International University Bremen

$x^2 + y^3 = z^7$

Michael Stoll

International University Bremen

with

Bjorn Poonen, UC Berkeley

and

Ed Schaefer, University of Santa Clara

The Result

The following is now a 100% theorem.
(Last year in Oberwolfach, it was only 90%.)

Theorem.
The complete list of primitive integral solutions of

$$x^2 + y^3 = z^7$$

is given by

$$(\pm 1, -1, 0)\,, \quad (\pm 1, 0, 1)\,, \quad \pm(0, 1, 1)$$
$$(\pm 3, -2, 1)\,, \quad (\pm 71, -17, 2)\,, \quad (\pm 2\,213\,459, 1\,414, 65)$$
$$(\pm 15\,312\,283, 9\,262, 113)\,, \quad (\pm 21\,063\,928, -76\,271, 17)$$

Some General Theory

We consider the Generalized Fermat Equation

$$\boxed{x^p + y^q = z^r}\,.$$

Let
$$\boxed{\chi_{p,q,r} = \chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1\,.}$$

Let $P \subset \mathbb{P}^2$ be the line $x + y = z$.
There is a branched Galois covering $X \xrightarrow{\pi} P$, defined over $\mathbb{Q}$,
ramified above $(0 : 1 : 1)$, $(1 : 0 : 1)$, $(1 : -1 : 0)$
with ramification index p, q, r, respectively.

- $\chi > 0 \Longrightarrow X \cong \mathbb{P}^1$
- $\chi = 0 \Longrightarrow X$ is an elliptic curve
- $\chi < 0 \Longrightarrow$ genus$(X) \geq 2$

Note that $\chi_{2,3,7} = -1/42$ is closest to zero from below.

A General Theorem

Let $S_{p,q,r} = \{(a^p : b^q : c^r) : a, b, c \in \mathbb{Z}, \text{gcd}(a, b, c) = 1, a^p + b^q = c^r\} \subset P(\mathbb{Q})$.

Theorem (Darmon-Granville).
There is a number field K such that $\pi(X(K)) \supset S_{p,q,r}$.

Corollary.
If $\chi < 0$, then $S_{p,q,r}$ is finite.

Theorem (Variant).
There are finitely many twists $X_j \xrightarrow{\pi_j} P$ of $X \xrightarrow{\pi} P$
such that $\bigcup_j \pi_j(X_j(\mathbb{Q})) \supset S_{p,q,r}$.
(These twists are all unramified outside pqr.)

More precisely:
Let $Y_j(\mathbb{Q}) \subset X_j(\mathbb{Q})$ be the points satisfying certain conditions
mod powers of the primes dividing pqr. Then $S_{p,q,r} = \coprod_j \pi_j(Y_j(\mathbb{Q}))$.

A Side Remark

Instead of P,
one should consider $x^p + y^q = z^r$ as a curve $X_{p,q,r}$ in a weighted $\mathbb{P}^2$.

Note that $S_{p,q,r} \cong X_{p,q,r}(\mathbb{Z})$ (modulo signs).

$X_{p,q,r}$ is P with the points $(0:1:1)$, $(1:0:1)$, $(1:-1:0)$
replaced with $1/p$, $1/q$, $1/r$ times a point, respectively.
(Assuming p, q, r coprime in pairs.)

Then $X \xrightarrow{\pi} X_{p,q,r}$ is *unramified*
and χ is the Euler characteristic of $X_{p,q,r}$.

This explains why one can do descent using π.

We also find $2 - 2\,\text{genus}(X) = \deg(\pi)\chi$.

Overall Strategy for (2,3,7)

In our special case, X can be taken to be the *Klein Quartic*

$$\boxed{X : x^3 y + y^3 z + z^3 x = 0}$$

Note that $X \cong X(7)$ (the modular curve).

1. Find the relevant twists X_j of X explicitly.
2. Find $X_j(\mathbb{Q})$ (or at least $Y_j(\mathbb{Q})$).

Step 1 uses modular arguments
(plus a separate consideration for reducible 7-torsion).

Step 2 uses descent on the Jacobians of the X_j and Chabauty,
plus a Brauer-Manin obstruction argument for one curve
where Chabauty fails.

