Generalized Fermat equations
$x^2 + y^3 = z^p$
a progress report

Nuno Freitas, Bartosz Naskręcki, Michael Stoll

Max Planck Institute Bonn/Universität Bayreuth

Algorithmic & Experimental Methods
In Algebra, Geometry and Number Theory
02.10.2015, Osnabrück

Generalized Fermat equations

We consider the problem of solving the equation $x^p + y^q + z^r = 0$ for fixed exponents p, q, r and in integers x, y, z which are pairwise coprime.

(Some) known results

- Wiles et al. : $\{p, q, r\} = \{n, n, n\}$
- Darmon–Merel: $\{p, q, r\} = \{2, n, n\}, \{3, n, n\}$
- Bennett: $\{p, q, r\} = \{2n, 2n, 5\}$
- Elkies: $\{p, q, r\} = \{2, 4, \ell\}$ for $\ell \geq 211$
- Siksek–Anni: $\{p, q, r\} = \{2l, 2m, p\}$ for $3 \leq p \leq 13$ (and more if someone is willing to share a stronger computer...)

Generalized Fermat equations

We consider the family $x^2 + y^3 = z^r$ where $r \geq 7$ and its coprime solutions

Known results

- Poonen–Schaefer–Stoll for $r = 7$
- Bruin: $r = 8, 9$
- Zureick-Brown: $r = 10$
- Siksek–Stoll: $r = 15$

The remaining open cases are $r = p \geq 11$ a prime and $r = 25$ (Freitas–Stoll, a work in progress).

Problem

Let $p \geq 11$ be a prime. Let (a, b, c) be a solution to the equation

$$x^2 + y^3 = z^p$$

such that $(a, b, c) = 1$ and $abc \neq 0$.
Find the explicit list of such triples (a, b, c).

Problem

Let $p \geq 11$ be a prime. Let (a, b, c) be a solution to the equation

$$x^2 + y^3 = z^p$$

such that $(a, b, c) = 1$ and $abc \neq 0$.
Find the explicit list of such triples (a, b, c).

We call such solutions *primitive*.

Work of Darmon and Granville implies that for each prime p the list of such solutions is finite (using Faltings' resolution of Mordell's conjecture).

For $c = 1$ we have a pair of *Catalan solutions* $(a, b, c) = (\pm 3, 2, 1)$.

Frey curve

To a putative primitive solution (a, b, c) of $x^2 + y^3 = z^p$ with $p \geq 7$ we can attach a Frey curve

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

of discriminant $\Delta = -12^3 c^p$ and j-invariant $j = \frac{12^3 b^3}{c^p}$.

Frey curve

To a putative primitive solution (a, b, c) of $x^2 + y^3 = z^p$ with $p \geq 7$ we can attach a Frey curve

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

of discriminant $\Delta = -12^3 c^p$ and j-invariant $j = \frac{12^3 b^3}{c^p}$.

Theorem 1 (Generalization of Poonen-Schaefer-Stoll)

Let $p \geq 7$ and (a, b, c) be coprime integers satisfying $a^2 + b^3 = c^p$ and $c \neq 0$. Assume that the Galois representation on $E_{(a,b,c)}[p]$ is irreducible.

Frey curve

To a putative primitive solution (a, b, c) of $x^2 + y^3 = z^p$ with $p \geq 7$ we can attach a Frey curve

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

of discriminant $\Delta = -12^3 c^p$ and j-invariant $j = \frac{12^3 b^3}{c^p}$.

