The Uniform Boundedness Conjecture and a result of Poonen

Alex Epelde

January 2024

Abstract

We introduce Morton and Silverman's Uniform Boundedness Conjecture in arithmetic dynamics and discuss some of Poonen's work on the particular case of degree 2 maps of $\mathbb{P}^1$. In particular we go over the full proof of the results in [Poo98], introducing the necessary number-theoretic techniques that get used.

Contents

1 Introduction

This minor thesis revolves around Morton and Silverman's Uniform Boundedness Conjecture for morphisms $\phi : \mathbb{P}^N \to \mathbb{P}^N$. Falling within the realm of arithmetic dynamics, it showcases the sorts of questions one ends up asking which would not make sense in a more general dynamical context.

The precursor to the conjecture is Northcott's theorem [Nor50] on the finiteness of the set of rational pre-periodic points for such morphisms ϕ. In section 2, we discuss this theorem and its proof based on the theory of *heights* of points in $\mathbb{P}^N$.

After stating the conjecture and emphasizing its difficulty, the majority of the minor thesis is devoted to the discussion of a positive result of Poonen in the direction of the conjecture concering the family of quadratic polynomials $f_c(z) = z^2 + c$ [Poo98]. We will see how the question of whether such an f_c can admit a pre-periodic point of a certain type translates into the number-theoretic problem of finding rational points on certain algebraic curves.

The end result is that Poonen is able to give a list of the possible graph types $\mathrm{PrePer}(f_c, \mathbb{Q})$ can exhibit — assuming the conjectural result that f_c may not admit a rational point with period $m \geq 4$. The main theorem is 4.3, and section 4 is devoted to its proof. Along the way, we use a number of results on the rational points of certain elliptic and modular curves.

In the final section 5 we pull out all the stops to count the rational points on a particular genus 2 curve C. This rational point count is a key ingredient in the proof of theorem 4.3 and requires some sophisticated number-theoretic machinery. We run through a descent argument on the Jacobian of C and apply a method of Chabauty and Coleman to effectively control the number of rational points on C.

2 Northcott's theorem

In this section we discuss Northcott's theorem on pre-periodic points of morphisms of $\mathbb{P}^N$ over number fields. This serves to illustrate the difference in flavour between arithmetic dynamics and more traditional complex dynamics. We also find it essential to motivate the uniform boundedness conjecture of Morton and Silverman.

Our main reference throughout is chapter 3 of [Sil07].

Definition 2.1. Let $\phi : X \to X$ be any map. Then $\mathrm{PrePer}(\phi, X)$ is the set of points of X with finite forward orbit under ϕ, i.e.

$$\mathrm{PrePer}(\phi, X) = \{x \in X : \exists\, m + n > n \geq 0 \text{ s.t. } \phi^{m+n}(x) = \phi^n(x)\}.$$

Remark. Here and in the following, ϕ^n stands for the n-fold iterate of ϕ.

Theorem 2.2 [Nor50]**.** *Fix a number field K and let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over K. Then the set* $\mathrm{PrePer}\left(\phi, \mathbb{P}^N(K)\right)$ *of pre-periodic K-points of ϕ is finite.*

This is in contrast with the situation over an algebraically closed field, e.g. the complex numbers $\mathbb{C}$. For example, the solutions to $\phi^m(x) = x$ are given by the intersection in $\mathbb{P}^N \times \mathbb{P}^N$ of the diagonal $\Delta_{\mathbb{P}^N}$ and the graph of ϕ^m. Counted with multiplicity, there are hence $d^m + 1$ such solutions over $\mathbb{C}$. We find that ϕ has points with arbitrarily large period.

The proof of theorem 2.2 is based on the theory of *heights* of points in $\mathbb{P}^N(K)$. The height of $P \in \mathbb{P}^N(K)$ is meant to be a measure of its arithmetic complexity. For example, it carries information about the primes that occur in the homogeneous coordinates of P.

We prepare by introducing some terminology from number theory.

Definition 2.3. The set $M_{\mathbb{Q}}$ of *standard absolute values on* $\mathbb{Q}$ contains

- one Archimedean absolute value: the restriction of the usual absolute value on $\mathbb{R}$

$$|x|_\infty = \max\{x, -x\},$$

- and, for each prime p, the p-adic absolute value

$$\left|\frac{a}{b}\right|_p = p^{v_p(b) - v_p(a)},$$

where v_p is the p-adic valuation: $p^{v_p(a)}$ is the highest power of p dividing a.

Definition 2.4. Let K be a number field. The set M_K of *standard absolute values on K* consists of those absolute values on K whose restriction to $\mathbb{Q}$ is standard.

Definition 2.5. Let K be a number field and let $v \in M_K$. Then the *local degree* of v is given by

$$n_v = [K_v : \mathbb{Q}_v],$$

where K_v, $\mathbb{Q}_v$ denote the respective completions of K, $\mathbb{Q}$ with respect to v.

We are now ready to define the height function H_K.

Definition 2.6. Let $P \in \mathbb{P}^N(K)$ have homogeneous coordinates $(x_0 : \cdots : x_N)$, with $x_i \in K$. Then the *height of P relative to K* is

$$H_K(P) := \prod_{v \in M_K} \max\left\{ |x_0|_v, \ldots, |x_N|_v \right\}^{n_v}.$$

Remark. One shows this definition is independent of the choice of homogeneous coordinates for P. The key fact one needs is that for all non-zero $\alpha \in K$, one has $\prod_{v \in M_K} |\alpha|_v^{n_v} = 1$.

This identity also serves to prove that $H_K(P) \geq 1$ for all P.

Example 2.7. Let us consider the situation for $K = \mathbb{Q}$. Then given $P \in \mathbb{P}^N(\mathbb{Q})$, we can find homogeneous coordinates $(x_0 : \cdots : x_N)$ for P where the x_j are integers and have no common prime factor.

It follows that for each prime p, all of the $|x_j|_p$ are at most 1, and that equality is attained for some j. Hence the formula for $H(P) := H_{\mathbb{Q}}(P)$ reduces to

$$H(P) = \max\left\{ |x_0|_\infty, \ldots, |x_N|_\infty \right\}.$$

The key properties of the height function $H_K : \mathbb{P}^N(K) \to \mathbb{R}$ we will use to prove Northcott's theorem are summarised in the following proposition.

Proposition 2.8. *Let K be a number field. Then*

(i) given $B > 0$, the set

$$\{P \in \mathbb{P}^N(K) : H_K(P) \leq B\}$$

of points in $\mathbb{P}^N(K)$ of height at most B is finite, *and*

(ii) moreover if $\phi : \mathbb{P}^N \to \mathbb{P}^N$ is a morphism of degree d defined over K, then there are constants $C_1, C_2 > 0$ such that for all $P \in \mathbb{P}^N(K)$,

$$C_1 H_K(P)^d \leq H_K(\phi(P)) \leq C_2 H_K(P)^d.$$

Proof. Given example 2.7, part (i) is easy to establish over $\mathbb{Q}$. For the proof in the case of a general number field K, see chapter 3 of [Sil07]. The idea is to reduce to the case $K = \mathbb{Q}$ by considering the minimal polynomials of the coordinates of $P \in \mathbb{P}^N(K)$.

Let us prove (ii) in the case $K = \mathbb{Q}$.

The morphism ϕ is represented by a tuple $(f_0, \ldots, f_N)$ of homogeneous polynomials of degree d with coefficients in $\mathbb{Q}$ and no common factor. Clearing denominators, we may assume all the coefficients of the f_i are in $\mathbb{Z}$.

Now fix $P \in \mathbb{P}^N$ with homogeneous coordinates $(x_0 : \cdots : x_N)$, where the $x_j \in \mathbb{Z}$ have no common prime factor. Let $M_2 > 0$ be a constant greater in absolute value than all of the coefficients appearing in the f_i. Then for each i we have the bound

$$|f_i(x_0, \ldots, x_N)| \leq \binom{N+d}{d} M_2 \left(\max_{0 \leq j \leq N} |x_j| \right)^d,$$

where $\binom{N+d}{d}$ is the number of monomials of degree d in $N+1$ variables.

By assumption, the $f_i(x_0, \ldots, x_N)$ are all integers. They may have a common prime factor, but we can still deduce the bound

$$H(\phi(P)) \leq C_2 H(P)^d$$

with the constant $C_2 = \binom{N+d}{d} M_2$.

For the bound in the other direction, we need to use the assumption that ϕ is a morphism out of $\mathbb{P}^N$. That is, that the common zero locus of $f_0, \ldots, f_N$ in $\mathbb{P}^N$ is empty.

Warning. This is not merely the statement that there is no $\mathbb{Q}$-rational point at which the f_i all vanish! Put this way, what we use is that there is no point of $\mathbb{P}^N(\overline{\mathbb{Q}})$ at which the f_i all vanish.

