Diophantine Equations using the Modular Approach

Diana Mocanu, University of Warwick

Tue 22$^{\text{nd}}$ Oct, 2024

Outline

WARWICK

1. Introduction - Chapter 1
2. The Modular Method - Chapter 2
3. Signatures $(p, p, 2)$ and $(p, p, 3)$ - Chapter 3
4. Signature (r, r, p) - Chapter 4
5. First step in Darmon's Program - Chapter 5

WARWICK

Introduction - Chapter 1

Introduction

WARWICK

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

WARWICK

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 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.

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 - Chapter 2

Asymptotic Fermat Last Theorem

Let K be a totally real number field. We say the **asymptotic Fermat Last Theorem** holds for

$$a^p + b^p = c^p$$

if there is some bound B_K such that for all $p > B_K$, the equation has no non-trivial (i.e. $abc \neq 0$), primitive (i.e. $a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K = \mathcal{O}_K$) solutions $(a, b, c) \in \mathcal{O}_K^3$.

Let K be a totally real number field. We say the **asymptotic Fermat Last Theorem** holds for

$$a^p + b^p = c^p$$

if there is some bound B_K such that for all $p > B_K$, the equation has no non-trivial (i.e. $abc \neq 0$), primitive (i.e. $a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K = \mathcal{O}_K$) solutions $(a, b, c) \in \mathcal{O}_K^3$.

Theorem (Freitas-Siksek, 2014)

Let $d \geq 2$ be squarefree such that $d \equiv 3 \mod 8$. Then the effective asymptotic Fermat's Last Theorem holds over $K = \mathbb{Q}(\sqrt{d})$.

Idea: Diophantine equations $\rightsquigarrow$ S-unit equations (finetely many computable solutions)

Modular Method over totally real fields

Let K as above, denote by $\mathfrak{P}$ its unique (totally ramified) prime above 2.
Assume $a^p + b^p = c^p$ with $(a, b, c) \in (\mathcal{O}_K)^3$ non-trivial, primitive.

Modular Method over totally real fields

Let K as above, denote by $\mathfrak{P}$ its unique (totally ramified) prime above 2.
Assume $a^p + b^p = c^p$ with $(a, b, c) \in (\mathcal{O}_K)^3$ non-trivial, primitive.

- **Frey curve**:

$$E(a, b, c)/K : y^2 = x(x - a^p)(x + b^p)$$

with $\mathcal{N}_E = \mathfrak{P}^r \prod_{\substack{\mathfrak{q} | abc, \\ \mathfrak{q} \nmid 2}} \mathfrak{q}$.

Modular Method over totally real fields

Let K as above, denote by $\mathfrak{P}$ its unique (totally ramified) prime above 2.
Assume $a^p + b^p = c^p$ with $(a, b, c) \in (\mathcal{O}_K)^3$ non-trivial, primitive.

- **Frey curve**:
$$E(a, b, c)/K : y^2 = x(x - a^p)(x + b^p)$$
with $\mathcal{N}_E = \mathfrak{P}^r \prod_{\substack{\mathfrak{q} | abc, \\ \mathfrak{q} \nmid 2}} \mathfrak{q}$.
- **Modularity** (Freitas-Siksek):
elliptic curves / totally real fields $E/K \rightsquigarrow$ Hilbert modular forms of level $\mathcal{N}_E$

Modular Method over totally real fields

Let K as above, denote by $\mathfrak{P}$ its unique (totally ramified) prime above 2.
Assume $a^p + b^p = c^p$ with $(a, b, c) \in (\mathcal{O}_K)^3$ non-trivial, primitive.

- **Frey curve**:
$$E(a, b, c)/K : y^2 = x(x - a^p)(x + b^p)$$
with $\mathcal{N}_E = \mathfrak{P}^r \prod_{\substack{\mathfrak{q} \mid abc, \\ \mathfrak{q} \nmid 2}} \mathfrak{q}$.
- **Modularity** (Freitas-Siksek):
elliptic curves / totally real fields $E/K \rightsquigarrow$ Hilbert modular forms of level $\mathcal{N}_E$
- **Irreducibility**, **Level Lowering** (Freitas-Siksek): for p large enough
$E/K \rightsquigarrow$ Hilbert modular form $\mathfrak{f}$ of level
$$\mathcal{N}_p = \mathfrak{P}^{r'}, \quad 0 \leq r' \leq r \leq 14$$

.

Elimination Step

WARWICK

- **Eichler-Shimura curve:** for p large enough

$$E/K \rightsquigarrow \mathfrak{f} \rightsquigarrow E'/K$$

where E'/K elliptic curve with full 2-torsion* and $\mathcal{N}_{E'} = \mathcal{N}_p = \mathfrak{P}^{r'}$;

Elimination Step

- **Eichler-Shimura curve:** for p large enough

$$E/K \rightsquigarrow \mathfrak{f} \rightsquigarrow E'/K$$

  where E'/K elliptic curve with full 2-torsion* and $\mathcal{N}_{E'} = \mathcal{N}_p = \mathfrak{P}^{r'}$;
- **Image of inertia comparison:** E' has potentially multiplicative reduction at $\mathfrak{P}$;

Elimination Step

WARWICK

- **Eichler-Shimura curve:** for p large enough

$$E/K \rightsquigarrow \mathfrak{f} \rightsquigarrow E'/K$$

where E'/K elliptic curve with full 2-torsion* and $\mathcal{N}_{E'} = \mathcal{N}_p = \mathfrak{P}^{r'}$;
- **Image of inertia comparison:** E' has potentially multiplicative reduction at $\mathfrak{P}$;
- S-unit equations: all such elliptic curves E' are parametrized by S-unit equations

$$\lambda + \mu = 1,$$

where $S := \{\mathfrak{P}\}$, $\lambda, \mu \in \mathcal{O}_S^*$ such that

$$\max(|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|) > 8;$$

Elimination Step

WARWICK

- **Eichler-Shimura curve:** for p large enough

$$E/K \rightsquigarrow \mathfrak{f} \rightsquigarrow E'/K$$

where E'/K elliptic curve with full 2-torsion* and $\mathcal{N}_{E'} = \mathcal{N}_p = \mathfrak{P}^{r'}$;

- **Image of inertia comparison:** E' has potentially multiplicative reduction at $\mathfrak{P}$;
- S-unit equations: all such elliptic curves E' are parametrized by S-unit equations

$$\lambda + \mu = 1,$$

where $S := \{\mathfrak{P}\}$, $\lambda, \mu \in \mathcal{O}_S^*$ such that

$$\max(|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|) > 8;$$

- **Contradiction:** such pairs (λ, μ) do not exist.

Signatures $(p, p, 2)$ and $(p, p, 3)$ - Chapter 3

Signature $(p, p, 2)$

WARWICK

Theorem (M. 2021)

Let $d > 5$ be a rational prime satisfying $d \equiv 5 \mod 8$. Write $K = \mathbb{Q}(\sqrt{d})$. Then, there is a constant B_K such that for each rational prime $p > B_K$, the equation

$$a^p + b^p = c^2$$

has no coprime, non-trivial solutions $(a, b, c) \in \mathcal{O}_K^3$ with $2|b$.

Signature $(p, p, 2)$

WARWICK

Let K as above and denote by $\mathfrak{2}$ the unique (inert) prime above 2.
Assume $a^p + b^p = c^2$ with $(a, b, c) \in (\mathcal{O}_K)^3$ non-trivial, primitive and $\mathfrak{2} | b$.

- **Modularity machinery** $\rightsquigarrow$ find solutions to

$$\alpha + \beta = \gamma^2 \tag{3.1}$$

where $S = \{\mathfrak{2}\}$, $\alpha, \beta \in \mathcal{O}_S^*$, and $\gamma \in \mathcal{O}_S$ such that $|v_{\mathfrak{2}}(\frac{\alpha}{\beta})| > 6$.

Signature $(p, p, 2)$

WARWICK

Let K as above and denote by $\mathfrak{2}$ the unique (inert) prime above 2.
Assume $a^p + b^p = c^2$ with $(a, b, c) \in (\mathcal{O}_K)^3$ non-trivial, primitive and $\mathfrak{2}|b$.

- **Modularity machinery** $\rightsquigarrow$ find solutions to

$$\alpha + \beta = \gamma^2 \tag{3.1}$$

  where $S = \{\mathfrak{2}\}$, $\alpha, \beta \in \mathcal{O}_S^*$, and $\gamma \in \mathcal{O}_S$ such that $|v_{\mathfrak{2}}(\frac{\alpha}{\beta})| > 6$.
- Class Field Theory $\rightsquigarrow$ relate (3.1) to an S-unit equation

$$\lambda + \mu = 1, \tag{3.2}$$

  such that $|v_{\mathfrak{2}}(\lambda\mu)| > 4$.

Signature $(p, p, 2)$

Let K as above and denote by $\mathfrak{2}$ the unique (inert) prime above 2.
Assume $a^p + b^p = c^2$ with $(a, b, c) \in (\mathcal{O}_K)^3$ non-trivial, primitive and $\mathfrak{2}|b$.

- **Modularity machinery** $\rightsquigarrow$ find solutions to

$$\alpha + \beta = \gamma^2 \tag{3.1}$$

  where $S = \{\mathfrak{2}\}$, $\alpha, \beta \in \mathcal{O}_S^*$, and $\gamma \in \mathcal{O}_S$ such that $|v_{\mathfrak{2}}(\frac{\alpha}{\beta})| > 6$.

- Class Field Theory $\rightsquigarrow$ relate (3.1) to an S-unit equation

$$\lambda + \mu = 1, \tag{3.2}$$

  such that $|v_{\mathfrak{2}}(\lambda\mu)| > 4$.

- **Contradiction:** the only solutions to (3.2) are the so-called *irrelevant* solutions $(-1, 2), (1/2, 1/2), (2, -1)$.

Signature $(p, p, 3)$

Theorem (M. 2021)

Let d a positive, square-free satisfying $d \equiv 2 \mod 3$. Write $K = \mathbb{Q}(\sqrt{d})$ and suppose $3 \nmid h_{K(\zeta_3)}$, $3 \nmid h_K$. Then, there is a constant B_K such that for each prime $p > B_K$, the equation

$$a^p + b^p = c^3$$

has no coprime, non-trivial solutions $(a, b, c) \in \mathcal{O}_K^3$ with $3 \mid b$.

S-unit equations and computabiity

WARWICK

Theorem

Let K be a number field and S a finite set of prime ideals. Consider the equation

$$\alpha + \beta = \gamma^i,\ \alpha, \beta \in \mathcal{O}_S^*,\ \ \gamma \in \mathcal{O}_S.$$

For $i = 2, 3$, the equation has a finite number of solutions up to scaling.

Idea of the proof: break it down in several S-unit equations over some L/K

Signature (r, r, p) - Chapter 4

Signature (r, r, p)

Theorem (M. 2022)

There exists a constant B_r depending on r such that the equation

$$a^r + b^r = c^p$$

no non-trivial, primitive, integer solutions with $2 \mid c$ and $p > B_r$ for

$$r \in \{5, 7, 11, 13, 19, 23, 37, 47, 53, 59, 61, 67, 71, 79, 83, 101, 103, 107, 131, 139, 149\}.$$

Signature (r, r, p)

WARWICK

Assume $a^r + b^r = c^p$ with (a, b, c) non-trivial, primitive, r is a fixed prime, and p is a varying prime and $2 \mid c$.

- **Frey curve** Define $E(a, b)/\mathbb{Q}(\zeta_r + \zeta_r^{-1})$ as follows. Consider

$$a^r + b^r = (a + b)(a + \zeta_r b)(a + \zeta_r^2 b) \cdots (a + \zeta_r^{r-2} b)(a + \zeta_r^{r-1} b).$$

Signature (r, r, p)

Assume $a^r + b^r = c^p$ with (a, b, c) non-trivial, primitive, r is a fixed prime, and p is a varying prime and $2 \mid c$.

- **Frey curve** Define $E(a, b)/\mathbb{Q}(\zeta_r + \zeta_r^{-1})$ as follows. Consider

$$a^r + b^r = (a + b)(a + \zeta_r b)(a + \zeta_r^2 b) \cdots (a + \zeta_r^{r-2} b)(a + \zeta_r^{r-1} b).$$

Let

$$f_k(a, b) = a^2 + (\zeta_r^k + \zeta_r^{r-k})ab + b^2, \quad 0 \leq k \leq \frac{r-1}{2}.$$

Signature (r, r, p)

We find (α, β, γ) such that

$$\alpha f_{k_1} + \beta f_{k_2} + \gamma f_{k_3} = 0$$

for some suitable chosen $0 \leq k_1 < k_2 < k_3 \leq \frac{r-1}{2}$.
Write $A = \alpha f_{k_1}, B = \beta f_{k_2}, C = \gamma f_{k_3}$ and define

$$E : y^2 = x(x - A)(x + B). \tag{4.1}$$

Signature (r, r, p)

Let $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, 2 is inert for the specified values of r, and let $\mathfrak{P}_r$ be the unique prime above r.

- **Modularity machinery** $\rightsquigarrow$ find solutions to the S-unit equation

$$\lambda + \mu = 1$$

  where $S := \{2, \mathfrak{P}_r\}$ such that $2^5 | \lambda$.

Signature (r, r, p)

WARWICK

Let $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, 2 is inert for the specified values of r, and let $\mathfrak{P}_r$ be the unique prime above r.

- **Modularity machinery** $\rightsquigarrow$ find solutions to the S-unit equation

$$\lambda + \mu = 1$$

  where $S := \{2, \mathfrak{P}_r\}$ such that $2^5|\lambda$.
- Class Field Theory argument $\rightsquigarrow$ construct (λ_n, μ_n) with $v_2(\lambda_{n+1}) > v_2(\lambda_n)$.

Signature (r, r, p)

Let $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$, 2 is inert for the specified values of r, and let $\mathfrak{P}_r$ be the unique prime above r.

- **Modularity machinery** $\rightsquigarrow$ find solutions to the S-unit equation

$$\lambda + \mu = 1$$

  where $S := \{2, \mathfrak{P}_r\}$ such that $2^5 | \lambda$.
- Class Field Theory argument $\rightsquigarrow$ construct (λ_n, μ_n) with $v_2(\lambda_{n+1}) > v_2(\lambda_n)$.
- **Contradiction:** Infinite descent on finiteness of solutions of S-unit equations.

First step in Darmon's Program - Chapter 5

Darmon's Program

WARWICK

Darmon's Program

WARWICK

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

- **Frey representation:** Kraus constructs a family of hyperelliptic curves $C_r(a, b)$
- Compute the conductor of $C_r(a, b)$ = conductor of the l-adic representation $\rho_{J_r,l}$.

Darmon's Program

WARWICK

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

- **Frey representation:** Kraus constructs a family of hyperelliptic curves $C_r(a, b)$
- Compute the conductor of $C_r(a, b)$ = conductor of the l-adic representation $\rho_{J_r,l}$.
- BCDF22 show that Jac$(C_r) \otimes K \rightsquigarrow$

$$\rho_{J_r,\lambda} : G_K \to GL_2(K_\lambda).$$

  where $K := \mathbb{Q}(\zeta_r + \zeta_r^{-1})$ and $J_r :=$ Jac(C_r)
- **Modularity**, **Irreducibility**, **Level Lowering** apply to $\rho_{J_r,\lambda}$.
- 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

WARWICK

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 (ACKMM24 (⋆))

The conductor of $C_r(a,b)/K$ 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, Céline Maistret

Cluster Pictures

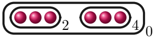
Cluster Pictures

Example

Consider the hyperelliptic curve

$$C : y^2 = x(x-p^2)(x-3p^2)(x-1)(x-1+p^4)(x-1-p^4)$$

where $p \geq 5$ is a prime. Its cluster picture at p is given by



.

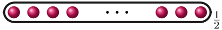
Cluster Pictures

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 $i = 0, \dots, r-1$.

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 $n := p v_{\mathfrak{q}}(c) \in \mathbb{Z}$.
  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

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

Thank you!