Theorem 1 (Generalization of Poonen-Schaefer-Stoll)

Let $p \geq 7$ and (a, b, c) be coprime integers satisfying $a^2 + b^3 = c^p$ and $c \neq 0$. Assume that the Galois representation on $E_{(a,b,c)}[p]$ is irreducible. Then there exists a quadratic twist $E^{(d)}_{(a,b,c)}$ of $E_{(a,b,c)}$ with $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ such that $E^{(d)}_{(a,b,c)}[p]$ is isomorphic to $E[p]$ as a $G_{\mathbb{Q}}$-Galois module, where E is one of the following elliptic curves (specified by their Cremona label):

$$27a1,\ 54a1,\ 96a1,\ 288a1,\ 864a1,\ 864b1,\ 864c1\,.$$

For prime $p \geq 17$ and $p = 11$ the Galois module $E^{(d)}_{(a,b,c)}[p]$ is irreducible for primitive solutions (a, b, c).

To prove the theorem we apply Tate's algorithm to first show that the conductor of the twist $E^{(d)}_{(a,b,c)}$ has the form $12^3 N$ where N is a product of primes dividing c. Then application of level-lowering leaves us with a finite list of modular forms of suitable levels.

For prime $p \geq 17$ and $p = 11$ the Galois module $E^{(d)}_{(a,b,c)}[p]$ is irreducible for primitive solutions (a, b, c).

To prove the theorem we apply Tate's algorithm to first show that the conductor of the twist $E^{(d)}_{(a,b,c)}$ has the form $12^3 N$ where N is a product of primes dividing c. Then application of level-lowering leaves us with a finite list of modular forms of suitable levels.

All but one of them correspond to elliptic curves over $\mathbb{Q}$. For a newform of level 864 with coefficients in $\mathbb{Q}(\sqrt{13})$ we apply the Loeffler-Weinstein algorithm and a result of Kraus.

Irreducibility of the Galois module $E^{(d)}_{(a,b,c)}[p]$ is a direct consequence of Mazur's results.

Primitive solutions to $x^2 + y^3 = z^p$ can be detected by branched Galois covering $X \to \mathbb{P}^1$ defined over $\mathbb{Q}$ with three ramified points $0, 12^3, \infty$ of ramification indices $3, 2, p$. We consider $X = X(p)$ a modular curve which classifies pairs (E, ϕ) where

$$\phi : E[p] \to \mu_p \times \mathbb{Z}/p\mathbb{Z}$$

is an isomorphism of Galois modules which respects the Weil pairing. The natural forgetful map $j : X(p) \to X(1)$ satisfies the required properties.

Primitive solutions to $x^2 + y^3 = z^p$ can be detected by branched Galois covering $X \to \mathbb{P}^1$ defined over $\mathbb{Q}$ with three ramified points $0, 12^3, \infty$ of ramification indices $3, 2, p$. We consider $X = X(p)$ a modular curve which classifies pairs (E, ϕ) where

$$\phi : E[p] \to \mu_p \times \mathbb{Z}/p\mathbb{Z}$$

is an isomorphism of Galois modules which respects the Weil pairing. The natural forgetful map $j : X(p) \to X(1)$ satisfies the required properties.

Following Darmon and Granville for each p there exists a number field K such that the finite set $j(X(p)(K))$ contains points that correspond to the primitive solutions of $x^2 + y^3 = z^p$.

In general the field K might be of large degree so we construct rather a finite list of twists $X' \to \mathbb{P}^1$ where $X' \cong_{\overline{\mathbb{Q}}} X(p)$ and for each twist X' which is defined over $\mathbb{Q}$ compute the points $X'(\mathbb{Q})$ that correspond to primitive solutions of $x^2 + y^3 = z^p$.

For two elliptic curves E_1 and E_2 over a field K we say that the Galois modules $E_1[p]$ and $E_2[p]$ are *symplectically* isomorphic if the isomorphism of Galois modules $\phi : E_1[p] \to E_2[p]$ respects the Weil pairing e_p. We call ϕ anti-symplectic if

$$e_p(\phi(P), \phi(Q)) = e_p(P, Q)^r$$

for all $P, Q \in E_1[n]$ where r is a non-square in $\mathbb{F}_p^\times$.

