell} = z^{3p}$$

has no solutions in non-zero coprime integers x, y, and z.

We could take

$$C(p) = \underbrace{(\sqrt{p}+1)^2}_{p|y} \cdot \underbrace{\mathrm{Norm}_{K/\mathbb{Q}}(\epsilon^{12}-1)\cdot(1+3^{3(p-1)h_K/2})^2}_{\text{irreducibility}} \cdot \underbrace{(\sqrt{\mathrm{Norm}(\mathfrak{q}_3)}+1)^{2d}}_{\text{eliminating } \overline{\rho}_{E,\ell}\sim\overline{\rho}_{f,\lambda}}$$

The case $p = 7$

Theorem (M)

Let $\ell \geq 2$. The equation

$$x^2 + y^{2\ell} = z^{21}$$

has no solutions in non-zero coprime integers x, y, and z.