Variants of the modular method

YRANT, 2024

Diana Mocanu, University of Warwick

Introduction

Generalized Fermat Equation:

$$a^p + b^q = c^r, \quad p, q, r \text{ primes.}$$

A solution $(a, b, c) \in \mathbb{Z}^3$ is called **non-trivial** if $abc \neq 0$ and **primitive** if $\gcd(a, b, c) = 1$.

Introduction

Generalized Fermat Equation:

$$a^p + b^q = c^r, \quad p, q, r \text{ primes.}$$

A solution $(a, b, c) \in \mathbb{Z}^3$ is called **non-trivial** if $abc \neq 0$ and **primitive** if $\gcd(a, b, c) = 1$.

Conjecture(Fermat-Catalan)

Over all choices of prime exponents p, q, r satisfying $1/p + 1/q + 1/r < 1$ the above equation has only finitely many (10) integer solutions (a, b, c) which are non-trivial and primitive. (Here solutions like $2^3 + 1^q = 3^2$ are counted only once.)

Introduction

Generalized Fermat Equation:

$$a^p + b^q = c^r, \quad p, q, r \text{ primes } \geq 2.$$

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

Introduction

Generalized Fermat Equation:

$$a^p + b^q = c^r, \quad p, q, r \text{ primes } \geq 2.$$

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

- $(p, p, p), p \geq 3$ Wiles, Taylor–Wiles 1995;
- $(p, p, 2), p \geq 4$ and $(p, p, 3), p \geq 3$ Darmon–Merel, Poonen 1998;
- $(11, 11, p)^*, p \geq 2$, Billerey, Chen, Dieulefait, Freitas 2022 (BCDF22);
- $(13, 13, p)^*, (19, 19, p)^*, (23, 23, p)^*, (37, 37, p)^*, (43, 43, p)^*, p$ large enough M. 2022.

The Modular Method-Sketch

Assume $a^p + b^p = c^p$ with (a, b, c) non-trivial and $p > 7$.

Select a Frey curve	$E(a,b) : y^2 = x(x - a^p)(x + b^p)$, $\Delta_E = 2^4(abc)^{2p}, N_E = 2 \prod_{q\mid abc} q$
Modularity	Wiles: All rational semistable elliptic curves are modular $\Rightarrow \bar{\rho}_{E,l} \cong \bar{\rho}_{f,l}, \forall l$ for some newform f of weight 2 and level N_E
Irreducibility	Mazur's Theorem on Isogenies: $\bar{\rho}_{E,p}$ is irreducible for $p > 7$
Level Lowering	Ribet: $\bar{\rho}_{E,p} \cong \bar{\rho}_{g,p}$ for some newform g of weight 2 and level $N_p = N_E / \prod_{\substack{q \mid\mid N_E \\ p \mid \mathrm{ord}_q(\Delta_E)}} q = 2$
Eliminate	There are no newforms at level 2

New Directions - Darmon Program

- Limited number of instances of generalized Fermat equations possessing Frey elliptic curves $/\mathbb{Q}$ associated with them - known to Darmon from 1997

New Directions - Darmon Program

- Limited number of instances of generalized Fermat equations possessing Frey elliptic curves $/\mathbb{Q}$ associated with them - known to Darmon from 1997

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

Signature (r, r, p) via Darmon's program

Assume $a^r + b^r = c^p$ with (a, b, c) primitive, non-trivial, r is a fixed prime, and p is a varying prime.

Signature (r, r, p) via Darmon's program

Assume $a^r + b^r = c^p$ with (a, b, c) primitive, non-trivial, r is a fixed prime, and p is a varying prime.

- **Step 1:** Kraus constructs a Frey hyperelliptic curve $C_r(a, b)/\mathbb{Q}$, of genus $\frac{r-1}{2}$.
- Let $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, $J_r :=$ Jac$(C_r(a, b))/K$
- Today: Compute the conductor of $C_r(a, b)/K$ = Artin conductor of $\rho_{J_r,l}$.

Signature (r, r, p) via Darmon's program

Assume $a^r + b^r = c^p$ with (a, b, c) primitive, non-trivial, r is a fixed prime, and p is a varying prime.

- **Step 1:** Kraus constructs a Frey hyperelliptic curve $C_r(a, b)/\mathbb{Q}$, of genus $\frac{r-1}{2}$.
- Let $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, $J_r := \text{Jac}(C_r(a, b))/K$
- Today: Compute the conductor of $C_r(a, b)/K$ = Artin conductor of $\rho_{J_r,l}$.
- BCDF22 $\rightsquigarrow \forall l$ of good reduction, $\rho_{J_r,l} \cong \bigoplus_{\mathfrak{l}|l} \rho_{J_r,\mathfrak{l}}$, where

$$\overline{\rho}_{J_r,\mathfrak{l}} : G_K \to GL_2(\mathbb{F}_{\mathfrak{l}}).$$

- **Steps 2,3,4** apply to $\overline{\rho}_{J_r,\mathfrak{l}}$.
- BCDF22 $\rightsquigarrow (11, 11, p)$ has no solution with $2|a+b$ or $11|a+b$.