Composition of ϕ with multiplication by n (coprime with p) on E_1 changes the Weil pairing exponent by n^2. We consider a fixed curve E and denote by $X_{E'}(p)$ a modular curve that classifies pairs (E, ϕ) where $\phi : E[p] \to E'[p]$ is a symplectic Galois invariant isomorphism. We denote by $X^-_{E'}(p)$ an analogous curve which classifies pairs (E, ϕ) where ϕ is anti-symplectic.

This table is valid for $p \geq 17$ (and also for $p = 11$). We classify all possible twists that might come with a primitive solution to $x^2 + y^3 = z^p$.

p mod 24	$27a1$	$54a1$	$96a1$	$288a1$	$864a1$	$864b1$	$864c1$
1		$+$	$+$		$+$	$+$	$+$
5	$+$	$-$	$+$		$+-$	$+-$	$+-$
7		$-$	$+$	$+$	$+$	$+$	$+$
11	$+$	$+$	$+$	$+-$	$+$	$+$	$+$
13			$-$		$+$	$+$	$+$
17	$+$	$+$			$+$	$+$	$+$
19		$+$	$-$	$+-$	$+-$	$+-$	$+-$
23	$+$			$+$	$+$	$+$	$+$

In consequence for each choice of congruence classes $a \mod 36$ and $b \mod 24$ the solution $a^2 + b^3 = c^p$ that corresponds to the Frey curve $E^{(d)}_{(a,b,c)}$ will determine a rational point on the symplectic or antisymplectic twist $X^{\pm}_E(p)$ where E comes from the finite list of curves determined before.

Multiplicative reduction

Theorem 2 (Halberstadt–Kraus 2002, Proposition A.1)

Let E, E' be elliptic curves over $\mathbb{Q}$ with minimal discriminants Δ, Δ'. Let p be a prime such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$. Suppose that E and E' have multiplicative reduction at a prime $\ell \neq p$ and that $p \nmid v_\ell(\Delta)$. Then $p \nmid v_\ell(\Delta')$, and the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are symplectically isomorphic if and only if $v_\ell(\Delta)/v_\ell(\Delta')$ is a square mod p.

Multiplicative reduction

Isogeny graph of elliptic curves of conductor 54:

$$54a2 \xrightarrow{3} 54a1 \xrightarrow{3} 54a3$$

The Frey curve $E^{(d)}_{(a,b,c)}$ has multiplicative reduction at $\ell = 2$ if and only if c is even and $d = \pm 1, \pm 3$, in which case its minimal discriminant is $\Delta = 2^{-6}3^3 d^6 c^p$. In particular, $v_2(\Delta) \equiv -6 \bmod p$.

Then the Frey curve must be p-congruent to $E = 54a1$ (which is the only curve in our list that has multiplicative reduction at 2). On the other hand, $\Delta_E = -2^3 3^9$, so that the isomorphism between $E^{(d)}_{(a,b,c)}[p]$ and $E[p]$ is symplectic if and only if $(-2/p) = 1$.

Multiplicative reduction

Isogeny graph of elliptic curves of conductor 54:

$$54a2 \xrightarrow{3} 54a1 \xrightarrow{3} 54a3$$

The Frey curve $E_{(a,b,c)}^{(d)}$ has multiplicative reduction at $\ell = 2$ if and only if c is even and $d = \pm 1, \pm 3$, in which case its minimal discriminant is $\Delta = 2^{-6} 3^3 d^6 c^p$. In particular, $v_2(\Delta) \equiv -6 \bmod p$.

Then the Frey curve must be p-congruent to $E = 54a1$ (which is the only curve in our list that has multiplicative reduction at 2). On the other hand, $\Delta_E = -2^3 3^9$, so that the isomorphism between $E_{(a,b,c)}^{(d)}[p]$ and $E[p]$ is symplectic if and only if $(-2/p) = 1$.