By the Nullstellensatz, we have $\sqrt{(f_0, \ldots, f_N)} = (X_0, \ldots, X_N)$ as ideals in $\mathbb{Q}[X_0, \ldots, X_N]$. So there are $e \geq 1$ and $\widetilde{g_{ij}} \in \mathbb{Q}[X_0, \ldots, X_N]$ homogeneous of degree $e - d$ such that

$$X_j^e = \sum_{i=0}^{N} \widetilde{g_{ij}} f_i.$$

Clearing denominators, we can find $a \in \mathbb{Z}$ with

$$aX_j^e = \sum_{i=0}^{N} g_{ij} f_i, \tag{$*$}$$

and where the g_{ij} now have integer coefficients.

Let $P \in \mathbb{P}^N$ have homogeneous coordinates $(x_0 : \cdots : x_N)$ as above. Let $b \in \mathbb{Z}$ be the gcd of the $f_i(x_0, \ldots, x_N)$. Observe that by ($*$), we have the uniform bound $|b| \leq |a|$. And let $M_1 > 0$ be greater in absolute value than all of the coefficients appearing in the g_{ij}. We obtain

$$\begin{aligned} |a|\,|x_j|^e &\leq N \binom{N+d-e}{d-e} M_1 \left(\max_{0 \leq j \leq N} |x_j| \right)^{d-e} \left(\max_{0 \leq i \leq N} |f_i(x_0, \ldots, x_N)| \right) \\ &= N \binom{N+d-e}{d-e} M_1 \, H(P)^{d-e} \;\; |b| \;\; H(\phi(P)). \end{aligned}$$

Taking the maximum of the left-hand-side over j, moving terms around, the inequality

$$C_1 H(P)^d \leq H(\phi(P))$$

follows, with

$$C_1 = \frac{1}{N \binom{N+d-e}{d-e} M_1}.$$

□

Remark. Part (ii) of proposition 2.8 is a statement about the geometric significance of the function H_K. Of note is the fact that the bound $H_K(\phi(P)) \leq C_2 H_K(P)^d$ holds under the assumption just that ϕ be a rational map defined at P, and not necessarily a morphism.

Given these properties of H_K, the proof of theorem 2.2 is quite easy.

Proof of theorem 2.2. If $H_K(P)^{d-1} > 1/C_1$, then using the lower bound in proposition 2.8 we see that the sequence of heights $H_K(\phi^n(P))$ diverges to infinity.

It follows that the elements of $\mathrm{PrePer}(\phi, \mathbb{P}^N(K))$ are of bounded height. By the first part of proposition 2.8, the theorem follows. □

3 The Conjecture

Given a particular morphism $\phi : \mathbb{P}^N \to \mathbb{P}^N$ of degree $d \geq 2$ defined over K, the proof of proposition 2.8 gives an explicit way to compute the values of the constants C_1, C_2. From this, we can obtain quantitative bounds on the size of $\mathrm{PrePer}(\phi, \mathbb{P}^N(K))$. This is of course quite sensitive to the coefficients of the morphism ϕ in question.

Nevertheless, Morton-Silverman put forward the following conjecture: no matter which ϕ one takes, the size of $\mathrm{PrePer}\left(\phi, \mathbb{P}^N(K)\right)$ should be controlled by the degree of ϕ alone.

Conjecture 3.1 [MS94]**.** *Fix integers $d \geq 2$, $N \geq 1$ and $D \geq 1$. Then there is a constant $C(d, N, D)$ such that for all number fields K with $[K : \mathbb{Q}] \leq D$ and all morphisms $\phi : \mathbb{P}^N \to \mathbb{P}^N$ of degree d defined over K, we have the uniform bound*

$$\#\,\mathrm{PrePer}\left(\phi, \mathbb{P}^N(K)\right) \leq C(d, N, D).$$

This is a very strong uniformity conjecture. Very little is known about it and positive results are sparse. In section 4 we will see how results of Poonen and others can be used to attack a certain family of quadratic maps on $\mathbb{P}^1$.

Remark. The only non-trivial family of maps for which the conjecture is known to hold is the family of Lattès maps. A map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is Lattès if it arises as a quotient of an affine map $L : E \to E$ on an elliptic curve E under a cyclic group action.

Writing $E(\mathbb{C}) = \mathbb{C}/\Lambda$, the simplest example would be to take the multipication-by-2 map $L(z) = 2z$, together with the $\mathbb{Z}/2\mathbb{Z}$-action on E via $z \mapsto -z$. The pre-periodic points of the resulting degree 4 Lattès map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ are the images of the torsion points of E under the quotient map $E \to \mathbb{P}^1$. The uniform bounds on the size of $\mathrm{PrePer}(\phi, \mathbb{P}^1(K))$ then come from important results of Mazur [Maz77] and Merel [Mer96] on the size of the torsion groups $E_{\mathrm{tors}}(K)$ of elliptic curves over number fields K.

4 The family $f_c(z) = z^2 + c$

Conjecture 3.1 remains quite intractable. Even for the family of quadratic polynomials

$$f_c(z) = z^2 + c, \quad c \in \mathbb{Q},$$

we have no uniform bound on the number of pre-periodic rational points. A first step would be a proof of the following [FPS97].

Conjecture 4.1. *If $n \geq 4$, then there is no quadratic polynomial $f(z) \in \mathbb{Q}[z]$ with a rational point of exact period n.*

This conjecture has been proven for $n = 4$ [Mor98] and $n = 5$ [FPS97].

Another approach towards constraining the dynamics over $\mathbb{Q}$ of this family is taken in [Poo98]. Observe that the set of rational pre-periodic points $\mathrm{PrePer}(f_c, \mathbb{Q})$ is naturally made into a directed graph by f_c. Poonen restricts the possible graph types that occur.

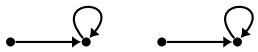
In general, Poonen studies which values of c admit pre-periodic points of a given type. For example, the possibility of a 3-cycle and a 2-cycle occurring at the same time is ruled out. To state the results, we use the following terminology.

Definition 4.2. Let $\phi : X \to X$ be any map, $m \geq 1$, $n \geq 0$. We say $x \in X$ is a *pre-periodic point of type m_n* if x enters an m-cycle after n iterations of ϕ. That is, if $\phi^n(x)$ is a periodic point with exact period m while any $\phi^k(x)$ with $k < n$ is not periodic.

Theorem 4.3 [Poo98]. *Let $f_c(z) = z^2 + c$. Write* $\mathrm{PrePer}^*(f_c, \mathbb{Q})$ *for the subgraph of* $\mathrm{PrePer}(f_c, \mathbb{Q})$ *consisting of those pre-periodic points of types m_n with $m \leq 3$.*

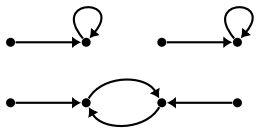
Then, generically, $\mathrm{PrePer}^*(f_c, \mathbb{Q})$ *is one of the following:*

[the empty graph] — *if f_c has no rational points of period $m \leq 3$, e.g. $c = 1$,*

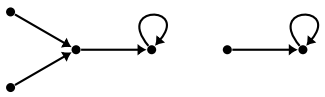


if f_c has rational fixed points but neither rational type 1_2 nor period 2 points, e.g. $c = -3/4$,

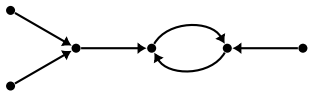
if f_c has rational points of period 2 but neither rational fixed nor type 2_2 points, e.g. $c = -7/4$,



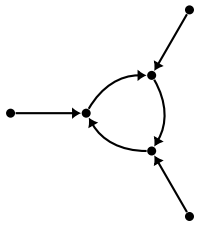
if f_c has both rational fixed points and rational points of period 2, e.g. $c = -21/16$,



if f_c has rational points of type 1_2, e.g. $c = -10/9$,

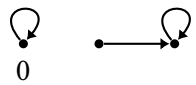


if f_c has rational points of type 2_2, e.g. $c = -13/9$,

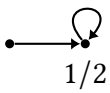


if f_c has rational points of period 3, e.g. $c = -301/144$.

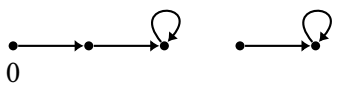
Other than these, there is a finite number of exceptional values of c for which $\mathrm{PrePer}^*(f_c, \mathbb{Q})$ *is not covered by the above. These graphs are*



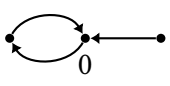
for $c = 0$,



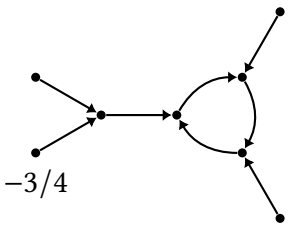
for $c = 1/4$,



for $c = -2$,



for $c = -1$,



for $c = -29/16$.

The proof of theorem 4.3 is composed of a number of smaller lemmas. The general idea throughout is that pairs (c, ι) with $c \in \mathbb{Q}$ and $\iota : G \to \mathrm{PrePer}^*(f_c, \mathbb{Q})$ an embedding of G as a subgraph correspond to rational points on a suitable algebraic curve $C_1(G)$.