Step 1: Quick Overview

Given a solution $a^2 + b^3 = c^7$, consider

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

The usual arguments show that $E_{(a,b,c)}$ is semistable outside $\{2, 3\}$ and that, if $E_{(a,b,c)}[7]$ is irreducible, $E_{(a,b,c)}[7] \cong E[7]$ (up to quadratic twist) for E out of a list of 13 elliptic curves.

By work of Kraus and Halberstadt, we can write down explicit equations of twists $X_E(7)$ and $X_E^-(7)$ classifying E' such that $E'[7] \cong E[7]$.

A more direct argument produces several hundreds of twists arising from the case when $E_{(a,b,c)}[7]$ is reducible.

For many of these curves, local considerations show $Y_j(\mathbb{Q}) = \emptyset$.

We are left with just 10 twists X_j.

The Twists

$$X_1 : 6x^3y + y^3z + z^3x = 0$$

$$X_2 : 3x^3y + y^3z + 2z^3x = 0$$

$$X_3 : 3x^3y + 2y^3z + z^3x = 0$$

$$X_4 : 7x^3z + 3x^2y^2 - 3xyz^2 + y^3z - z^4 = 0$$

$$X_5 : -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0$$

$$X_6 : x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + 18xyz^2 + 9y^2z^2 - 9z^4 = 0$$

$$X_7 : -3x^4 - 6x^3z + 6x^2y^2 - 6x^2yz + 15x^2z^2 - 4xy^3 - 6xyz^2 - 4xz^3 + 6y^2z^2 - 6yz^3 = 0$$

$$X_8 : 2x^4 - x^3y - 12x^2y^2 + 3x^2z^2 - 5xy^3 - 6xy^2z + 2xz^3 - 2y^4 + 6y^3z + 3y^2z^2 + 2yz^3 = 0$$

$$X_9 : 2x^4 + 4x^3y - 4x^3z - 3x^2y^2 - 6x^2yz + 6x^2z^2 - xy^3 - 6xyz^2 - 2y^4 + 2y^3z - 3y^2z^2 + 6yz^3 = 0$$

$$X_{10} : x^3y - x^3z + 3x^2z^2 + 3xy^2z + 3xyz^2 + 3xz^3 - y^4 + y^3z + 3y^2z^2 - 12yz^3 + 3z^4 = 0$$

The Points

We find the following rational points on these curves.

$$X_1 : (1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : -1 : 2)$$

$$X_2 : (1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : -1), (1 : -2 : -1)$$

$$X_3 : (1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : -1)$$

$$X_4 : (1 : 0 : 0), (0 : 1 : 0), (0 : 1 : 1)$$

$$X_5 : (1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1)$$

$$X_6 : (0 : 1 : 0), (1 : -1 : 0), \boxed{(0 : 1 : 1)}, \boxed{(0 : 1 : -1)}$$

$$X_7 : (0 : 1 : 0), \boxed{(0 : 0 : 1)}, \boxed{(0 : 1 : 1)}$$

$$X_8 : \boxed{(0 : 0 : 1)}, (2 : -1 : 0)$$

$$X_9 : (0 : 0 : 1), (1 : 1 : 0)$$

$$X_{10} : \boxed{(1 : 0 : 0)}, (1 : 1 : 0)$$

The boxed points lead to nontrivial primitive solutions.

Step 2: Overview

It remains to prove that there are no other points in $X_j(\mathbb{Q})$,
or at least in $Y_j(\mathbb{Q})$.

The only good and widely applicable way of doing this
is Chabauty's method.

Chabauty's method works
when the rank of $J_j(\mathbb{Q}) = \mathrm{Jac}(X_j)(\mathbb{Q})$ is less than 3.

So we first have to determine this rank
and find generators of a finite index subgroup of $J_j(\mathbb{Q})$.

2-Descent on J_j

For general plane quartics, descent is infeasible.