Kraus' Frey hyperelliptic curves

Given primitive, non-trivial $(a, b, c) \in \mathbb{Z}^3$ such that $a^r + b^r = c^p$ define

$$C_r(a, b) : y^2 = \underbrace{(ab)^{(r-1)/2} x h_r\left(\frac{x^2}{ab} + 2\right) + b^r - a^r}_{f_r(a,b)}$$

where $h_r(x) := \prod_{j=1}^{\frac{r-1}{2}} (x - (\zeta_r^j + \zeta_r^{-j}))$ the defining polynomial of $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$.

- $C_r(a, b)$ is a hyperelliptic curve of genus $\frac{r-1}{2}$.

Kraus' Frey hyperelliptic curves

Given primitive, non-trivial $(a, b, c) \in \mathbb{Z}^3$ such that $a^r + b^r = c^p$ define

$$C_r(a,b) : y^2 = \underbrace{(ab)^{(r-1)/2} x h_r\left(\frac{x^2}{ab} + 2\right) + b^r - a^r}_{f_r(a,b)}$$

where $h_r(x) := \prod_{j=1}^{\frac{r-1}{2}} (x - (\zeta_r^j + \zeta_r^{-j}))$ the defining polynomial of $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$.

- $C_r(a,b)$ is a hyperelliptic curve of genus $\frac{r-1}{2}$.

Example

- $r = 5 : C_5(a,b) : y^2 = x^5 + 5abx^3 + 5a^2b^2x + b^5 - a^5$
- $r = 7 : C_7(a,b) : y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7$

Frey Curve and Conductor

The discriminant of the curve is

$$\Delta(C_r(a,b)) = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r c^{p(r-1)}.$$

Frey Curve and Conductor

The discriminant of the curve is

$$\Delta(C_r(a,b)) = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r c^{p(r-1)}.$$

Theorem (M3DC (⋆))

The conductor of $C_r(a,b)/K$ (equivalently the Artin conductor of $\rho_{J_r,l}$) at odd primes is

$$\mathcal{N} = 2^{e_2} \mathfrak{p}_r^{r-1} \prod_{\mathfrak{q}|c} \mathfrak{q}^{(r-1)/2}.$$

In particular, J_r is semistable at all primes not dividing $2r$.

(⋆) joint work with Martin Azon, Mar Curcó-Iranzo, Maleeha Khawaja, Celine Maistret

Cluster Pictures

Definition

Let p be an odd prime, K a p-adic field and C/K a hyperelliptic curve of genus g given by

$$y^2 = f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n).$$

Let $\mathcal{R} = \{a_1, \cdots, a_n\}$ denote the set of roots of f . Let $\mathfrak{p}$ be the unique prime of $\mathcal{O}_K$. We define the cluster picture Σ_p associated to C with respect to p as

$$\Sigma_p := \{\mathfrak{s} \in \mathcal{P}(\mathcal{R}) | = D_{z,d} \cap \mathcal{R} \text{ for some } z \in \bar{K}, d \in \mathbb{Q}\}$$

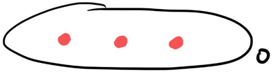
where $D_{z,d} := \{x \in \bar{K} | v_{\mathfrak{p}}(x-z) \geq d\}$.

- In short, Σ_p are the subsets of $\mathcal{R}$ which are cut out by bounded p-adic discs in K.

Cluster Pictures

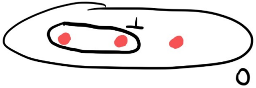
$p > 3$ prime

$E : y^2 = x(x-p+1)(x-p+2)$



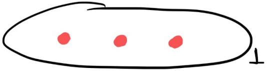
$\Rightarrow$ good reduction

$E : y^2 = x(x-p)(x-p+1)$



$\Rightarrow$ multiplicative reduction

$E : y^2 = x(x-p)(x-p^2)$



$\Rightarrow$ additive reduction

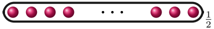
Cluster Pictures

Recall $C_r(a,b)/K : y^2 = f_r(a,b)$.

- The roots of $f_r(a,b)$ are given by $\alpha_i := \zeta_r^i a - \zeta_r^{-i} b$, where $i = 0, \ldots, r-1$.

Cluster Pictures

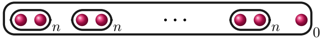
Recall $C_r(a,b)/K : y^2 = f_r(a,b)$.