In a few cases, $C_1(G)$ has genus 0 and it is an easy task to parametrize its rational points. Other times $C_1(G)$ is recognised as birational to an elliptic curve and Poonen can refer to the extensive literature on rational points of elliptic curves.

In further cases yet, $C_1(G)$ is recognized as birational to a genus 2 *modular curve*. Thanks to important results in arithmetic geometry, one is then able to effectively control the number of rational points on $C_1(G)$ and deduce results about the behaviour of $\mathrm{PrePer}^*(f_c, \mathbb{Q})$. This is also the method used in [Mor98] to rule out the presence of rational points of period 4.

However, when studying the behaviour of rational type 3_2 points, the resulting genus 2 curve $C_1(G)$ is not modular. To compute its rational points, [Poo98] follows the approach in [FPS97] of performing descent on the Jacobian of $C_1(G)$ to bound its rank to then apply a refinement of a method of Chabauty and Coleman.

The remainder of this section follows [Poo98] unless indicated otherwise.

4.1 Periodic points

First we have some results telling us the values of c for which f_c has a rational point of period m with $m \leq 3$, and how many of each kind can occur at one time.

Lemma 4.4 [WR94]**.**

(i) The map f_c has a rational fixed point if and only if $c = \frac{1}{4} - \rho^2$ for some $\rho \in \mathbb{Q}$. In this case, there are exactly two of them at $\frac{1}{2} \pm \rho$, except when $\rho = 0$, where they coincide.

(ii) The map f_c has a rational point of period 2 if and only if $c = -\frac{3}{4} - \sigma^2$ for some non-zero $\sigma \in \mathbb{Q}$. In this case, there are exactly two of them at $-\frac{1}{2} \pm \sigma$.

Proof. In each case we seek the roots of a quadratic equation, namely

$$x^2 - x + c = 0 \qquad \text{for part (i), and}$$

$$\frac{f_c^2(x) - x}{f_c(x) - x} = x^2 + x + (c+1) = 0 \qquad \text{for part (ii).}$$

The only subtle point is that the equations share a root if $c = -\frac{3}{4}$; the common root being $x = -\frac{1}{2}$. This is what rules out $\sigma = 0$ in part (ii) of the statement. □

The characterisation of those values of c for which f_c has a rational point of period 3 is slightly more involved.

Lemma 4.5 [WR94; Mor92]**.** *The map f_c has a rational point of period 3 if and only if*

$$c = -\frac{\tau^6 + 2\tau^5 + 4\tau^4 + 8\tau^3 + 9\tau^2 + 4\tau + 1}{4\tau^2(\tau+1)^2}$$

for some $\tau \in \mathbb{Q} \setminus \{-1, 0\}$. In this case, there are exactly three such points at

$$x_1 = \frac{\tau^3 + 2\tau^2 + \tau + 1}{2\tau(\tau+1)}, \qquad x_2 = \frac{\tau^3 - \tau - 1}{2\tau(\tau+1)}, \qquad x_3 = -\frac{\tau^3 + 2\tau^2 + 3\tau + 1}{2\tau(\tau+1)}.$$

Proof. Checking that for such c the given x_i form a rational 3-cycle is a matter of computation. That all rational 3-cycles of f_c arise in this way is an elementary manipulation [WR94].

What is harder to pin down is the fact that there can be no more than one rational 3-cycle for a given value of c. Theorem 3 of [Mor92] establishes that the degree 6 polynomial

$$\Phi_{3,f_c}(x) := \frac{f_c^3(x) - x}{f_c(x) - x}$$

never splits completely over $\mathbb{Q}$.

So in the case where f_c has a rational 3-cycle as above, $\Phi_{3,f_c}(x)$ is the product of 3 linear factors and an irreducible degree 3 piece. This concludes the proof. Put another way, f_c does have another 3-cycle over $\mathbb{C}$, say; it is simply not contained in $\mathbb{Q}$. □

Remark. Just for fun, here is the cubic polynomial whose irreducibility for all $\tau \in \mathbb{Q} \setminus \{-1, 0\}$ is asserted by the second part of the proof of lemma 4.5:

$$\begin{aligned} & x^3 \; + \; (\tau^3 + 2\tau^2 - \tau - 1)\, x^2 \\ & + (-\tau^6 - 2\tau^4 - 14\tau^3 - 17\tau^2 - 6\tau - 1)\, x \\ & + (-\tau^9 - 2\tau^8 - \tau^7 - 9\tau^6 - 19\tau^5 + 26\tau^3 + 21\tau^2 + 7\tau + 1)\,. \end{aligned}$$

Lemma 4.6 [Poo98]**.** *The map f_c has both a rational fixed point and a rational point of period 2 if and only if*

$$c = -\frac{3\mu^4 + 10\mu^2 + 3}{4(\mu^2 - 1)^2}$$

for some $\mu \in \mathbb{Q} \setminus \{-1, 0, 1\}$.

Proof. By lemma 4.4, such c give rise to a rational point (ρ, σ) on

$$\tfrac{1}{4} - \rho^2 = -\tfrac{3}{4} - \sigma^2.$$

This is a conic with a rational point at $(1, 0)$, so we can parametrise it via $\mu = \frac{1-\rho}{\sigma}$. The general rational solution becomes

$$\rho = \frac{1 + \mu^2}{1 - \mu^2}, \quad \sigma = \frac{-2\mu}{1 - \mu^2}, \quad \mu \in \mathbb{Q},$$

giving c of the desired form.

The values $\mu = \pm 1$ are ruled out since they correspond to points at infinity on the conic. And $\mu = 0$ is ruled out since it has $\sigma = 0$ and hence no rational 2-cycle. □

Lemma 4.7 [Poo98]**.** *If the map f_c has a rational point of period 3, then it does not have either a rational fixed point or a rational point of period 2.*

Proof. Assume first that f_c has both a rational fixed point and a rational point of period 3. Then by lemmas 4.4, 4.5, we get a rational point (ρ, τ) on

$$\tfrac{1}{4} - \rho^2 = -\frac{\tau^6 + 2\tau^5 + 4\tau^4 + 8\tau^3 + 9\tau^2 + 4\tau + 1}{4\tau^2(\tau + 1)^2}.$$

After some manipulation, we find that $(\tau, 2\tau(\tau + 1)\rho)$ is a rational point on the curve

$$C \;:\; y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1. \qquad (*)$$

It turns out, remarkably, that C is a model for the modular curve $X_1(18)$. One result in the landmark paper [Maz77] of Mazur is that the only rational points on the modular curves $X_1(m)$ with $m = 11$ or $m \geq 13$ are the *rational cusps*.

For the case at hand, this gives exactly 6 rational points on $X_1(18)$. Now, since the degree of the right-hand side in (∗) is even, we read off that C has 2 points at infinity in its smooth model — consider the map to $\mathbb{P}^1$ given by projection onto the x-coordinate. Since the leading coefficient of this right-hand side is a square, these points are rational, and we can also spot

$$(-1, \pm 1) \quad \text{and} \quad (0, \pm 1).$$

It follows that these are all the rational points on C.

Since $\tau = -1, 0$ are ruled out by lemma 4.5, this establishes that f_c cannot have both a rational fixed point and a rational point of period 3.

If, instead, we assume f_c has rational points with periods both 2 and 3, we get a rational solution (σ, τ) to

$$-\tfrac{3}{4} - \sigma^2 = -\frac{\tau^6 + 2\tau^5 + 4\tau^4 + 8\tau^3 + 9\tau^2 + 4\tau + 1}{4\tau^2(\tau+1)^2}$$

and from this that the point $(\tau, 2\tau(\tau+1)\sigma)$ lies on

$$C' \ : \ y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1.$$

This time C' is birational to $X_1(13)$, which has again 6 cusps. After spotting

$$(-1, \pm 1) \quad \text{and} \quad (0, \pm 1)$$

on C', the above argument rules out f_c having rational points with periods both 2 and 3 and completes the proof. □

4.2 An aside on modular curves

It is worth pausing after the appearance of the modular curves $X_1(13),\ X_1(18)$ in the above proof. Let us give some brief exposition on their definition and what the original motivation for working with them in [Maz77] was.

Definition 4.8. The *modular group* Γ is the quotient $\mathrm{SL}(2, \mathbb{Z})/\{\pm \mathrm{Id}\}$.

The group Γ acts on the upper half plane $\mathbb{H} \subset \mathbb{C}$ by fractional linear transformations. The quotient space $\Gamma\backslash\mathbb{H}$ is canonically made into a Riemann surface and classifies elliptic curves over $\mathbb{C}$. Indeed, here $\tau \in \mathbb{H}$ corresponds to $E_\tau := \mathbb{C}/\Lambda_\tau$ where Λ_τ is the lattice $\mathbb{Z} \oplus \mathbb{Z}\tau$. The curves $E_\tau, E_{\tau'}$ are isomorphic precisely when τ, τ' are related via the action of Γ.

One can extend Γ to act on the *extended upper half plane* $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. The result is that the Riemann surface $X(1) := \Gamma\backslash\mathbb{H}^*$ is a compactification of the above moduli space by adding a single *cusp* at infinity (Γ acts transitively on $\mathbb{Q} \cup \{\infty\}$).