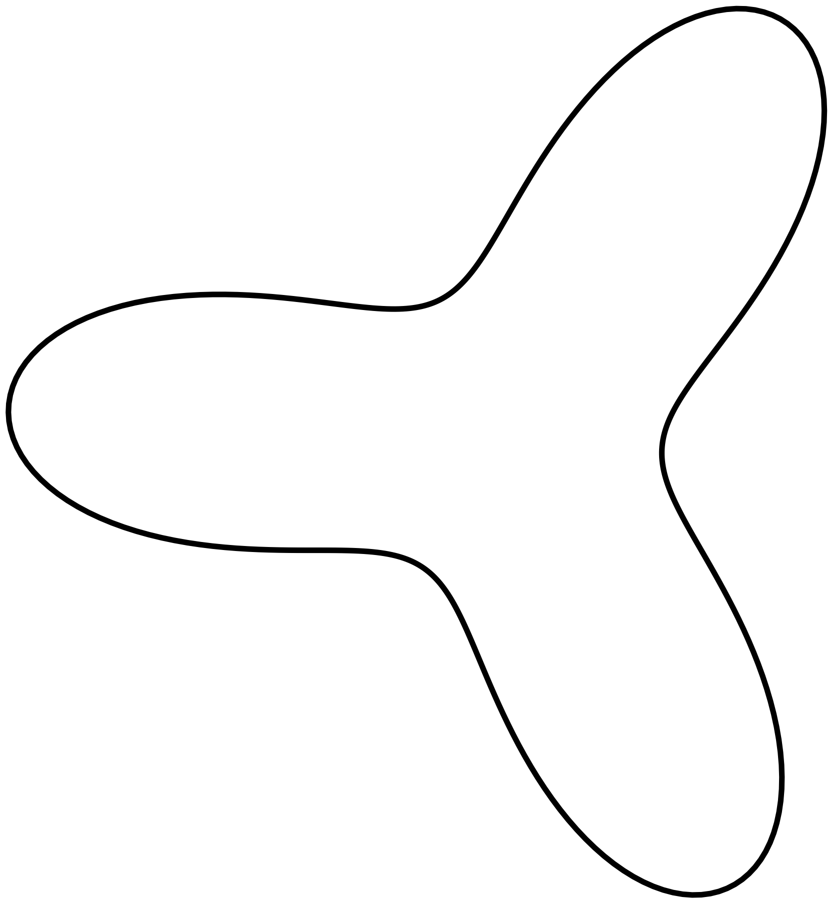
However, our curves are very special:
They are twists of X, so they have a large automorphism group:

$$\mathrm{Aut}(X_j) \cong \mathrm{Aut}(X) \cong \mathrm{PSL}(2, \mathbb{F}_7)$$

In fact, $X_{2,3,7} \cong X_j / \mathrm{Aut}(X_j)$ via π_j.

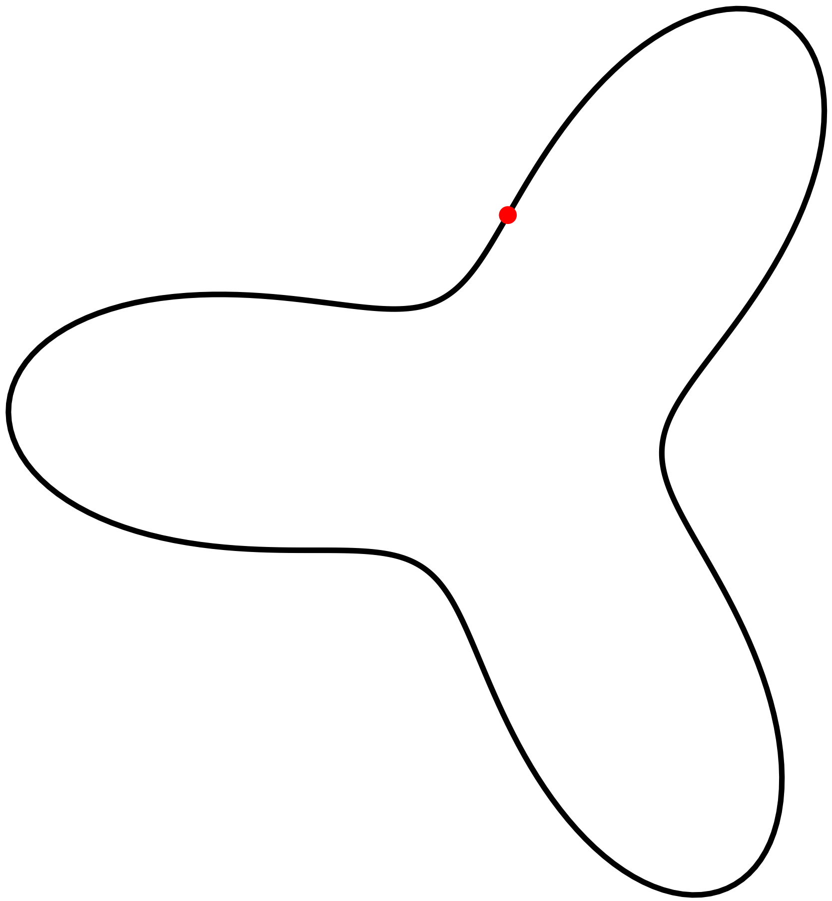
This results in a special geometry.

