Conductor computations for the modular method via cluster pictures

Warwick, December 2023

Diana Mocanu, University of Warwick

Introduction

Generalized Fermat Equation:

$$a^p + b^q = c^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

We call (p, q, r) **the signature** of the equation. A solution (a, b, c) is called **non-trivial** if $abc \neq 0$ and primitive if $\gcd(a, b, c) = 1$.

Introduction

Generalized Fermat Equation:

$$a^p + b^q = c^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}.$$

We call (p, q, r) **the signature** of the equation. A solution (a, b, c) is called **non-trivial** if $abc \neq 0$ and primitive if $\gcd(a, b, c) = 1$.
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;
- $(2l, 2n, p), p \geq 2$ Anni, Siksek 2016;
- $(11, 11, p)^*$, Billerey, Chen, Dieulefait, Freitas 2022 (BCDF22);
- $(13, 13, p)^*, (19, 19, p)^*, (23, 23, p)^*, (37, 37, p)^*, (43, 43, p)^*$ M. 2022.
- $a^r + b^r = dc^{p*}$, $r \geq 5$ and infinitely many $d \neq 1$, Freitas, Najman 2022.

The Modular Method-Sketch

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

Select a Frey curve	$E(a,b) : y^2 = x(x - a^p)(x + b^p)$, $N_E = 2 \prod_{q \mid abc} q$
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 level N_E
Irreducibility	Mazur's Theorem on Isogenies: $\bar{\rho}_{E,p}$ is irreducible
Level Lowering	Ribet: $\bar{\rho}_{E,p} \cong \bar{\rho}_{g,p}$ for some newform g of level $N_p = 2$
Eliminate	There are no newforms at level 2

☺

New Directions - Darmon Program

- Limited number of instances of generalized Fermat equations possessing Frey elliptic curves associated with them - known to Darmon from 1997

New Directions - Darmon Program

- Limited number of instances of generalized Fermat equations possessing Frey elliptic curves associated with them - known to Darmon from 1997

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

Signature (r, r, p)

Assume $a^r + b^r = c^p$ with (a, b, c) primitive, non-trivial.

- Let $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$ and $\mathfrak{p}_r$ the unique prime above r in K.
- Kraus constructs a Frey hyperelliptic curve $C_r(a, b)/K$.
- $J_r := \mathrm{Jac}(C_r(a, b))/K$, BCDF22 $\rightsquigarrow \rho_{J_r,l} \cong \bigoplus_{\mathfrak{l}|l} \rho_{J_r,\mathfrak{l}}$.

Select a Frey curve	$C_r(a, b)/K$, $\mathcal{N} := 2^{e_2}\mathfrak{p}_r^2 \prod_{\mathfrak{q}\mid c} \mathfrak{q}$
Modularity	$\overline{\rho}_{J_r,\mathfrak{l}} : G_K \to GL_2(\mathbb{F}_l), \forall l$ is modular $\Rightarrow \overline{\rho}_{J_r,\mathfrak{l}} \simeq \overline{\rho}_{\mathfrak{f},\mathfrak{L}}$, for some Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}$
Irreducibility	$\overline{\rho}_{J_r,\mathfrak{p}}$ is absolutely irreducible (under some assumptions on r)
Level Lowering	$\overline{\rho}_{J_r,\mathfrak{p}} \simeq \overline{\rho}_{\mathfrak{g},\mathfrak{P}}$ for some Hilbert newform $\mathfrak{g}$ of level $\mathcal{N}_p := 2^2\mathfrak{p}_r^2$
Eliminate	Compare traces of Frobenius

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 $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$.

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 $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$.
The discriminant of the curve is

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

In particular, it defines a hyperelliptic curve of genus $\frac{r-1}{2}$.

Frey Curve and Conductor

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

Example

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

Theorem (BCDF22,M3DC)

The common conductor of the compatible system $\rho_{J_r,\mathfrak{p}}$ is

$$\mathcal{N} := 2^{e_2}\mathfrak{p}_r^2 \prod_{\mathfrak{q}|c} \mathfrak{q}.$$

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

Remark: BCDF22 shows that $e_2 = 2$.

Cluster Pictures

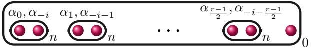
Recall $C_r(a,b)/K : y^2 = f_r(a,b)$.

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

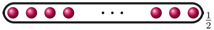
Cluster Pictures

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 $i = 0, \ldots, r-1$.
- 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 $n := pv_{\mathfrak{q}}(c) \in \mathbb{Z}$.

2. 

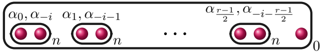
, if $\mathfrak{q} = \mathfrak{p}_r$ and $\mathfrak{q} \nmid c$.

3. 

, if $\mathfrak{q} = \mathfrak{p}_r$ and $\mathfrak{q} \mid c$. Here $m = \frac{r-1}{2} v_r(a+b) - \frac{1}{2}$.

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

$$n_{\mathfrak{q}} := \begin{cases} \#A - 1, & \textit{if } \mathcal{R} \textit{ is übereven}, \\ \#A & \end{cases}$$

where $A = \{$all even, not übereven, proper clusters$\}$.

Conductors from the Cluster Pictures

- Using a more general Theorem from DDMM17 $\Longrightarrow$ the conductor associated to $\rho_{J_r,p}$, the representation corresponding to the action of G_K on the $J_r[p]$ is

$$\mathcal{N}' = 2^{e'_2}\mathfrak{p}_r^{r-1}\prod_{\mathfrak{q}|c}\mathfrak{q}^{(r-1)/2}$$

Conductors from the Cluster Pictures

- Using a more general Theorem from DDMM17 $\Longrightarrow$ the conductor associated to $\rho_{J_r,p}$, the representation corresponding to the action of G_K on the $J_r[p]$ is

$$\mathcal{N}' = 2^{e'_2}\mathfrak{p}_r^{r-1}\prod_{\mathfrak{q}|c}\mathfrak{q}^{(r-1)/2}$$

- Since $\rho_{J_r,p} \cong \bigoplus_{\mathfrak{p}|p}\rho_{J_r,\mathfrak{p}} \Rightarrow \mathcal{N}' = \mathcal{N}^{\frac{r-1}{2}}$

Conductors from the Cluster Pictures

- Using a more general Theorem from DDMM17 $\Longrightarrow$ the conductor associated to $\rho_{J_r,p}$, the representation corresponding to the action of G_K on the $J_r[p]$ is

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

- Since $\rho_{J_r,p} \cong \bigoplus_{\mathfrak{p}|p}\rho_{J_r,\mathfrak{p}} \Rightarrow \mathcal{N}' = \mathcal{N}^{\frac{r-1}{2}}$
- $\mathcal{N} := 2^{e_2}\mathfrak{p}_r^2\prod_{\mathfrak{q}|c}\mathfrak{q}$

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 $r \not\equiv 1 (mod\ 4)$ 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