Going further, one observes $X(1)$ has genus 0. The *j-invariant* gives an explicit isomorphism with $\mathbb{P}^1$ and is used to build a model $X(1)_{\mathbb{Q}}$ defined over $\mathbb{Q}$. An elliptic curve defined over $\mathbb{Q}$ yields a rational point on $X(1)_{\mathbb{Q}}$.

Warning. This is not important for our discussion, but one should note $X(1)_{\mathbb{Q}}$ is *not* in any sense the moduli space of elliptic curves over $\mathbb{Q}$. The issue is that an isomorphism of elliptic curves over $\mathbb{C}$ does not translate to one over $\mathbb{Q}$.

Now we introduce the congruence subgroups $\Gamma(N), \Gamma_1(N) \subset \Gamma$.

Definition 4.9. The *principal congruence subgroup of level N* is

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : a \equiv d \equiv 1,\ b \equiv c \equiv 0 \pmod N \right\}.$$

The related group $\Gamma_1(N)$ is given by

$$\Gamma_1(N) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : a \equiv d \equiv 1,\ c \equiv 0 \pmod{N} \right\}.$$

The significance of these subgroups is the following. Given $\tau \in \mathbb{H}$, we can build not only the curve E_τ, but also give it extra structure. We can for example remember the pair $\left(E_\tau, \frac{1}{N} + \Lambda_\tau\right)$ of an elliptic curve together with a point of order N for the group structure. The statement then is that τ, τ' are related via the action of $\Gamma_1(N)$ if and only if the corresponding pairs are isomorphic.

The quotient space $X_1(N) \coloneqq \Gamma_1(N)\backslash\mathbb{H}^*$ becomes a moduli space for elliptic curves *with level structure*. It classifies elliptic curves together with an element of order N in the group law. An important point is that in general $\mathbb{Q} \cup \{\infty\}$ will split into several orbits under the action of $\Gamma_1(N)$. The corresponding points on $X_1(N)$ are the so-called *cusps* and correspond to degenerations of elliptic curves.

Remarkably, as was the case with $X(1)$, the modular curve $X_1(N)$ admits a canonical model over $\mathbb{Q}$. The function field of $X_1(N)$ is generated over $\mathbb{C}$ by two elements satisfying a polynomial equation with $\mathbb{Z}$ coefficients. Now an elliptic curve E defined over $\mathbb{Q}$ carrying a rational point of order N in the group law determines a rational point on the resulting $X_1(N)_{\mathbb{Q}}$.

Mazur's result [Maz77] that the only rational points on $X_1(N)_{\mathbb{Q}}$ for $N = 11$ or $N \geq 13$ are the cusps translates into the statement that an elliptic curve E over $\mathbb{Q}$ cannot have such $\mathbb{Z}/N\mathbb{Z}$ as a subgroup of $E(\mathbb{Q})$. It is surprising to see these curves appear in the study of the periodic points of $f_c(z) = z^2 + c$, and moreover ruling out the presence of certain subgraphs G of $\mathrm{PrePer}(f_c, \mathbb{Q})$ just as Mazur rules out the presence of subgroups of $E(\mathbb{Q})$.

4.3 Pre-periodic points

We return to the proof of theorem 4.3. First off we deal with the cases where $z = 0$ is a pre-periodic point of f_c — this is behind most of the exceptional graphs of theorem 4.3. We then start to look at what sorts of rational pre-periodic points f_c can admit.

Lemma 4.10. *The only values of $c \in \mathbb{Q}$ for which 0 is a pre-periodic point of f_c are $c = -2, -1, 0$.*

Proof. If c is not an integer, say with the prime p in its denominator, then the orbit of 0 diverges to infinity p-adically. And similarly, if $|c| > 2$, one checks that this time the orbit diverges to infinity in the usual absolute value.

Checking the remaining finitely many values of c completes the proof. □

Lemma 4.11. *Outside of the cases covered by lemma 4.10, there is a bijection between the rational points of period m of f_c and its rational pre-periodic points of type m_1.*

Proof. If x is a rational pre-periodic point of type m_1, then it follows that $f_c^m(x) \neq x$ is the other element of $\mathbb{Q}$ mapping to $f_c(x)$ under f_c. From the form of f_c it follows that

$$f_c^m(x) = -x, \quad x \neq 0.$$

The lemma follows: the desired bijection sends a rational type m_1 point to its negative. □

Now let us see what the consequences of having a rational point of type 1_2 are. This is the first time we encounter an example of $C_1(G)$ with genus 1.

Lemma 4.12 [Poo98]. *The map f_c has a rational point of type 1_2 if and only if*

$$c = \frac{-2(\eta^2+1)}{(\eta^2-1)^2}$$

for some $\eta \in \mathbb{Q} \setminus \{-1, 1\}$. In this case there are exactly two such points at

$$r = \pm \frac{2\eta}{\eta^2-1},$$

except when $\eta = 0$, where they coincide.

In this case f_c does not have a rational point of period 2.

Proof. Let $r \neq 0$ be a rational point of type 1_2 for f_c. By lemma 4.11, $f_c(r) = r^2 + c$ is the negative of a fixed point of f_c. Without loss of generality, write $c = \frac{1}{4} - \rho^2$ c.f. lemma 4.4 and

$$r^2 + \tfrac{1}{4} - \rho^2 = -(\tfrac{1}{2} + \rho).$$

This is the equation for a conic with a rational point at $(r, \rho) = (0, -\frac{1}{2})$. So just as we did in lemma 4.6, introducing the parameter $\eta = \frac{r}{\frac{1}{2}+\rho}$ gives the general rational solution as

$$r = -\frac{2\eta}{\eta^2-1}, \qquad \rho = -\frac{\eta^2+3}{2(\eta^2-1)}$$

and with c of the desired form.

The values $\eta = \pm 1$ are ruled out since they correspond to the points at infinity on the conic. And $\eta = \infty$ is ruled out since it gives $r = 0$ which is covered by lemma 4.10.

Next we consider the possibility of there being further rational type 1_2 points. Any other such point s would have to map to the negative of the other fixed point:

$$s^2 + \tfrac{1}{4} - \rho^2 = -(\tfrac{1}{2} - \rho)$$

from which

$$s^2 = \frac{-\eta^4 + 2\eta^2 + 3}{(\eta^2-1)^2}.$$

Let $t = s(\eta^2 - 1)$ to get a rational point on the curve

$$C \;:\; t^2 = -\eta^4 + 2\eta^2 + 3.$$

We read off the genus of C as 1. Since $(\eta, t) = (1, 2)$ is a rational point on C, it follows that C is birational to an elliptic curve. One can explicitly show that the desired curve is

$$E_{24} \;:\; y^2 = x^3 - x^2 + x.$$

This is curve 24A4 in Cremona's tables [Cre92], where we read off that $E_{24}(\mathbb{Q})$ has order 4. These rational points correspond to $(\eta, t) = (\pm 1, \pm 2)$ on C. Since $\eta = \pm 1$ was ruled out above, it follows that there can be no such additional rational type 1_2 point s.

It remains to show that there can be no rational point of period 2 in the presence of the rational type 1_2 point r. If so, lemma 4.6 gives $\mu \in \mathbb{Q} \setminus \{-1, 0, 1\}$ such that

$$c = -\frac{3\mu^4 + 10\mu^2 + 3}{4(\mu^2-1)^2}, \qquad \rho = \frac{1+\mu^2}{1-\mu^2},$$

and hence a rational solution to

$$r^2 = -(\tfrac{1}{2} + \rho) - c = \frac{5\mu^4 + 14\mu^2 - 3}{4(\mu^2-1)^2}.$$

Let $t = 2r(\mu^2 - 1)^2$ to get a rational point on the curve

$$C' \ : \ t^2 = 5\mu^4 + 14\mu^2 - 3.$$

Once again, this has genus 1 and a rational point at $(\mu, t) = (1, 4)$. So C' is birational to an elliptic curve. The elliptic curve in question is

$$E_{15} \ : \ y^2 + xy + y = x^3 + x^2.$$

This is curve 15A8 in [Cre92], where we read off that $E_{15}(\mathbb{Q})$ has order 4. Since we already have the rational points $(\mu, t) = (\pm 1, \pm 4)$ on C', and $\mu = \pm 1$ is ruled out above, it follows that there can be no rational point of period 2 as desired. □

The next lemma is the analogue of 4.12 for type 2_2 points.

Lemma 4.13 [Poo98]. *The map f_c has a rational point of type 2_2 if and only if*

$$c = \frac{-v^4 - 2v^3 - 2v^2 + 2v - 1}{(v^2 - 1)^2}$$

for some $v \in \mathbb{Q} \setminus \{-1, 0, 1\}$. In this case there are exactly two such points at

$$r = \pm \frac{v^2 + 1}{v^2 - 1}.$$

Moreover in this case f_c does not have a rational fixed point.

