Journées Arithmétiques 2023

On differences of perfect and prime powers

Pedro-José Cazorla García

University of Manchester

4th July 2023

Catalan's conjecture

Conjecture (Catalan, 1844)

The only solution to the Diophantine equation

$$y^n - z^m = 1$$

($y, z > 0$ and $n, m > 1$) is given by

$$(y, z, n, m) = (3, 2, 2, 3).$$

Catalan's conjecture

Conjecture (Catalan, 1844)

The only solution to the Diophantine equation

$$y^n - z^m = 1$$

($y, z > 0$ and $n, m > 1$) is given by

$$(y, z, n, m) = (3, 2, 2, 3).$$

Open for many years, and finally proved by **Mihăilescu** in 2002

A natural generalisation

Question:

Can we solve

$$y^n - z^m = D$$

for an arbitrary $D > 0$?

A natural generalisation

Question:

Can we solve

$$y^n - z^m = D$$

for an arbitrary $D > 0$?

Answer:

We do not even know if it has **finitely many** solutions!

What we can solve

Question:

Can we solve

$$y^n - q^\alpha = C_1 x^2$$

where q is a fixed prime number and C_1 is a fixed positive squarefree integer?

What we can solve

Question:

Can we solve

$$y^n - q^\alpha = C_1 x^2$$

where q is a fixed prime number and C_1 is a fixed positive squarefree integer?

Answer:

Yes!

What we can solve

Question:

Can we solve

$$y^n - q^\alpha = C_1 x^2$$

where q is a fixed prime number and C_1 is a fixed positive squarefree integer?

Answer:

Yes! The equation

$$C_1 x^2 + q^\alpha = y^n$$

is a particular case of the **generalised Lebesgue–Nagell equation**, which has been studied extensively (most recently by Bennett-Siksek in 2022).

Strategy

Our equation

$$C_1 x^2 + q^\alpha = y^n$$

Strategy

Our equation

$$C_1x^2 + q^\alpha = y^n$$

For the rest of the talk, we assume that y is even.

Strategy

Our equation

$$C_1 x^2 + q^\alpha = y^n$$

For the rest of the talk, we assume that y is even.

1. Bound n, so that $n < N_0(C_1, q)$.
2. Solve for each outstanding value of n.

Strategy: bound n

Our equation

$$C_1x^2 + q^\alpha = y^n$$

1. Bound n, so that $n < N_0(C_1, q)$. Two techniques:

Strategy: bound n

Our equation

$$C_1 x^2 + q^\alpha = y^n$$

1. Bound n, so that $n < N_0(C_1, q)$. Two techniques:
   - Linear forms in logarithms ($q-$adic and complex): They always work, but the bound is quite bad.

Strategy: bound n

Our equation

$$C_1x^2 + q^\alpha = y^n$$

1. Bound n, so that $n < N_0(C_1, q)$. Two techniques:
   - Linear forms in logarithms ($q-$adic and complex): They always work, but the bound is quite bad.
   - Modular method: does not always work but bound is sharp.

Strategy: solve for fixed n

Our equation

$$C_1x^2 + q^\alpha = y^n$$

2. Solve for each outstanding value of n.

Strategy: solve for fixed n

Our equation

$$C_1 x^2 + q^\alpha = y^n$$

2. Solve for each outstanding value of n.
    - Thue–Mahler equations (Gherga-Siksek, 2022): useful in theory, impractical for large ($n > 11$) exponents.

Strategy: solve for fixed n

Our equation

$$C_1 x^2 + q^\alpha = y^n$$

2. Solve for each outstanding value of n.

   - Thue–Mahler equations (Gherga-Siksek, 2022): useful in theory, impractical for large ($n > 11$) exponents.
   - Modular method: can be applied for all exponents $n > 5$, but **fails if there are solutions**.

The modular method in a nutshell

$$C_1 x^2 + q^\alpha = y^n$$

The modular method in a nutshell

$$C_1 x^2 + q^\alpha = y^n$$

Following Bennett and Skinner (2004), We define F via:

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

This is an **elliptic curve**, which we shall call the **Frey curve**.

Modular method continued

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

This is an **elliptic curve**, which we shall call the **Frey curve**.

Modular method continued

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

This is an **elliptic curve**, which we shall call the **Frey curve**.

By the modularity theorem (Wiles, Conrad, Diamond, Taylor, Breuil, 2001) and Ribet's Level Lowering Theorem (1986), it follows that

$$\overline{\rho}_n(F) \cong \overline{\rho}_n(f)$$

for some $f \in S_2^{new}(\Gamma_0(N))$.

Modular method continued

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

This is an **elliptic curve**, which we shall call the **Frey curve**.

By the modularity theorem (Wiles, Conrad, Diamond, Taylor, Breuil, 2001) and Ribet's Level Lowering Theorem (1986), it follows that

$$\overline{\rho}_n(F) \cong \overline{\rho}_n(f)$$

for some $f \in S_2^{new}(\Gamma_0(N))$.

Aim: Show that, for all f, there exists some ℓ such that

$$\overline{\rho}_n(F)(Frob_\ell) \neq \overline{\rho}_n(f)(Frob_\ell).$$

A key lemma

Lemma

Let $\ell = 2kn + 1$ *be prime (+ some other conditions). Then,* $\overline{\rho}_n(F)(Frob_\ell)$ *depends only on:*

- *The residue class of* $q \pmod{\ell}$.
- *The residue class of* $\alpha \pmod{2n}$, *which we shall denote by* β.
- *Some* $\omega \in \{0, 1, \ldots, \ell - 1\}$ *satisfying:*

$$(C_1\omega^2 + q^\beta)^{2k} \equiv 1 \pmod{\ell}.$$

A key lemma

Lemma

Let $\ell = 2kn + 1$ *be prime (+ some other conditions). Then,* $\overline{\rho}_n(F)(Frob_\ell)$ *depends only on:*

- *The residue class of* $q \pmod{\ell}$*.*
- *The residue class of* $\alpha \pmod{2n}$*, which we shall denote by* β*.*
- *Some* $\omega \in \{0, 1, \ldots, \ell - 1\}$ *satisfying:*

$$(C_1\omega^2 + q^\beta)^{2k} \equiv 1 \pmod{\ell}.$$

Computing all the possibilities for $\overline{\rho}_n(F)(Frob_\ell)$ is now a finite computation, so we can find an ℓ proving that

$$\overline{\rho}_n(F)(Frob_\ell) \neq \overline{\rho}_n(f)(Frob_\ell).$$

Conclusions

With all the described methodology, we are able to prove that

Theorem (C-G, 2023+)

We can find all solutions to

$$C_1 x^2 + q^\alpha = y^n,$$

where $1 \leq C_1 \leq 20$ is squarefree and $2 \leq q < 25$ is prime.

Conclusions

With all the described methodology, we are able to prove that

Theorem (C-G, 2023+)

We can find all solutions to

$$C_1 x^2 + q^\alpha = y^n,$$

where $1 \leq C_1 \leq 20$ is squarefree and $2 \leq q < 25$ is prime.

This is "maximal" because:

$$21 \cdot 79^2 + 11^1 = 2^{17}$$

$$3 \cdot 209^2 + 29^1 = 2^{17}.$$

Icebreaker


Did you know that 8 and 9 are the only consecutive perfect powers?
Cool!

Any questions?