A Feature of the Klein Quartic



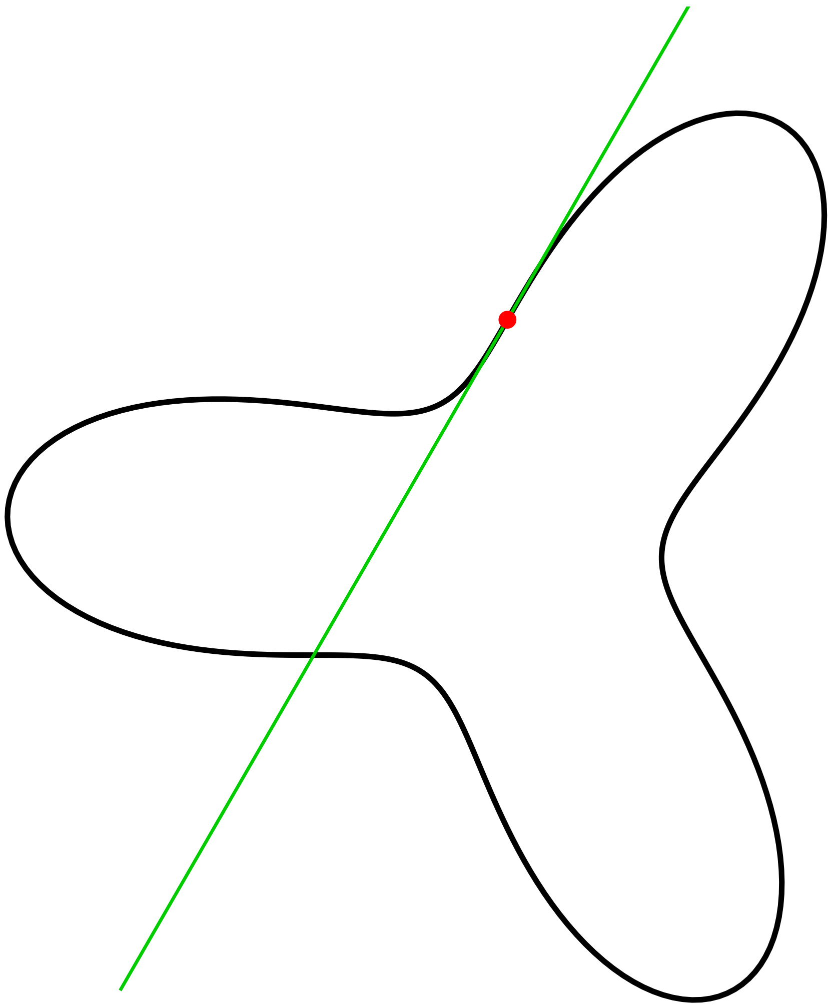
The Klein Quartic

A Feature of the Klein Quartic



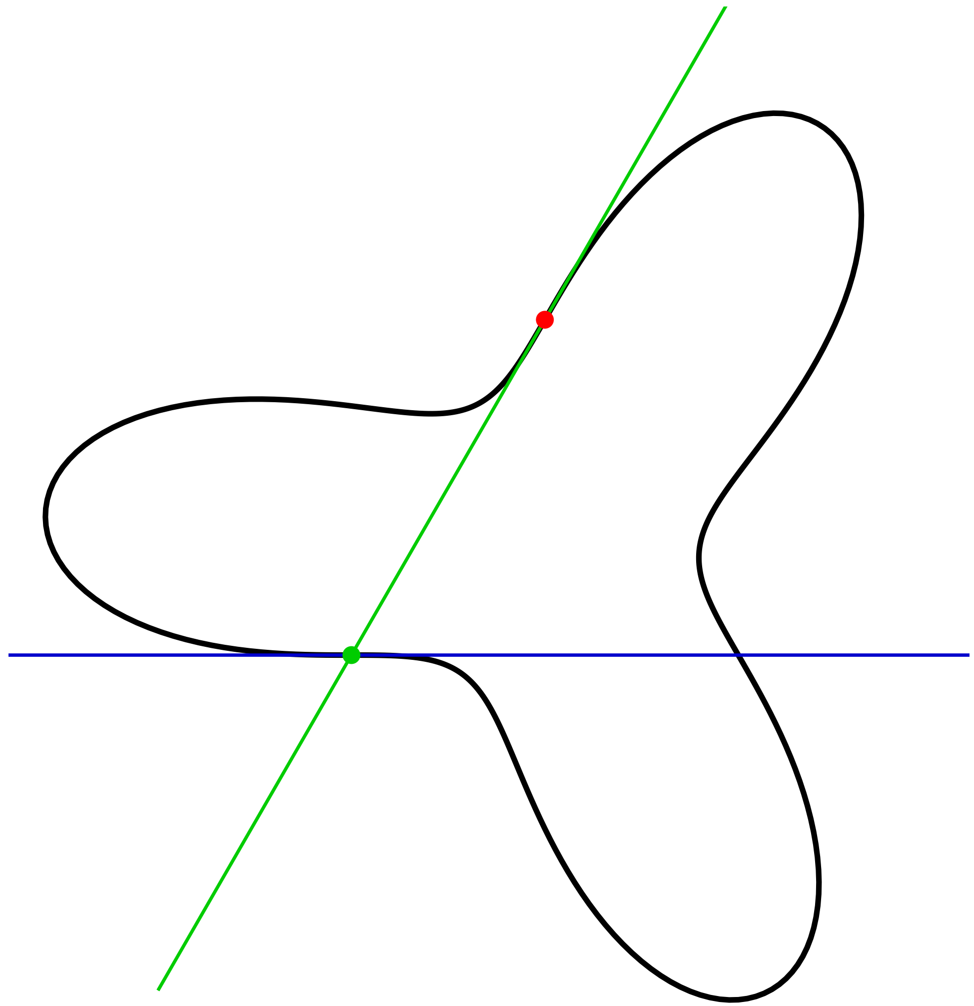
A flex point

A Feature of the Klein Quartic



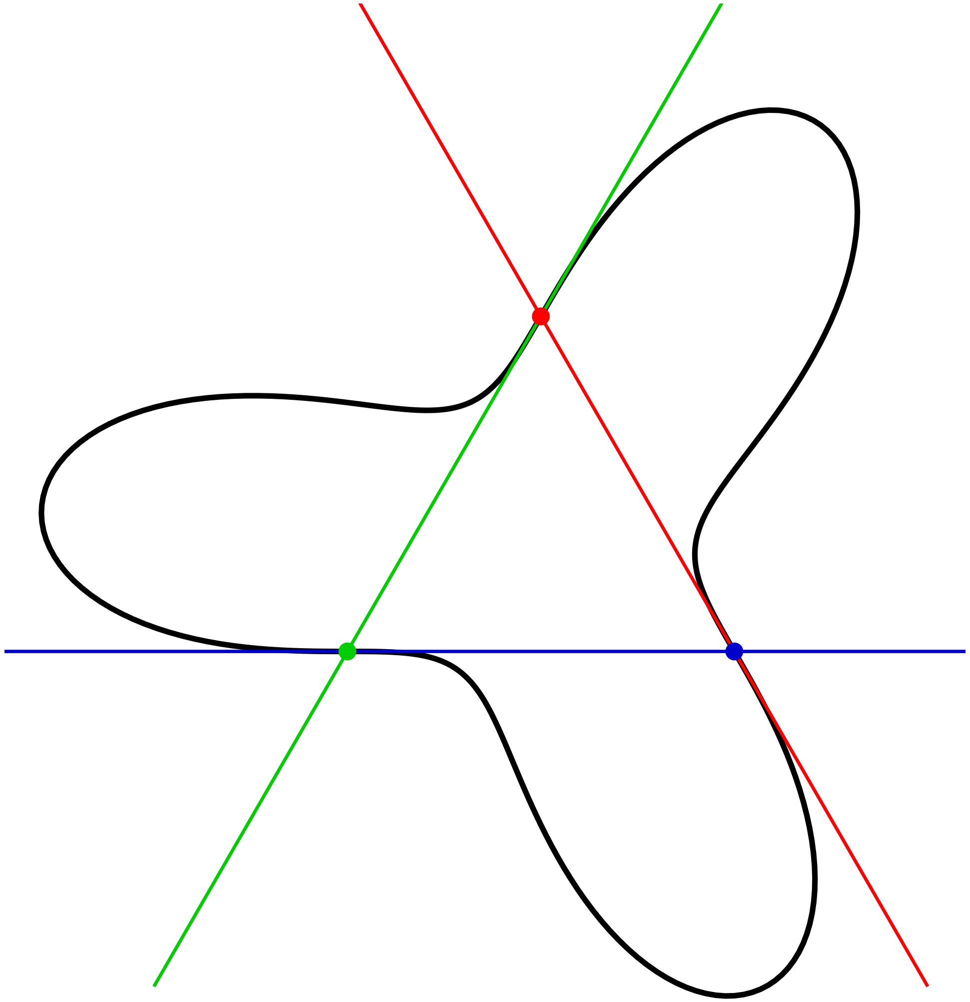
A flex point with its tangent

A Feature of the Klein Quartic



We get another flex point!

A Feature of the Klein Quartic



In the end, we have a “flex triangle”

2-Descent: Structure of $J_j[2]$

Let T_i $(1 \le i \le 8)$ be the eight degree 3 divisors corresponding to the flex triangles on J_j.

Lemma.
Let $V = \mathbb{F}_2 \cdot T_1 \oplus \cdots \oplus \mathbb{F}_2 \cdot T_8$; this is a Galois module.
Consider

$$\mathbb{F}_2 \xrightarrow{\alpha} V \xrightarrow{\beta} \mathbb{F}_2$$

where $\alpha(1) = T_1 + \cdots + T_8$ and $\beta(a_1 T_1 + \cdots + a_8 T_8) = a_1 + \cdots + a_8$.
Then $J_j[2] \cong \ker(\beta) / \operatorname{im}(\alpha)$ as a Galois module.

This is completely analogous to *hyperelliptic* genus 3 curves (where the T_i are replaced by the Weierstrass points).