Proof. Given the similarity between parts (i) and (ii) of lemma 4.4, it's not surprising that the proof is essentially the same as that of 4.12. We will not go into detail.

Identifying the values of c giving a rational point of type 2_2 corresponds to parametrising the rational points on a suitable genus 0 curve.

Showing that there can be no more than two such points comes from a study of the rational points of an elliptic curve, this time 40A3 in [Cre92].

And finally, ruling out the presence of a rational fixed point also comes from a count of rational points on an elliptic curve, namely 17A4 of [Cre92]. □

The end is within sight. Elliptic curves make an appearance in the following lemma too.

Lemma 4.14 [Poo98]. *The map f_c does not have rational points of type 1_n or 2_n with $n \geq 3$.*

Proof. It is enough to rule out rational points of type 1_3 or 2_3.

Suppose q is a rational type 1_3 point for f_c. Then by lemma 4.12, there is $\eta \in \mathbb{Q} \setminus \{-1, 1\}$ such that

$$q^2 + c = \frac{2\eta}{\eta^2 - 1}, \qquad c = \frac{-2(\eta^2 + 1)}{(\eta^2 - 1)^2}.$$

Hence

$$q^2 = \frac{2(\eta^3 + \eta^2 - \eta + 1)}{(\eta^2 - 1)^2}, \tag{$*$}$$

so that if $t = q(\eta^2 - 1)$ then we obtain a rational point on the elliptic curve

$$C \ : \ t^2 = 2(\eta^3 + \eta^2 - \eta + 1).$$

A linear change of variables lets us recognise C as curve 11A3 in [Cre92], where we read off that C has 5 rational points. These are: the point at infinity, and $(\eta, t) = (\pm 1, \pm 2)$.

Since $\eta = \pm 1$ is ruled out, it follows that f_c does not admit such a point q.

The argument ruling out a rational point of type 2_3 is similar, using lemma 4.13 instead. If q is a candidate rational type 2_3 point, we find $v \in \mathbb{Q} \setminus \{-1, 0, 1\}$ such that

$$q^2 + c = -\frac{v^2+1}{v^2-1}, \qquad c = \frac{-v^4 - 2v^3 - 2v^2 + 2v - 1}{(v^2-1)^2}.$$

This yields the same equation $(*)$ above, at which point we're done.

Remark. Note that the change of variables $v \mapsto -1/v$ leaves c unchanged and flips the sign of the type 2_2 point that q maps to. So the case

$$q^2 + c = \frac{v^2+1}{v^2-1}$$

is covered by the above. □

The following is the last lemma completing the proof of theorem 4.3.

Lemma 4.15. *The map f_c has a rational point of type 3_2 if and only if $c = -29/16$. The graph given in the statement of theorem 4.3 is the full* $\mathrm{PrePer}(f_c, \mathbb{Q})$ *for this value of c.*

Proof. If r is a rational type 3_2 point of f_c, then $r^2 + c$ is the negative of a rational period 3 point. By lemma 4.5, we find $\tau \in \mathbb{Q} \setminus \{-1, 0\}$ such that, without loss of generality,

$$r^2 + c = -\frac{\tau^3 + 2\tau^2 + \tau + 1}{2\tau(\tau+1)}, \qquad c = -\frac{\tau^6 + 2\tau^5 + 4\tau^4 + 8\tau^3 + 9\tau^2 + 4\tau + 1}{4\tau^2(\tau+1)^2}.$$

We obtain

$$r^2 = \frac{\tau^6 - 2\tau^4 + 2\tau^3 + 5\tau^2 + 2\tau + 1}{4\tau^2(\tau+1)^2}$$

and hence deduce that $(\tau, 2r\tau(\tau+1))$ is a rational point on the curve

$$C \ : \ y^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1.$$

We claim that C has exactly 8 rational points: two of them $\infty_\pm$ at infinity, and

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

We devote section 5 to the proof of this fact. With $\tau = -1, 0$ ruled out this leaves

$$\tau = 1, \qquad 2r\tau(\tau+1) = \pm 3,$$

which is the case $c = -29/16$.

The computation of the full graph $\mathrm{PrePer}(f_c, \mathbb{Q})$ in this case is as follows.

Let $x \in \mathrm{PrePer}(f_c, \mathbb{Q})$. If $|x|_2 > 4$, then the orbit of x diverges to infinity in the 2-adic absolute value. Likewise $|x|_p \leq 1$ for all other primes p. And if $|x| \geq 2$ then the orbit of x diverges to infinity in the usual absolute value. This leaves finitely many values of x on which to compute f_c and completes the proof. □

With this lemma, the proof of theorem 4.3 is complete! It remains only to fill in the gap in the proof of lemma 4.15 — we are to count the rational points on the genus 2 curve C. Unfortunately, unlike in lemma 4.7, C is not related to any modular curve $X_1(N)$ and we have to work by hand to bound the size of $C(\mathbb{Q})$.

5 Counting rational points on the genus 2 curve C

In this section we go over the argument in [Poo98] proving that the curve

$$C \ : \ y^2 = g(x), \qquad g(x) \coloneqq x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$$

has exactly 8 rational points, as discussed in lemma 4.15.

It is a landmark result of Faltings [Fal83] that a curve of genus $g \geq 2$, defined over a number field K, has finitely many K-rational points. For our particular curve C, this fact can be deduced from earlier work of Chabauty [Cha41]. Their result is in terms of the Jacobian variety J: if the rank of $J(K)$, as an abelian group, is less than g, then $C(K)$ is finite.

Coleman [Col85] goes on to turn Chabauty's method into an effective technique for giving quantitative bounds on $\#C(K)$. In [FPS97], this is refined and nails down the number of $\mathbb{Q}$-rational points on their curve $C_0(5)$ of interest. This is how they are able to prove no polynomial $f_c(z) = z^2 + c$ has a rational point of period 5.

Our first step then is to bound the rank of $J(\mathbb{Q})$ via a descent argument. In fact, we will prove that $J(\mathbb{Q}) \cong \mathbb{Z}$ in 5.2. The main idea is to find a suitable map out of $J(\mathbb{Q})$ whose kernel approximates $2J(\mathbb{Q})$ and whose image we can control using p-adic methods.

Once this is done, in 5.3 we study the image of $C(\mathbb{Q})$ in $J(\mathbb{Q})$ under a suitable Albanese map j. For each point of the reduction $C(\mathbb{F}_3)$, we find a patch U_i of $J(\mathbb{Q}_3)$ modelled on a 3-adic disc and a power series $\theta_i(n) \in \mathbb{Z}_3[\![n]\!]$ such that points in the image of j within U_i are zeros of θ_i. Our control of the rank of $J(\mathbb{Q})$ implies that the U_i cover the image of j. So using a standard theorem of Strassman to bound the number of zeros of the θ_i will complete the proof.

5.1 The curve $C_0(5)$

As mentioned previously, the method in this section comes from [FPS97], where it is used to count the rational points on

$$C_0(5) \ : \ y^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1.$$

The curve $C_0(5)$ arises as a quotient of $C_1(5)$, the genus 14 curve classifying period 5 points of the family $f_c(z) = z^2 + c$. The equation for $C_1(5)$ in the (z, c) plane is

$$\Phi_{5,f_c}(z) \coloneqq \frac{f_c^5(z) - z}{f_c(z) - z} = 0$$

c.f. the proof of lemma 4.5. The observation is that $\sigma : (z, c) \mapsto (z^2 + c, c)$ defines an order-5 automorphism of $C_1(5)$. Rational points on $C_1(5)$ get sent to rational points on the quotient

$$C_0(5) = C_1(5)/\langle\sigma\rangle.$$

So bounding $\#C_0(5)$ leads directly to a bound on $\#C_1(5)$ and is what enables [FPS97] to rule out the presence of rational points of period 5 for the family f_c.

Remark. Rational points on $C_1(5)$ generically correspond to rational points of period 5 for the family f_c. It is an instructive aside to understand what precisely rational points on $C_0(5)$ mean.

Let $P : \mathrm{Spec}(\mathbb{Q}) \mapsto C_0(5)$ be a rational point on $C_0(5)$.

This admits a lift to a $\overline{\mathbb{Q}}$ point of $C_1(5)$. Fix such a point $\widetilde{P}$ as below.

$$\begin{array}{ccc} \mathrm{Spec}(\overline{\mathbb{Q}}) & \xrightarrow{\widetilde{P}} & C_1(5) \\ \downarrow & & \downarrow \pi \\ \mathrm{Spec}(\mathbb{Q}) & \xrightarrow{P} & C_0(5) \end{array}$$

Now if we act on $\mathrm{Spec}(\overline{\mathbb{Q}})$ via $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, this may change $\widetilde{P}$ but the resulting point must remain in the fiber of P under π. The result is that the fiber of P corresponds not necessarily to a 5-cycle of f_c consisting of rational points, but in general could give a 5-cycle whose elements are Galois conjugate elements of $\overline{\mathbb{Q}}$.