So for $p \equiv 1, 11, 17, 19 \bmod 24$, we get rational points on $X_{54a1}(p)$, whereas for $p \equiv 5, 7, 13, 23 \bmod 24$, we get rational points on $X_{54a1}^{-}(p)$ (which is $X_{54a2}(p)$ when $(3/p) = -1$).

Additive reduction

Let E, E' be elliptic curves over $\mathbb{Q}_\ell$ with potentially good reduction. Let $L = \mathbb{Q}_\ell^{\mathrm{unr}}(E[p])$ and $L' = \mathbb{Q}_\ell^{\mathrm{unr}}(E'[p])$ be the smallest extensions of $\mathbb{Q}_\ell^{\mathrm{unr}}$ over which they respectively acquire good reduction.

These extensions do not depend on $p \neq \ell$ (Serre–Tate). We will say that E and E' *have the same inertia type (at ℓ)* if they have the same conductor and $L = L'$.

Write $I = \mathrm{Gal}(L/\mathbb{Q}_\ell^{\mathrm{unr}})$ and $I_\ell = G_{\mathbb{Q}_\ell^{\mathrm{unr}}}$. If I is not abelian, then we can prove that that $E[p]$ and $E'[p]$ are symplectically isomorphic as $G_{\mathbb{Q}_\ell}$-modules if and only if they are symplectically isomorphic as I_ℓ-modules.

Additive reduction

Theorem 3

Let $p \geq 3$ be a prime. Let E and E' be elliptic curves over $\mathbb{Q}_2$ with potentially good reduction. Suppose they have the same inertia type and that $I \simeq H_8$ (quaternion group). Then $E[p]$ and $E'[p]$ are isomorphic as I_2-modules. Moreover,

(1) *if $(2/p) = 1$, then $E[p]$ and $E'[p]$ are symplectically isomorphic I_2-modules;*

(2) *if $(2/p) = -1$, then $E[p]$ and $E'[p]$ are symplectically isomorphic I_2-modules if and only if $E[3]$ and $E'[3]$ are symplectically isomorphic I_2-modules.*

Additive reduction

Consider the curves E with conductor at 2 equal to 2^5; these are 96a1, 288a1, 864a1, 864b1 and 864c1.

They all have potentially good reduction at 2 and $I = \mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{unr}}) \simeq H_8$. Since H_8 is non-abelian the isomorphism of mod p Galois representations is symplectic if and only if it is symplectic on the level of inertia groups. It follows that when $(2/p) = 1$ the isomorphism $E_{(a,b,c)}^{(d)}[p] \simeq E[p]$ can only be symplectic.

So for $p \equiv 1, 7, 17, 23 \bmod 24$, we can exclude the 'minus' twists $X_E^-(p)$ for $E \in \{96a1, 288a1, 864a1, 864b1, 864c1\}$.

Ruling out CM curves

Bilu–Parent–Rebolledo proved that for $p \geq 11$, $p \neq 13$, the image of the mod p Galois representation of any elliptic curve E over $\mathbb{Q}$ is never contained in the normalizer of a split Cartan subgroup unless E has complex multiplication. This allows us to deduce the following.

Corollary 4

Let $p = 11$ or $p \geq 17$ be a prime number.

(1) *If $p \equiv 1 \bmod 3$, then the only primitive solutions coming from rational points on $X^{\pm}_{27a1}(p)$ are the trivial solutions $(\pm 1)^2 + 0^3 = 1^p$.*

(2) *If $p \equiv 1 \bmod 4$, then the only primitive solutions coming from rational points on $X^{\pm}_{288a1}(p)$ are the trivial solutions $0^2 + (\pm 1)^3 = (\pm 1)^p$ (with the same sign on both sides).*

Global points on modular curves, p=7

For $p = 7$ the modular curve $X(7)$ can be realized as the Klein quartic

$$x^3y + y^3z + z^3x = 0.$$

The equations for twists $X_E^{\pm}(7)$ were found by Kraus and Halberstadt. This was exploited in the paper by Poonen-Schaefer-Stoll.

