The modular approach for solving $\mathbf{x^r + y^r = z^p}$

Cambridge, September 2023

Diana Mocanu, University of Warwick

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}. \tag{1}$$

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}. \tag{1}$$

Conjecture(Fermat-Catalan)

Over all choices of prime exponents p, q, r satisfying $1/p + 1/q + 1/r < 1$ the equation (1) admits only finitely many integer solutions (a, b, c) which are non-trivial (i.e. $abc \neq 0$) coprime (i.e. $\gcd(a, b, c) = 1$). (Here solutions like $2^3 + 1^q = 3^2$ are counted only once.)

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

Theorem(Darmon-Granville 1995)

If we fix the prime exponents p, q, r such that $1/p + 1/q + 1/r < 1$, then there are only finitely many coprime integers solutions to the above equation.

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

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

Introduction

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

We call (p, q, r) **the signature** of the equation.
Families of signatures that have been 'solved':

- $(n, n, n), n \geq 3$ Wiles, Taylor–Wiles 1995;
- $(n, n, 2), n \geq 4$ and $(n, n, 3), n \geq 3$ Darmon–Merel, Poonen 1998;
- $(3j, 3k, n), j, k \geq 2, n \geq 3$ Kraus 1998;
- $(2n, 2n, 5), n \geq 2$ Bennett 2006;
- $(5, 5, 7), (5, 5, 19)$, and $(7, 7, 5)$ Dahmen, Siksek 2014;
- $(5, 5, n)$* Billerey, Chen, Dembélé, Dieulefait and Freitas 2022;
- $(11, 11, n)$*,$(13, 13, n)$* Billerey, Chen, Dieulefait, Freitas and Najman 2022.

Asymptotic (r, r, p)

Today: $x^r + y^r = z^p$ where $r \geq 5$ is fixed and p varies.

Asymptotic (r, r, p)

Today: $x^r + y^r = z^p$ where $r \geq 5$ is fixed and p varies.

Theorem (M.)

Fix $r \geq 5$ such that $r \not\equiv 1 \mod 8$. Let $\mathbb{Q}^+ := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, suppose that 2 is inert in $\mathbb{Q}^+$ and $2 \nmid h^+_{\mathbb{Q}^+}$. Then, there is a constant B_r (depending only on r) such that for each rational prime $p > B_r$, the equation $x^r + y^r = z^p$ has no integer solutions with $2 | z$.

Asymptotic (r, r, p)

Today: $x^r + y^r = z^p$ where $r \geq 5$ is fixed and p varies.

Theorem (M.)

Fix $r \geq 5$ such that $r \not\equiv 1 \mod 8$. Let $\mathbb{Q}^+ := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, suppose that 2 is inert in $\mathbb{Q}^+$ and $2 \nmid h^+_{\mathbb{Q}^+}$. Then, there is a constant B_r (depending only on r) such that for each rational prime $p > B_r$, the equation $x^r + y^r = z^p$ has no integer solutions with $2 | z$.

Example

This implies that there are no integer solutions (x, y, z) with $2|z$ for p large enough for signatures:

$$(5, 5, p), (7, 7, p), (11, 11, p), (13, 13, p), (19, 19, p), (23, 23, p), (37, 37, p), (43, 43, p).$$

Modular Method - Sketch

Modular Method - Sketch

Step 1: Select a Frey curve.
Suppose we have $x, y, z \in \mathbb{Z}$, non-trivial, coprime with $x^p + y^p = z^p$. We construct the following Frey Curve:

$$E/\mathbb{Q} : Y^2 = X(X - x^p)(X + y^p)$$

which has Artin conductor $N_p = 2$.

Modular Method - Sketch

Step 1: Select a Frey curve.
Suppose we have $x, y, z \in \mathbb{Z}$, non-trivial, coprime with $x^p + y^p = z^p$. We construct the following Frey Curve:

$$E/\mathbb{Q} : Y^2 = X(X - x^p)(X + y^p)$$

which has Artin conductor $N_p = 2$.

Step 1: Select a Frey curve.
Suppose we have $x, y, z \in \mathbb{Z}$, non-trivial, coprime with $x^r + y^r = z^p$ and $2|z$. We construct a Frey elliptic curve over **the totally real** number field $\mathbb{Q}^+$:

$$E_{x,y,z} : Y^2 = X(X - A)(X + B) \qquad (2)$$

defined over the totally real number field $\mathbb{Q}^+ := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$. The Artin conductor of E is

$$\mathcal{N}_p = 2^{e_2}\mathfrak{P}_r^{e_r}.$$

Modular Method - Sketch

Step 2: Modularity. Wiles, Taylor-Wiles (1995) proved Modularity of semistable elliptic curves over $\mathbb{Q}$.

$$E \rightsquigarrow f$$

where f is a newform of weight 2 and level N, where N is the conductor of E.