5.2 Descent on the Jacobian $J(C)$

We won't give a careful definition of the Jacobian $J := J(C)$ as an abelian variety over $\mathbb{Q}$. We refer to [Mil86] for details. Important for us will be the following concepts.

Definition 5.1. A $\mathbb{Q}$-*rational divisor* on C is a finite $\mathbb{Z}$-linear of $\overline{\mathbb{Q}}$-points on C

$$D = \sum n_P P, \qquad P \in C(\overline{\mathbb{Q}}),$$

which is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Definition 5.2. A $\mathbb{Q}$-*rational divisor class* on C is a linear equivalence class of $\overline{\mathbb{Q}}$-divisors on C which is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. That is, $[D]$ defines a $\mathbb{Q}$-rational divisor class if for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the divisors D and $\sigma(D)$ are linearly equivalent.

It is important to think carefully through what the above definitions mean. However, it is a pleasant fact that when $C(\mathbb{Q})$ is non-empty (as is the case for us), any $\mathbb{Q}$-rational divisor class may be represented by a $\mathbb{Q}$-rational divisor.

And now, the Jacobian J is an abelian variety over $\mathbb{Q}$ whose set of $\mathbb{Q}$-points $J(\mathbb{Q})$ consists of the degree zero $\mathbb{Q}$-rational divisor classes on C. Familiar from complex algebraic geometry is the fact that the dimension of J coincides with the genus g of C.

Remark. If K is a general field of characteristic 0, the above definitions modify in the obvious way to give the notion of a *K-rational divisor (class)* and we have a similar understanding of the K points of the Jacobian J.

For our first result on $J(\mathbb{Q})$ we need the concept of reduction mod p for C and J. Observe that the equation for C has integer coefficients. So we can just as well reduce mod p throughout and view it as the equation for a curve over $\mathbb{F}_p$.

More generally, note one of the advantages of projective space over affine space is that we have a well-defined map $\mathbb{P}^N(\mathbb{Q}) \to \mathbb{P}^N(\mathbb{F}_p)$: given a point P, find homogeneous coordinates for it $(x_0 : \cdots : x_N)$ with the x_i in $\mathbb{Z}$ and having no common factor c.f. example 2.7.

This reduction map sends varieties over $\mathbb{Q}$ to varieties over $\mathbb{F}_p$. However it need not preserve properties such as irreducibility or smoothness. This motivates the following definition.

Definition 5.3. We say p is a *prime of good reduction* for C if we can find a model for C in $\mathbb{P}^N$ such that the reduced curve C over $\mathbb{F}_p$ is irreducible, non-singular.

For example, the discriminant of $g(x) = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$ is $-2^{12} \cdot 743$, from which it follows that for any finite prime $p \notin \{2, 743\}$ the curve C has good reduction. (In fact, one can also find a suitable model for which the 2-reduction is good.)

Proposition 5.4 [Poo98]**.** *The torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}}$ is trivial.*

Proof. We will use the reduction maps $J(\mathbb{Q}) \to J(\mathbb{F}_p)$ for well-chosen primes p.

The important fact we need is that if p is a prime of good reduction for C and J, the reduction map $J(\mathbb{Q}) \to J(\mathbb{F}_p)$ is injective on torsion (see the appendix in [Kat80], for example).

And computing the size of $J(\mathbb{F}_p)$ is a finite problem we can ask our computer to do.

Now: $\#J(\mathbb{F}_3) = 27$ and $\#J(\mathbb{F}_5) = 43$. Since $\gcd(27, 43) = 1$, the proposition follows. □

Recall that the curve C has two rational points at infinity $\infty_\pm$ in the non-singular model. We distinguish these by letting the rational function y/x^3 take values ± 1 at $\infty_\pm$. Consider the divisor $\infty_+ - \infty_-$. From proposition 5.4 we deduce that $D = [\infty_+ - \infty_-]$ has infinite order in $J(\mathbb{Q})$, so this last group has rank at least 1.

Our aim now is to show that $J(\mathbb{Q}) \cong \mathbb{Z}$ by proving that $\# J(\mathbb{Q})/2J(\mathbb{Q}) = 2$.

Definition 5.5. Let K be a field of characteristic 0 and write $L_K = K[T]/(g(T))$. Let $D = \sum n_P P$ be a divisor on C of degree zero, and whose support does not contain $\infty_\pm$ or any point with zero y-coordinate. Then we set

$$(x - T)(D) = \prod_P (x_P - T)^{n_P} \in L_K^*,$$

where x_P are the x-coordinates of the points P.

Remark. Here L_K need not be a field, if $g(T)$ fails to be irreducible over K. However, in the particular case $L := L_{\mathbb{Q}}$ we *do* get a field.

It is shown in [FPS97] that this definition extends to a map $(x - T) : J(K) \to L_K^*/L_K^{*2}K^*$. We have left K general because we will use $(x - T)$ both for $\mathbb{Q}$ and the completion $\mathbb{Q}_{743}$.

Since $(x - T)$ maps into a 2-group, its kernel contains $2J(K)$. Our next result is that the index of $2J(K)$ in $\ker(x-T)$ can be effectively computed in terms of the behaviour of $g(T)$ over K. This allows us to translate information about $J(K)/2J(K)$ into information about $\ker(x-T)$, and viceversa.

Proposition 5.6 [FPS97]**.** *The index of $2J(K)$ in $\ker(x - T)$ is either*

- 1, *if $g(T)$ has a root over K or if the roots of $g(T)$ in $\overline{K}$ admit a $\mathrm{Gal}(\overline{K}/K)$-stable decomposition into two indistinguishable 3-element subsets $\{\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}\}, \{\alpha_{i_4}, \alpha_{i_5}, \alpha_{i_6}\}$, or*
- 2, *otherwise.*

Proof. For the proof we fix a K-point P of $C : y^2 = g(x)$. [Cas83] shows that $\ker(x - T)$ is generated by $2J(K)$ and the divisor class $[2P - \infty_+ - \infty_-]$.

It follows that the index of $2J(K)$ in $\ker(x - T)$ is at most 2, and that it equals 2 precisely when $[2P - \infty_+ - \infty_-]$ is *not* in $2J(K)$. Now it's a matter of going over the 16 divisor classes in $J(\overline{K})$ with double $[2P - \infty_+ - \infty_-]$ and seeing under which conditions they are K-rational.

If $\alpha_1, \ldots, \alpha_6$ are the roots of $g(T)$ over $\overline{K}$, one checks that these 16 elements of $J(\overline{K})$ are

- $[P + (\alpha_i, 0) - \infty_+ - \infty_-]$ for $1 \le i \le 6$, and
- $[P + (\alpha_1, 0) + (\alpha_j, 0) + (\alpha_k, 0) - 2\infty_+ - 2\infty_-]$ for $1 < j < k \le 6$.

For example, $[2(\alpha_i, 0) - \infty_+ - \infty_-] = 0$ by considering the rational function $x - \alpha_i$, whence

$$2[P + (\alpha_i, 0) - \infty_+ - \infty_-] = [2P - \infty_+ - \infty_-].$$

Now $\mathrm{Gal}(\overline{K}/K)$ acts on the first 6 in the same way as it acts on the roots of $g(T)$, giving the first condition of the statement. The final claim is that the action on the other 10 matches the action on the set of partitions of $\{\alpha_1, \ldots, \alpha_6\}$ into two indistinguishable 3-element subsets.

For this, simply observe that if $\{\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}\}, \{\alpha_{i_4}, \alpha_{i_5}, \alpha_{i_6}\}$ is such a partition, then

$$[(\alpha_{i_1}, 0) + (\alpha_{i_2}, 0) + (\alpha_{i_3}, 0)] = [(\alpha_{i_4}, 0) + (\alpha_{i_5}, 0) + (\alpha_{i_6}, 0)]$$

by considering the rational function

$$(x - \alpha_{i_1})(x - \alpha_{i_2})(x - \alpha_{i_3})/y = \big((x - \alpha_{i_4})(x - \alpha_{i_5})(x - \alpha_{i_6})/y\big)^{-1}.$$

So the divisors in question can be identified with such partitions of the set $\{\alpha_1, \ldots, \alpha_6\}$ of roots and the action of $\mathrm{Gal}(\overline{K}/K)$ is as desired, yielding the result. □

Corollary 5.7. *We have that both*

- $2J(\mathbb{Q})$ *has index* 2 *in* $\ker(x - T)$, *and*
- $2J(\mathbb{Q}_{743})$ *has index* 2 *in* $\ker(x - T)$.

Proof. Poonen uses PARI to compute that the Galois group of $g(T)$ over $\mathbb{Q}$ is the full symmetric group. So the first part of the corollary follows immediately from proposition 5.6.

Poonen also computes that $L_{743} := L_{\mathbb{Q}_{743}} = E \times F \times F$, where E, F are quadratic extensions of $\mathbb{Q}_{743}$, with E ramified and F unramified. It follows that $g(T)$ does not have a root in $\mathbb{Q}_{743}$, and that there is no decomposition of its roots over $\overline{\mathbb{Q}}_{743}$ of the form in proposition 5.6. □

By the first part of the corollary, it remains to show that the image of $(x - T)$ in L^*/L^{*2} is trivial. To do so, the first ingredient is the following lemma.