Global points on modular curves, p=11

For $p = 11$ we can realize $X(11)$ as a curve in $\mathbb{P}^4$ given a by Hessian of the cubic threefold

$$v^2w + w^2x + x^2y + y^2z + z^2v = 0.$$

This gives a curve determined by 25 equations (!) of genus 26. The twists by E were worked out by Tom Fisher.

For $p = 11$ we have to find points over $\mathbb{Q}$ on the twists $X_E^+(11)$ with $E \in \{54a1, 96a1, 864a1, 864b1, 864c1\}$. A direct approach to this problem seems to be hopeless...

Global points on modular curves, p=11

For $p = 11$ we can realize $X(11)$ as a curve in $\mathbb{P}^4$ given a by Hessian of the cubic threefold

$$v^2w + w^2x + x^2y + y^2z + z^2v = 0.$$

This gives a curve determined by 25 equations (!) of genus 26. The twists by E were worked out by Tom Fisher.

For $p = 11$ we have to find points over $\mathbb{Q}$ on the twists $X_E^+(11)$ with $E \in \{54a1, 96a1, 864a1, 864b1, 864c1\}$. A direct approach to this problem seems to be hopeless...

However we can factor the forgetful map $X(11) \to X(1)$ into $X(11) \to X_1(11) \to X_0(11) \to X(1)$. We observe that $X_1(11)$ and $X_0(11)$ are 5-isogenous elliptic curves over $\mathbb{Q}$. But we need a twist of this map for $X_E(11)$ and the intermediate map $X_E(11) \to X_1(11)$ is defined over degree 60 field and $X_E(11) \to X_0(11)$ is realized over degree 12 field (with no subfields).

We are able to produce these maps explicitly. For example for $E = 864b1$ the twist $X_E(11)$ contains a point $[0, 1, 0, 0, 0]$ which corresponds to the Catalan solution and it generates a point in Mordell–Weil group of $X_1(11)(K_{60})$ and $X_0(11)(K_{12})$.

The obvious approach would be to use Elliptic Chabauty method but for this we need a finite index subgroup (for example in $X_0(11)(K_{12})$) and we have just a partial information on that.

The other approach might be to combine this explicit maps with the Chabauty method described during Michael Stoll's lecture..(tbc)

Summary

- Local methods enable us to eliminate many twists of $X(p)$ which might contribute to putative solutions of $x^2 + y^3 = z^p$
- Applied methods use the information on Galois action on $E[p]$ at the level of inertia
- The remaining curves contain ℓ–adic points for $\ell = 2, 3$ so there is no local obstruction to the existence of global points on the twists $X_E(p)$.
- We have applied an Elliptic Chabauty approach to eliminate CM cases for $p = 11$

Summary

- Local methods enable us to eliminate many twists of $X(p)$ which might contribute to putative solutions of $x^2 + y^3 = z^p$
- Applied methods use the information on Galois action on $E[p]$ at the level of inertia
- The remaining curves contain ℓ–adic points for $\ell = 2, 3$ so there is no local obstruction to the existence of global points on the twists $X_E(p)$.
- We have applied an Elliptic Chabauty approach to eliminate CM cases for $p = 11$
- We don't know (yet) how to use the global information about the maps from $X_E(11) \to X_0(11)$ to eliminate the remaining curves for $p = 11$.
- Provided some explicit models for $X(p)$ with $p \geq 17$ we could try to use some other global methods to eliminate those curves.
- The unlucky case $p = 13$ remains the most unfortunate to deal with...