Modular Method - Sketch

Step 2: Modularity. Wiles, Taylor-Wiles (1995) proved Modularity of semistable elliptic curves over $\mathbb{Q}$.

$$E \rightsquigarrow f$$

where f is a newform of weight 2 and level N, where N is the conductor of E.

Step 2: Modularity.
Freitas, Hung and Siksek (2013) proved Modularity of elliptic curves over totally real fields (up to a finite number of exceptions).

$$E \rightsquigarrow \mathfrak{f}$$

where $\mathfrak{f}$ is a Hilbert newform of parallel weight 2 and level $\mathcal{N}$, where $\mathcal{N}$ is the conductor of E

Modular Method - Sketch

Step 3: Irreducibility.
The representation $\overline{\rho}_{E,p}$ is irreducible by a Theorem due to Mazur (1978).

Modular Method - Sketch

Step 3: Irreducibility.
The representation $\overline{\rho}_{E,p}$ is irreducible by a Theorem due to Mazur (1978).

Step 3: Irreducibility.
Freitas and Siksek (2015) proved irreducibility of $\overline{\rho}_{E,p}$ for elliptic curves E over totally real number fields under a few technical assumptions, **if p is large enough**.

Modular Method - Sketch

Step 4: Level Lowering

Ribet's Level Lowering Theorem (1986) implies that there exists a rational newform f of level $N_p = 2$ and weight 2 such that $E \sim_p f$.

Modular Method - Sketch

Step 4: Level Lowering
Ribet's Level Lowering Theorem (1986) implies that there exists a rational newform f of level $N_p = 2$ and weight 2 such that $E \sim_p f$.

Step 4: Level lowering. Use level lowering theorems, which require irreducibility of $\overline{\rho}_{E,p}$, to conclude that

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

where $\mathfrak{f}$ is a Hilbert newform over $\mathbb{Q}^+$ of parallel weight 2, of trivial character, and rational Hecke eigenvalues, with level equal to the Artin conductor $\mathcal{N}_p$ of E.

Level Lowering

Step 5: Eliminate
Simply there are no newforms at level $N_p = 2$, hence giving the desired contradiction.

Level Lowering

Step 5: Eliminate
Simply there are no newforms at level $N_p = 2$, hence giving the desired contradiction.

Step 5: Eliminate
Prove that among the finitely many Hilbert newforms predicted above, none of them corresponds to $\bar{\rho}_{E,p}$ and get the desired **contradiction.**

Modular Method - Step 5

Step 5 is challenging in general.

Example

The approach we used:

1. an 'Eichler-Shimura'-type result;
2. image of inertia comparison arguments;
3. the study of certain S-unit equations;

to get a contradiction.

Modular Method - Recap

Recap steps 1,2,3,4:
Assuming we have a (non-trivial, primitive) solution

$$(x, y, z) \text{ to } x^r + y^r = z^p \text{ with } 2|z \quad + \quad \text{some class field theoretic assumptions}$$

Modular Method - Recap

Recap steps 1,2,3,4:
Assuming we have a (non-trivial, primitive) solution

$$(x, y, z) \text{ to } x^r + y^r = z^p \text{ with } 2|z \quad + \quad \text{some class field theoretic assumptions}$$

Step 1 $(x, y, z) \rightsquigarrow E_{x,y,z}$, Frey elliptic curve

Modular Method - Recap

Recap steps 1,2,3,4:
Assuming we have a (non-trivial, primitive) solution

$$(x,y,z) \text{ to } x^r + y^r = z^p \text{ with } 2|z \quad + \quad \text{some class field theoretic assumptions}$$

Step 1 $(x,y,z) \rightsquigarrow E_{x,y,z}$, Frey elliptic curve
Steps 2,3,4 Get a Hilbert newform $\mathfrak{f}$, of level $\mathcal{N}_p$, such that

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

Modular Method - Step 5

1. **Eichler-Shimura** gives an elliptic curve E' with conductor $\mathcal{N}_p$ such that

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

.

Modular Method - Step 5

1. **Eichler-Shimura** gives an elliptic curve E' with conductor $\mathcal{N}_p$ such that

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

.

2. **Image of inertia comparison** at the bad prime 2 gives $v_2(j_{E'}) < 0$.

Modular Method - Step 5

1. **Eichler-Shimura** gives an elliptic curve E' with conductor $\mathcal{N}_p$ such that

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

   .

2. **Image of inertia comparison** at the bad prime 2 gives $v_2(j_{E'}) < 0$.
3. Elliptic curves E' with such properties are parametrized by S-unit equations. By **finiteness of solutions** to S-unit equations $+$ the class field theoretic assumptions we get the contradiction.

Modular Method

Select a Frey Curve - **M**odularity - **I**rreducibility - **L**evel lowering - **E**liminate

Thank you!