Lemma 5.8 [FPS97]. *The image of* $(x - T) : J(K) \longrightarrow L_K^*/L_K^{*2}K^*$ *lies in the kernel of the norm*

$$N_{L_K/K} : L_K^*/L_K^{*2}K^* \longrightarrow K^*/K^{*2}.$$

Proof. If $\alpha_1, \ldots, \alpha_6$ are the roots of $g(T)$ over $\overline{K}$, and $D = \sum n_P P$ is as in definition 5.5, then

$$N_{L_K/K}\big((x - T)(D)\big) = \prod_{i=1}^{6} \prod_P (x_P - \alpha_i)^{n_P} = \prod_P (y_P^2)^{n_P} = \left(\prod_P y_P^{n_P}\right)^2 \in K^{*2}. \qquad \square$$

Next we see what information the primes p of good reduction for C can tell us about the image of $(x - T)$. This is the second ingredient we need to finish our descent argument.

Definition 5.9. Let $S = \{2, 743, \infty\}$. We say $l \in L^*$ is *unramified outside* S if the field extension $L(\sqrt{l})/L$ is unramified outside of primes lying over primes in S.

This is a property that depends only on the image of l in L^*/L^{*2}, and one shows that the set of elements of L^*/L^{*2} unramified outside S forms a subgroup. Write G for the image of this subgroup in $L^*/L^{*2}\mathbb{Q}^*$.

Lemma 5.10 [FPS97]. *The image of* $(x - T) : J(\mathbb{Q}) \longrightarrow L^*/L^{*2}\mathbb{Q}^*$ *is contained in* G.

Proof. Given $D = \sum n_P P$ a $\mathbb{Q}$-rational divisor as in definition 5.5 and $p \notin S$, set

$$a_p = v_p\left(\prod_{v_p(x_P)<0} x_P^{n_P}\right),$$

where v_p is an extension of the p-adic valuation to $\overline{\mathbb{Q}}$, which in particular is allowed to take on non-integer values. However, the fact that P is $\mathbb{Q}$-rational implies a_p *is* an integer.

Then importantly, with D fixed, there are only finitely many $p \notin S$ for which a_p is non-zero. So $m := \prod_{p \notin S} p^{a_p} \in \mathbb{Q}^*$ is well-defined. The proof will be complete if we can show that $m^{-1}(x - T)(D)$ is unramified outside S.

The strategy is to, given $p \notin S$ and an embedding $\iota : L \hookrightarrow \overline{\mathbb{Q}}_p$, show that the valuation of the image of $l := m^{-1}(x - T)(D)$ is even. Indeed, we can find an ι such that $v_p(\iota(l))$ is not even if and only if there is a prime $\mathfrak{p}$ of L lying over p dividing (l) to odd order. Note that since $p \notin S$ does not divide the discriminant of $g(T)$, we have that p does not ramify in L.

If $\alpha_1, \ldots, \alpha_6$ are the roots of $g(T)$ in $\overline{\mathbb{Q}}_p$, then without loss of generality $\iota(T) = \alpha_1$. Since $g(T)$ has distinct roots mod p, if P is such that $v_p(x_P - T) > 0$ then we have $v_p(x_P - \alpha_i) = 0$ for $2 \le i \le 6$. So in this case

$$v_p(x_P - T) = v_p(x_P - \alpha_1) = v_p\left(\prod_{i=1}^{6}(x_P - \alpha_i)\right) = v_p(y_P^2) = 2v_p(y_P).$$

And if we are in the case $v_p(x_P - T) < 0$, then since α_1 is integral (so in particular $v_p(\alpha_1) \geq 0$), we have $v_p(x_P - T) = v_p(x_P)$. It's now a matter of computing

$$\begin{aligned} v_p((x-T)(D)) &= v_p\left(\prod_{v_p(x_P-T)<0} (x_P - T)^{n_P}\right) + v_p\left(\prod_{v_p(x_P-T)>0} (x_P - T)^{n_P}\right) \\ &= v_p\left(\prod_{v_p(x_P-T)<0} x_P^{n_P}\right) + 2 \sum_{v_p(x_P-T)>0} n_P v_p(y_P) \\ &= v_p(m) + 2 \underbrace{\sum_{v_p(x_P-T)>0} n_P v_p(y_P)}_{\text{an integer}}, \end{aligned}$$

so that $v_p(l)$ is even as desired. □

The final piece of information we need to nail down the image of $(x - T)$ over $\mathbb{Q}$ comes from the following diagram.

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{x-T} & L^*/L^{*2}\mathbb{Q}^* \\ \downarrow & & \downarrow \\ J(\mathbb{Q}_{743}) & \xrightarrow{x-T} & L^*_{743}/L^{*2}_{743}\mathbb{Q}^*_{743} \end{array}$$

The simple observarion is that elements in the image of the top $(x - T)$ map into the image of the bottom $(x - T)$ in $L^*_{743}/L^{*2}_{743}\mathbb{Q}^*_{743}$.

Theorem 5.11 [Poo98]**.** $J(\mathbb{Q}) \cong \mathbb{Z}$

Proof. By proposition 5.4, it suffices to prove $\#J(\mathbb{Q})/2J(\mathbb{Q}) = 2$. And by corollary 5.7, this will follow from the image of $(x - T)$ in $L^*/L^{*2}\mathbb{Q}^*$ being trivial.

We will use the following elements of the field L, which are revealed by Poonen's computations on PARI as significant.

element	definition	norm
u_1	$(T^4 - T^3 - T^2 + 2T + 1)/2$	1
u_2	$(T^4 - T^3 - T^2 + 4T + 1)/2$	1
-1	-1	1
α	$(T^5 - 2T^3 + T^2 + 7T + 3)/2$	23
β_1	$(T^5 - 5T^3 + 5T^2 + 6T - 2)/2$	743
β_2	$(T^5 + 8T^4 - 10T^3 - 3T^2 + 35T + 13)/2$	743^2
β_3	$(-10T^5 + 9T^4 + 14T^3 - 33T^2 - 21T + 18)/2$	743^2

We have the factorisations into irreducibles

$$2 = -\alpha^2 u_1, \qquad 743 = \beta_1^2 \beta_2 \beta_3$$

of the primes which ramify in L. Moreover, the images of the 7 elements in the table form an $\mathbb{F}_2$-basis for the subgroup of L^*/L^{*2} of elements unramified outside $\{2, 743, \infty\}$.

From norm considerations, the intersection of the subgroup G of lemma 5.10 with the kernel of the norm to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is spanned by the images of u_2, β_2. Indeed, $u_1 = -2\alpha^{-2}$ vanishes in $L^*/L^{*2}\mathbb{Q}^*$, and similarly $\beta_2 = \beta_3^{-1} \cdot 743\beta_1^{-2}$ has the same image in $L^*/L^{*2}\mathbb{Q}^*$ as β_3.

So the proof will be complete if we can show that no non-trivial product of u_2, β_2 maps in $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*$ to something in the image of $(x-T)$.

Claim. *The image of* $(x-T)$ *in* $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*$ *has order* 2.

By corollary 5.7, this will follow from the index of $2J(\mathbb{Q}_{743})$ in $J(\mathbb{Q}_{743})$ being 4.

Now, $J(\mathbb{Q}_{743})$ is a 2-dimensional Lie group over $\mathbb{Q}_{743}$. Multiplication by 2 is an n-to-1 map, where n is the number of 2-torsion points $\#J(\mathbb{Q}_{743})[2]$. Arguing as in the proof of proposition 5.6 shows that the 15 non-trivial 2-torsion points of $J(\overline{\mathbb{Q}}_{743})$ are $[(\alpha_i,0)+(\alpha_j,0)-\infty_+-\infty_-]$ where α_i, α_j are distinct roots of $g(T)$ over $\overline{\mathbb{Q}}_{743}$. From the decomposition of L_{743}, we deduce exactly 3 of these are defined over $\mathbb{Q}_{743}$.

So $\#J(\mathbb{Q}_{743})[2] = 4$. Since the 743-adic norm $|2|_{743}$ is 1, multiplication by 2 preserves the Haar measure on $J(\mathbb{Q}_{743})$, and we deduce that the index of $2J(\mathbb{Q}_{743})$ in $J(\mathbb{Q}_{743})$ is indeed 4.

Claim. *The image of* $(x-T)$ *in* $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*$ *is generated by* $(2-T)$.

Hensel's lemma implies that $\sqrt{33} \in \mathbb{Q}_{743}$, so that

$$[(2,\sqrt{33})-\infty_-] \in J(\mathbb{Q}_{743}),$$

which gets mapped to $(2-T)$ by $(x-T)$. Note this divisor is not of the form in definition 5.5, so this requires an understanding of how $(x-T)$ is extended to $J(K)$ — see [Cas83].

The claim will follow from $(2-T) \notin L_{743}^{*2}\mathbb{Q}^*$. This is implied by following stronger claim, which also completes the proof of the theorem.