Thank you.

j	a	b	d	curves
1	$a \equiv 1 \bmod 4$	$b \equiv 1 \bmod 2$	$1, -3$	$54a1$
2	$a \equiv 3 \bmod 4$	$b \equiv 1 \bmod 2$	$-1, 3$	$54a1$
3	$a \equiv 0 \bmod 4$	$b \equiv 1 \bmod 4$	$\pm 1, \pm 3$	$288a1, 864a1, 864b1$
4	$a \equiv 0 \bmod 4$	$b \equiv 3 \bmod 4$	$\pm 2, \pm 6$	$288a1, 864a1, 864b1$
5	$a \equiv 2 \bmod 4$	$b \equiv 1 \bmod 4$	$\pm 1, \pm 3$	$96a1, 864c1$
6	$a \equiv 2 \bmod 4$	$b \equiv 3 \bmod 4$	$\pm 2, \pm 6$	$96a1, 864c1$
7	$a \equiv 1 \bmod 4$	$b \equiv 0 \bmod 8$	$-2, 6$	$27a1$
8	$a \equiv 3 \bmod 4$	$b \equiv 0 \bmod 8$	$2, -6$	$27a1$
9	$a \equiv 1 \bmod 2$	$b \equiv 2 \bmod 8$	$\pm 2, \pm 6$	$96a1, 864c1$
10	$a \equiv 1 \bmod 2$	$b \equiv 6 \bmod 8$	$\pm 2, \pm 6$	$288a1, 864a1, 864b1$
11	$a \equiv 1 \bmod 2$	$b \equiv 4 \bmod 8$	$\pm 2, \pm 6$	impossible

Table : 2-adic conditions

i	a	b	d	curves
1	$a \equiv 1 \bmod 3$	$b \equiv -1 \bmod 3$	$-3, 6$	$96a1$
2	$a \equiv -1 \bmod 3$	$b \equiv -1 \bmod 3$	$3, -6$	$96a1$
3	$a \equiv 0 \bmod 9$	$b \equiv \pm 1 \bmod 3$	$d \mid 6$	$288a1$
4	$a \equiv \pm 3 \bmod 9$	$b \equiv 1 \bmod 3$	$d \mid 6$	$27a1, 864b1, 864c1$
5	$a \equiv \pm 3 \bmod 9$	$b \equiv -1 \bmod 3$	$d \mid 6$	$54a1, 864a1$
6	$a \equiv \pm 1 \bmod 3$	$b \equiv 0 \bmod 3$	$d \mid 6$	$27a1, 864b1, 864c1$
7	$a \equiv \pm 2 \bmod 9$	$b \equiv 1 \bmod 3$	$d \mid 6$	$288a1$
8	$a \equiv \pm 1, \pm 4 \bmod 9$	$b \equiv 1 \bmod 3$	$d \mid 6$	$54a1, 864a1$

Table : 3-adic conditions

Remarks

- For $p = 13$ we don't have enough information to eliminate some of the twists only by local considerations.
- For $p = 11$ we can eliminate all curves that come from twists by CM curves (so $288a1$ and $27a1$). This follows from the fact that the image of Galois representation of curves with CM lies in the normalizer of non-split Cartan subgroup of $GL_2(\mathbb{F}_{11})$. The corresponding modular curve $X_{ns}^{+}(11)$ is an elliptic curve $121b1$ (Ligozat) and its double cover $X_{ns}(11)$ that classifies curves with 11–torsion contained in the non–split Cartan subgroup is of genus 4 with split Jacobian (isogenous to a product of elliptic curves $121a1$,$121b1$, $121c1$ and $121d1$).

Double cover $X_{ns}(11) \to X_{ns}^+(11)$ is realized as

$$t^2 = -(4x^3 + 7x^2 - 6x + 19)$$

where $X_{ns}^+(11)$ is

$$y^2 = 4x^3 - 4x^2 - 28x + 41$$

and

$$X_{ns}(11)\colon \begin{cases} y^2 = 4x^3 - 4x^2 - 28x + 41 \\ t^2 = -(4x^3 + 7x^2 - 6x + 19) \end{cases}$$

We apply Elliptic Chabauty method to twists of $X_{ns}(11)$ by $-1, -3$ to find all points over $\overline{\mathbb{Q}}$ with rational value at the canonical j–map $X_{ns}(11) \to X(1)$.