- The roots of $f_r(a,b)$ are given by $\alpha_i := \zeta_r^i a - \zeta_r^{-i} b$, where $i = 0, \dots, r-1$.
- The cluster pictures of $C_r(a,b)$ at odd bad primes $\mathfrak{q}$ of K are given as follows:
    1. , if $\mathfrak{q} \neq \mathfrak{p}_r$ and $\mathfrak{q} \mid c$. Here $n := p v_{\mathfrak{q}}(c) \in \mathbb{Z}$.
    2. , if $\mathfrak{q} = \mathfrak{p}_r$ and $\mathfrak{p}_r \nmid c$.
    3. , if $\mathfrak{q} = \mathfrak{p}_r$ and $\mathfrak{p}_r \mid c$. Here $m = \frac{r-1}{2} v_r(a+b) - \frac{1}{2}$.

  where $\mathfrak{p}_r$ is the unique prime above r in K.

Conductor from the Cluster Picture

Semistable case: $\mathfrak{q} \neq \mathfrak{p}_r, \mathfrak{q}|c$



Theorem (Dokchitser–Dokchitser–Maistret–Morgan, 2017)

Suppose C/K is semistable at a prime $\mathfrak{q}$. Then the exponent of the conductor at $\mathfrak{q}$ is the number of "twins".

Conductor from the Cluster Picture

Semistable case: $\mathfrak{q} \neq \mathfrak{p}_r, \mathfrak{q} | c$

Theorem (Dokchitser–Dokchitser–Maistret–Morgan, 2017)

Suppose C/K is semistable at a prime $\mathfrak{q}$. Then the exponent of the conductor at $\mathfrak{q}$ is the number of "twins".

$\rightsquigarrow$ exponent of $\mathfrak{q}$ in the conductor is $\frac{r-1}{2}$

Conductors from the Cluster Pictures

Using a more general Theorem from DDMM17 $\rightsquigarrow$ the Artin conductor associated to $\rho_{J_r,l}$

$$\mathcal{N} = 2^{e_2}\mathfrak{p}_r^{r-1}\prod_{\mathfrak{q}|c}\mathfrak{q}^{(r-1)/2}.$$

Thank you!

Signature (r, r, p): Step 1

Theorem (Billerey–Chen–Dieulefait–Freitas, 2022)

Let p be a rational prime. There is a compatible system of K-rational Galois representations associated with J_r

$$\rho_{J_r,\mathfrak{p}} : G_K \to GL_2(K_\mathfrak{p})$$

indexed by the prime ideals $\mathfrak{p}|p$ in $\mathcal{O}_K$.

Signature (r, r, p): Step 1

Theorem (Billerey–Chen–Dieulefait–Freitas, 2022)

Let p be a rational prime. There is a compatible system of K-rational Galois representations associated with J_r

$$\rho_{J_r,\mathfrak{p}} : G_K \to GL_2(K_\mathfrak{p})$$

indexed by the prime ideals $\mathfrak{p}|p$ in $\mathcal{O}_K$.

- They show that J_r is of $\mathrm{GL}_2(K)$-type, i.e. there is an embedding $K \hookrightarrow \mathrm{End}_K(J_r) \otimes_\mathbb{Z} \mathbb{Q}$, $[K : \mathbb{Q}] = \frac{r-1}{2} = \dim(J_r) = g$.
- Moreover, $\rho_{J_r,p} \cong \bigoplus_{\mathfrak{p}|p} \rho_{J_r,\mathfrak{p}}$, where $\rho_{J_r,p}$ is the dimension $2g = (r-1)$ representation corresponding to the action of G_K on the $J_r[p]$
- The proof uses Darmon's construction of Frey representations of signature (p, p, r).

Signature (r, r, p): Steps 2,3

Theorem (Modularity, BCDF22)

The abelian variety J_r/K is modular (for any prime $r \geq 3$), i.e. there exists a Hilbert newform $\mathfrak{f}$ of parallel weight 2 and conductor $\mathcal{N}$ such that the representation $\overline{\rho}_{J_r,\mathfrak{p}} : G_K \to GL_2(\mathbb{F}_p)$ satisfies $\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{\mathfrak{f},\mathfrak{P}}$ for all primes p (where $\mathfrak{p}|p$ in K and $\mathfrak{P}|p$ in $K_{\mathfrak{f}}$).

Signature (r, r, p): Steps 2,3

Theorem (Modularity, BCDF22)

The abelian variety J_r/K is modular (for any prime $r \geq 3$), i.e. there exists a Hilbert newform $\mathfrak{f}$ of parallel weight 2 and conductor $\mathcal{N}$ such that the representation $\overline{\rho}_{J_r,\mathfrak{p}} : G_K \to GL_2(\mathbb{F}_p)$ satisfies $\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{\mathfrak{f},\mathfrak{P}}$ for all primes p (where $\mathfrak{p}|p$ in K and $\mathfrak{P}|p$ in $K_{\mathfrak{f}}$).

Theorem (Irreducibility, BCDF22)

Assume that $r \not\equiv 1 (\text{mod } 4)$ and that $r \nmid a+b$. Then, for all primes $p \neq 2$ and all $\mathfrak{p}|p$ in K, the representation $\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible