



UNIVERSITÄT  
BAYREUTH

# The Generalized Fermat Equation

$$x^2 + y^3 = z^{11}$$

Michael Stoll  
Universität Bayreuth

**Explicit Methods in Number Theory: JEC 60**

University of Warwick

April 6, 2016

# Background

This is joint work with **Nuno Freitas** and **Bartosz Naskręcki**.

The **Generalized Fermat Equation** is the equation

$$x^p + y^q = z^r$$

with fixed exponents  $p, q, r \geq 2$ ,  
to be solved in **coprime integers**.

The structure of its solution set is governed by

$$\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1.$$

## Theorem.

- If  $\chi > 0$ , there are **infinitely many** solutions.
- If  $\chi \leq 0$ , there are only **finitely many** solutions.

# Known Solutions

Apart from trivial solutions (with  $xyz = 0$ ),  
there are only the following ten solutions known when  $\chi \leq 0$ :

$$\begin{aligned} 1 + 2^3 &= 3^2, & 2^5 + 7^2 &= 3^4, & 7^3 + 13^2 &= 2^9, & 2^7 + 17^3 &= 71^2, \\ 3^5 + 11^4 &= 122^2, & 17^7 + 76271^3 &= 21063928^2, & 1414^3 + 2213459^2 &= 65^7, \\ 9262^3 + 15312283^2 &= 113^7, & 43^8 + 96222^3 &= 30042907^2, & 33^8 + 1549034^2 &= 15613^3 \end{aligned}$$

(up to permutations and sign changes).

## Conjecture.

There are **no other** nontrivial solutions.

## Remark.

The **ABC Conjecture** (with any  $\varepsilon < 1/5$ ) would imply  
that there are only finitely many solutions **in total** for  $\chi \leq 0$ .

## The Next Case

Heuristically, one expects more solutions when  $\chi < 0$  is closer to zero:

{p, q, r}	{2, 3, 7}	{2, 3, 8}	{2, 4, 5}	{2, 3, 9}	{2, 3, 10}	{2, 3, 11}
$-\chi$	1/42	1/24	1/20	1/18	1/15	5/66
#solns	5	3	2	2	1	1?

The five cases that have  $\chi < 0$  closest to zero have been completely solved.  
({2, 3, 8}, {2, 4, 5}, {2, 3, 9}: N. Bruin; {2, 3, 7}: B. Poonen, E. Schaefer, MS;  
{2, 3, 10}: D. Zureick-Brown and S. Siksek independently)

The next case in this ordering is  $(p, q, r) = (2, 3, 11)$ .

The only nontrivial solutions should be  $(x, y, z) = (\pm 3, -2, 1)$ .

**Goal:** Solve  $x^2 + y^3 = z^{11}$ !

# Frey Curves

We follow the general approach taken in the proof of FLT.

To a putative solution  $(a, b, c)$  of  $x^2 + y^3 = z^{11}$   
we associate the Frey elliptic curve

$$E_{(a,b,c)}: y^2 = x^3 + 3bx - 2a.$$

It has discriminant  $-12^3 c^{11}$ .

The 11-torsion Galois module  $E_{(a,b,c)}[11]$  is always irreducible.

By the usual level lowering results and modularity (plus some extra work),  
we find that (up to quadratic twist)  $E_{(a,b,c)}[11] \simeq E[11]$  for some

$$E \in \{27a1, 54a1, 96a1, 288a1, 864a1, 864b1, 864c1\}.$$

Known solutions:  $(\pm 1, 0, 1) \leftrightarrow 27a1$ ,  $\pm(0, 1, 1) \leftrightarrow 288a1$ ,  $(\pm 3, -2, 1) \leftrightarrow 864b1$ .

The trivial solutions  $(\pm 1, -1, 0)$  result in a degenerate Frey curve.

# The CM Cases

The curves 27a1 and 288a1 have **complex multiplication**.

In both cases the image of the mod 11 Galois representation is contained in the normalizer of a non-split Cartan subgroup.

Elliptic curves  $E'$  such that  $E'[11] \simeq 27a1[11]$  or  $288a1[11]$  correspond to **rational points** on the quadratic twists

$$X_{\text{nonsplit}}^{(d)}(11) \longrightarrow X_{\text{nonsplit}}^+(11)$$

with  $d = -3$  or  $-1$  of the double cover  $X_{\text{nonsplit}}(11) \longrightarrow X_{\text{nonsplit}}^+(11)$ .

$X_{\text{nonsplit}}^{(d)}(11)$  has **genus 4** and can be defined by the equations

$$\begin{aligned}y^2 &= 4x^3 - 4x^2 - 28x + 41 \\t^2 &= -d(4x^3 + 7x^2 - 6x + 19)\end{aligned}$$

## The CM Cases (2)

$$X_{\text{nonsplit}}^{(d)}(11): \quad y^2 = 4x^3 - 4x^2 - 28x + 41, \quad t^2 = -d(4x^3 + 7x^2 - 6x + 19)$$

The Jacobian of each of the two curves **splits** up to isogeny as a product of four elliptic curves of **rank 1**.

So a direct application of Chabauty's method is not possible.

Let  $K = \mathbb{Q}(\alpha)$  with  $\alpha$  a root of  $4x^3 - 4x^2 - 28x + 41$ .

A rational point on  $X_{\text{nonsplit}}^{(d)}(11)$  will give a  $K$ -rational point **with rational  $x$ -coordinate** on

$$u^2 = -d(x - \alpha)(4x^3 + 7x^2 - 6x + 19) \quad \text{or} \quad u^2 = -d(4 - \alpha)(x - \alpha)(4x^3 + 7x^2 - 6x + 19).$$

These elliptic curves over  $K$  have **rank  $\leq 2 < [K : \mathbb{Q}]$** ,

so **Elliptic Curve Chabauty** applies and can be used to show

that the only solutions coming from 27a1 and 288a1 are the **trivial** ones.

## The Remaining Curves

We still have to deal with  $E = 54a1, 96a1, 864a1, 864b1, 864c1$ .

An elliptic curve  $E'$  such that  $E'[11] \simeq E[11]$  corresponds to a **rational point** on one of two twists  $X_E(11)$  and  $X_E^-(11)$  of the modular curve  $X(11)$ , depending on whether the isomorphism acts on the Weil pairing by a square or a nonsquare in  $\mathbb{F}_{11}^\times$ .

A detailed study of the possible Galois representations **over  $\mathbb{Q}_2$  and  $\mathbb{Q}_3$**  lets us **rule out** the twists  $X_E^-(11)$  for all curves  $E$ .

It remains to find the rational points on the five twists  $X_E(11)$  that correspond to **primitive** (= coprime integer) solutions of  $x^2 + y^3 = z^{11}$ .

## From $X(11)$ to $X_0(11)$

The **genus** of  $X(11)$  is **26**, which is **too large** for explicit computations.

Instead, we use the intermediate curve  $C := X_0(11)$ ,

which is the **elliptic curve 11a1**.

$$X_E(11) \simeq_{\bar{\mathbb{Q}}} X(11) \rightarrow X_0(11) \xrightarrow{j} \mathbb{P}^1$$

Let  $K_E$  be the field of definition of a **cyclic subgroup** of order 11 on  $E$ .

Then a **rational point** on  $X_E(11)$  maps to a  $K_E$ -**rational point** on  $C$ , whose image under the  **$j$ -invariant** map is in  $\mathbb{Q}$ .

This is again the setting for **Elliptic Curve Chabauty**.

### **Problem:**

We need to find **generators** of a finite-index subgroup of  $C(K_E)$ , but are **unable** to do so.

# Selmer Group Chabauty

We **work around** this problem by employing a **new approach** that allows us to perform Elliptic Curve Chabauty based only on the knowledge of a suitable **Selmer group**.

We can compute the **2-Selmer group  $S$**  of  $C$  over  $K_E$ , assuming the **Generalized Riemann Hypothesis**.

( $[K_E : \mathbb{Q}] = 12$ ; we need the class group of a cubic extension  $L_E$  of  $K_E$ .)

The Selmer group sits in the following diagram:

$$\frac{C(K_E)}{2C(K_E)} \hookrightarrow S \xrightarrow{\sigma} \frac{C(K_E \otimes \mathbb{Q}_2)}{2C(K_E \otimes \mathbb{Q}_2)} \hookrightarrow \frac{(L_E \otimes \mathbb{Q}_2)^\times}{(L_E \otimes \mathbb{Q}_2)^{\times 2}}$$

We check that  **$\sigma$  is injective** for each of our curves  $E$ .

# Partitioning the $j$ -Line

The main idea is to combine the **global** information from the Selmer group with local, in our case **2-adic**, information.

We first find the potential images in  $\mathbb{Q}_2$  under the  **$j$ -invariant map** of the points we are interested in.

For each curve  $E$ , we obtain a **finite collection** of sets  $\{a + bt^n : t \in \mathbb{Z}_2\}$ :

54a1: 1 set, 96a1: 3 sets, 864a1: 2 sets, 864b1: 3 sets, 864c1: 3 sets.

We **lift** these sets in all possible ways to  $C(K_E \otimes \mathbb{Q}_2)$

and check which of them **map into**  $\sigma(S)$  under  $\pi: C(K_E \otimes \mathbb{Q}_2) \rightarrow \frac{C(K_E \otimes \mathbb{Q}_2)}{2C(K_E \otimes \mathbb{Q}_2)}$ .

This leaves

54a1: 1 set, 96a1: 2 sets, 864a1: 0 sets, 864b1: 1 set, 864c1: 1 set.

This already **rules out 864a1**.

## Dealing With the Remaining Sets

For each of the remaining **sets**  $D$  there is a **point**  $P \in C(K_E)$  such that  $P$  and all points mapping into  $D$  have the **same image** in  $\frac{C(K_E \otimes \mathbb{Q}_2)}{2C(K_E \otimes \mathbb{Q}_2)}$ .

### **Lemma.**

Assume that for all  $P \neq Q \in C(K_E \otimes \mathbb{Q}_2)$  with  $j(Q) \in D$  there are  $n \geq 0$  and  $Q' \in C(K_E \otimes \mathbb{Q}_2)$  such that  $Q = P + 2^n Q'$  and  $\pi(Q') \notin \sigma(S)$ .

Then if  $j(P) \in D$ ,  $P$  is the **only point**  $Q \in C(K_E)$  with  $j(Q) \in D$ , and if  $j(P) \notin D$ , then there is **no such point**.

**Proof.** Let  $Q \in C(K_E)$  with  $j(Q) \in D$  and  $Q \neq P$ .

Then  $Q = P + 2^n Q'$  with  $Q' \in C(K_E \otimes \mathbb{Q}_2)$  and  $\pi(Q') \notin \sigma(S)$ .

Using that  $\sigma$  is injective and  $C(K_E)[2] = 0$ , we obtain  $Q' \in C(K_E)$ , which implies  $\pi(Q') \in \sigma(S)$ , a contradiction.  $\square$

## Finishing the Argument

The point  $Q'$  in the Lemma is unique (we have to take  $n$  maximal).  
The map  $Q \mapsto Q'$  is **locally constant** on any lift of  $D$  in an **explicit way**.  
So we can **effectively check** the assumption in the Lemma.

It turns out that the assumption **holds in all cases**.

This leaves us with three points  $P$  such that  $j(P) \in D$ ,  
only **one** of which gives a primitive solution, namely  $(\pm 3, -2, 1)$ .  
(This point comes from the 'tautological point' on  $X_{864b1}(11)$ .)

We finally obtain:

### **Theorem.**

Assume GRH. The only **coprime integer** solutions of  $x^2 + y^3 = z^{11}$  are

$$(\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 1, -1, 0), \quad (\pm 3, -2, 1).$$

Thank You!