Hence we can transfer the 2-descent method from hyperelliptic curves to our Klein Quartic twists.

2-Descent: More detail

To carry out the 2-descent, we need a suitable function F on X_j.

Fix a basepoint $P_0 \in X_j(\mathbb{Q})$.
Fit a cubic F_i through $3P_0 + 2T_i$.
Then $\mathrm{div}(F_i) = 2T_i + (3P_0 + R)$, where R is rational and independent of i.

Usually, all the T_i are conjugate. Assume this.
Set $T = T_1$ and $K = \mathbb{Q}(T)$ the corresponding octic number field.
Then $F = F_1/z^3$ is defined over K and induces a homomorphism

$$F : J_j(\mathbb{Q})/2J_j(\mathbb{Q}) \longrightarrow \ker\Big(N_{K/\mathbb{Q}} : K^\times/(K^\times)^2\mathbb{Q}^\times \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\Big)$$

with kernel of order 2 generated by $[R - 3P_0]$
and image contained in the subgroup unramified outside $\{2, 3, 7\}$.

We compute the 2-Selmer group in the usual way
and get a bound on the rank of $J_j(\mathbb{Q})$.

2-Descent and Chabauty: Results

Our 2-descent, applied to X_j, gives the following.

Proposition.
For all $1 \leq j \leq 10$, the subgroup of $J_j(\mathbb{Q})$ generated by divisors supported in the known rational points has finite index.

We have (with $r_j = \operatorname{rank} J_j(\mathbb{Q})$)

$$\begin{aligned} r_1 = r_2 = r_3 &= 1 \\ r_4 = r_6 = r_7 = r_8 = r_9 = r_{10} &= 2 \\ r_5 &= 3 \end{aligned}$$

Knowing this, we can use Chabauty on nine of the curves:

Proposition. For $1 \leq j \leq 10$, $j \neq 5$, the listed points exhaust $X_j(\mathbb{Q})$.

The Last Curve

It remains to deal with the last curve:

$$X_5 : -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0$$

Here, we have

$$\begin{aligned} Y_5(\mathbb{Q}) = \{P \in X_5(\mathbb{Q}) : & P \equiv (0:1:0) \text{ mod } 3, \\ & P \equiv (1:0:0) \text{ or } (1:1:1) \text{ mod } 2\} \end{aligned}$$

The known points in $X_5(\mathbb{Q})$,

$$(1:0:0)\,, \quad (0:1:0)\,, \quad (0:0:1)\,, \quad (1:1:1)\,,$$

all violate one of the conditions.

Can we show that $Y_5(\mathbb{Q})$ is empty?

The Idea

We have $J_5(\mathbb{Q}) \cong \mathbb{Z}^3$. Let P_1, P_2, P_3 be generators.
We have a map

$$\iota : X_5(\mathbb{Q}) \ni P \longmapsto [P - P_0] \in J_5(\mathbb{Q}) \xrightarrow{\cong} \mathbb{Z} \cdot P_1 \oplus \mathbb{Z} \cdot P_2 \oplus \mathbb{Z} \cdot P_3 \,.$$

So $\iota(P) = \iota_1(P)\, P_1 + \iota_2(P)\, P_2 + \iota_3(P)\, P_3$.
Let us find conditions on these coefficents!

For a prime p, we can find finite groups G_p such that

$$\phi_p : J_5(\mathbb{Q}) \hookrightarrow J_5(\mathbb{Q}_p) \longrightarrow\!\!\!\!\to G_p$$

On the other hand, $\quad Y_5(\mathbb{Q}) \hookrightarrow Y_5(\mathbb{Q}_p) \quad (= X_5(\mathbb{Q}_p)$ if $p \neq 2, 3)$
maps to a certain subset $S_p \subset G_p$.

Now $\quad \iota(Y_5(\mathbb{Q})) \subset \bigcap_p \phi_p^{-1}(S_p)$,
and $\phi_p(n_1 P_1 + n_2 P_2 + n_3 P_3) \in S_p$ gives congruence conditions on n_1, n_2, n_3.

Choosing G_p

We need to bring in the conditions at 2 and 3,
so we need to consider suitable G_2 and G_3.

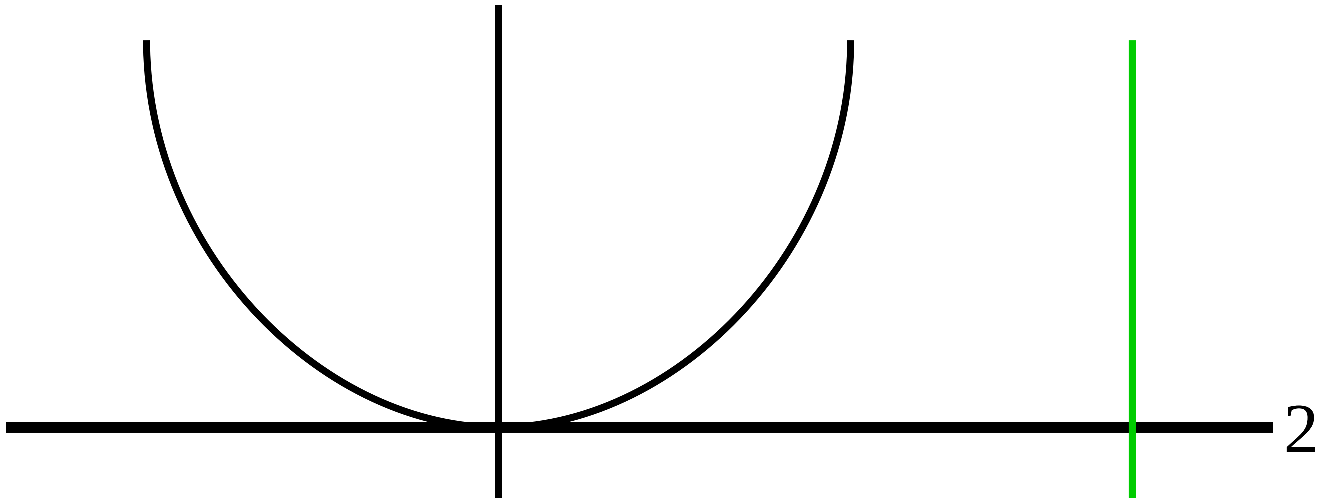
Note that 2 and 3 are primes of bad reduction,
so some work is required.

For additional p of good reduction,
we can simply take $G_p = J_5(\mathbb{F}_p)$ or a quotient of it;
then $S_p = \iota(X_5(\mathbb{F}_p))$ is the image of the points mod p.

How to get G_3

We need to find the structure of $J_5(\mathbb{Q}_3)$.

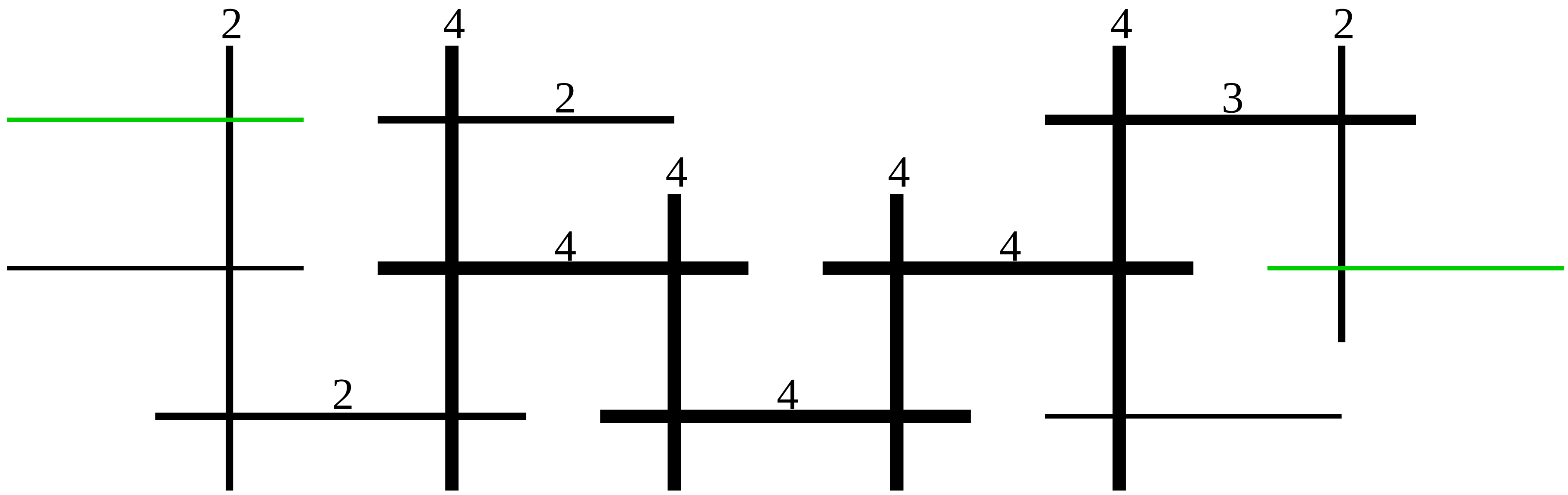
To do this, we compute a minimal regular model of X_5 over $\mathbb{Z}_3$.
The special fiber looks like this:



From this, we find $\Phi_3 \cong \mathbb{Z}/7\mathbb{Z}$;
we set $G_3 = \Phi_3$ and get $n_1 + 3n_3 \equiv 1 \bmod 7$.

How to get G_2

The minimal regular model of X_5 over $\mathbb{Z}_2$ has special fiber



From this, we find $\Phi_2 \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$;
we set $G_2 = \Phi_2$ and get $n_1 + n_2 \equiv 0 \bmod 4$ and $n_3 \equiv 0$ or $1 \bmod 4$.

We need some more primes
to "connect" this mod 7 and mod 4 information.

Auxiliary Primes

Besides

$$J_5(\mathbb{Q}_2) \twoheadrightarrow \Phi_2 \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$
$$J_5(\mathbb{Q}_3) \twoheadrightarrow \Phi_3 \cong \mathbb{Z}/7\mathbb{Z}$$

we find

$$J_5(\mathbb{Q}_{13}) \twoheadrightarrow J_5(\mathbb{F}_{13}) \twoheadrightarrow \mathbb{Z}/14\mathbb{Z}$$
$$J_5(\mathbb{Q}_{23}) \twoheadrightarrow J_5(\mathbb{F}_{23}) \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$
$$J_5(\mathbb{Q}_{97}) \twoheadrightarrow J_5(\mathbb{F}_{97}) \twoheadrightarrow \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$$

and computing the image of $X_5(\mathbb{F}_p)$ in the group on the right, we finally obtain contradictory conditions on n_1, n_2, n_3 mod 14.

Proposition.
$Y_5(\mathbb{Q})$ is empty.