Claim. *The elements* $(2-T), u_2, \beta_2$ *are* $\mathbb{F}_2$*-independent in* $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*$.

Since -1 is not a square mod 743, we have that $\mathbb{Q}_{743}^*/\mathbb{Q}_{743}^{*2}$ is generated by -1 and 743. So if the claim were not true, we'd have some product ρ of $\{-1, 743, (2-T), u_2, \beta_2\}$, involving at least one of the last 3, lying in L^{*2}.

Now recall $L = E \times F \times F$, where F is *the* unramified quadratic extension of $\mathbb{Q}_{743}$, namely $F = \mathbb{Q}_{743}(\sqrt{-1})$. Then since -1 is a square in F, we reduce to a product of $\{743, (2-T), u_2, \beta_2\}$ mapping into $F^{*2} \times F^{*2}$.

Since the β_3-adic valuation of ρ is even, we can rule out the presence of 743 in ρ. And then considering the β_2-adic valuation in turn rules out the presence of β_2.

We arrive at the situation where a non-trivial product of $(2-T), u_2$ maps into $F^{*2} \times F^{*2}$. We can now start to do hands-on computations. The factorisation of $g(T)$ over $\mathbb{F}_{743}$ is

$$g(T) = (T+45)^2 \cdot (T^2+83T+426) \cdot (T^2+570T+688).$$

We have isomorphisms of the residue fields of each F with $\mathbb{F}_{743^2} = \mathbb{F}_{743}(\sqrt{-1})$ as follows:

$$\begin{aligned} \mathbb{F}_{743}[T]/(T^2+83T+426) &\to \mathbb{F}_{743}(\sqrt{-1}) \\ T &\mapsto 330+2\sqrt{-1} \end{aligned}$$

and

$$\begin{aligned} \mathbb{F}_{743}[T]/(T^2+570T+688) &\to \mathbb{F}_{743}(\sqrt{-1}) \\ T &\mapsto 458+44\sqrt{-1}. \end{aligned}$$

So $(2-T)$ maps in the second copy of F to something congruent to $-456-44\sqrt{-1}$ in the residue field. And it is straightforward to verify this *is* a square in $\mathbb{F}_{743}(\sqrt{-1})$, with PARI giving a square root as $502+71\sqrt{-1}$. By Hensel's lemma, $(2-T)$ maps to a square in the second copy of F.

But taking norms and computing Legendre symbols shows that $(2 - T)$ does *not* map to a square in the first copy of F, and that u_2 maps to a square in *neither* copy of F. It follows that no non-trivial product of $(2 - T), u_2$ maps to a square in both copies of F, and the proof of the theorem is complete at last. □

5.3 The method of Chabauty and Coleman

To study $C(\mathbb{Q})$ itself, we apply a refinement of a method of Chabauty [Cha41] and Coleman [Col85], as discussed at the start of the section. We start with the following map j.

Definition 5.12. Let $P \in C(\mathbb{Q})$. Then $j(P) \in J(\mathbb{Q})$ is given by

$$j(P) := [P + P] = [P + P - \infty_+ - \infty_-].$$

Remark. Here and in the following, we identify divisor classes of degrees 2 and 0 via

$$[P + Q] \mapsto [P + Q - \infty_+ - \infty_-].$$

Lemma 5.13. *The map j is injective.*

Proof. We have shown in lemma 5.4 that $J(\mathbb{Q})$ in particular has no 2-torsion. So if $j(P) = j(Q)$, then $[P - Q] = 0$ follows. Since C is certainly not $\mathbb{P}^1$, we are done. □

Theorem 5.11 tells us that $J(\mathbb{Q}) \cong \mathbb{Z}$ but does not give a generator. Our next result is that $D = [\infty_+ - \infty_-]$, while as far as we know not necessarily a genuine generator for $J(\mathbb{Q})$, *is* a generator for $J(\mathbb{Q})$ in the following 3-adic sense.

Lemma 5.14 [Poo98]**.** *Let E be a generator for $J(\mathbb{Q}) \cong \mathbb{Z}$, and write $D = kE$ with $k \in \mathbb{Z}$. Then k is not divisible by 3. In particular any element of $J(\mathbb{Q})$ is of the form $n'D$ for some $n' \in \mathbb{Z}_3$.*

Proof. We use the reduction map $J(\mathbb{Q}) \to J(\mathbb{F}_3)$. Recall we have $\#J(\mathbb{F}_3) = 27$. Using the group law on $J(\mathbb{Q})$ as described in [Fly93], Poonen computes

$$9D = [(-1, -1) + (0, 1)], \qquad 27D = [(1, -3) + (1, -3)].$$

And it is a simple computation that the image $9\widetilde{D} \in J(\mathbb{F}_3)$ of $9D$ under the reduction map is *non-zero*. So $\widetilde{D} \notin 3J(\mathbb{F}_3)$ and the lemma follows. □

The strategy now is to cover the image of j with a collection of charts $U_i \subset J(\mathbb{Q}_3)$, one for each point of the reduction $C(\mathbb{F}_3)$. The elements of $j(C(\mathbb{Q}))$ within a given U_i correspond to the points of $C(\mathbb{Q})$ with a given reduction in $C(\mathbb{F}_3)$.

The reductions of the 8 known rational points on C,

$$(0, \pm 1), \quad (1, \pm 3), \quad (-1, \pm 1), \quad \infty_\pm,$$

give us all 7 points of $C(\mathbb{F}_3)$ — the points $(1, \pm 3)$ have the same reduction.

Now if $D' = 27D$, then each U_i will be a 3-adic disk of the form

$$U_P := \left\{ [P + P] + nD' : n \in \mathbb{Z}_3 \right\} \subset J(\mathbb{Q}_3)$$

with P one the known points in $C(\mathbb{Q})$. That these charts cover the image of j follows from the observation that any element in the kernel of the reduction $J(\mathbb{Q}) \to J(\mathbb{F}_3)$ is of the form nD' for some $n \in \mathbb{Z}_3$. It is this fact, which follows from the above arguments, that depends crucially on $J(\mathbb{Q}) \cong \mathbb{Z}$.

Theorem 5.15 [Poo98]. *Each U_P with $P \neq (1, \pm 3)$ contains exactly 1 point in the image of j.*

Proof. The argument, which goes back to [FPS97], is that the condition that the divisor class $[P + P] + nD' \in U_P$ be of the form $[Q + Q]$, for some $Q \in C(\mathbb{Q}_3)$, implies the vanishing of a certain power series $\theta_P(n) \in \mathbb{Z}_3[\![n]\!]$.

Finding $\theta_P(n)$ involves using the *formal group law* on $J(\mathbb{Q}_3)$. [Fly93] gives rational functions (s_1, s_2) which serve as the coordinates of a point $[(x_1, y_1) + (x_2, y_2)] \in J(\mathbb{Q}_3)$ relative to the group identity. In this context, the formal group law then refers to a pair $\mathscr{F} = (\mathscr{F}_1, \mathscr{F}_2)$ of power series in the variables s_1, s_2, t_1, t_2 which return the coordinates of the sum, in the group law, of the points with coordinates (s_1, s_2) and (t_1, t_2).

Flynn also describes how one can determine $(\mathscr{F}_1, \mathscr{F}_2)$ to any desired degree of accuracy, and similarly for the associated formal exponential map

$$E = (E_1, E_2), \qquad \mathscr{F}(E(s_1, s_2), E(t_1, t_2)) = E(s_1 + t_1, s_2 + t_2)$$

and formal logarithm map

$$L = (L_1, L_2), \qquad L(\mathscr{F}((s_1, s_2), (t_1, t_2))) = L(s_1, s_2) + L(t_1, t_2).$$

This lets Poonen compute the formal logarithm of D' to the following degree of accuracy:

$$l_1 = L_1(D') \equiv 3 \pmod{3^4}, \qquad l_2 = L_2(D') \equiv 75 \pmod{3^4}. \tag{$*$}$$

Another ingredient we need from [Fly93] are power series (k_1, k_2, k_3) in the coordinates (s_1, s_2) of $[(x_1, y_1) + (x_2, y_2)] \in J(\mathbb{Q}_3)$ that recover the triple $(1 : x_1 + x_2 : x_1 x_2)$. If a divisor class is of the form $[Q + Q]$, then in particular it lies in the zero set of $k_2^2 - 4k_1k_3$.

Now, for each known rational point $P \neq (1, \pm 3)$, use ($*$) to compute

$$\theta_P(n) := (k_2^2 - 4k_1k_2)([P + P] + nD')$$

with enough 3-adic accuracy that Strassman's theorem — see e.g. [Cas86], page 62 — can be applied to show that $\theta_P(n)$ has exactly one zero in $\mathbb{Z}_3$.

Poonen is able to compute

- $\theta_{(-1,1)}(n) \equiv 3n \pmod{3^2}$,
- $\theta_{(0,1)}(n) \equiv 6n \pmod{3^2}$,
- $\theta_{\infty_+}(n) \equiv 6n \pmod{3^2}$,

which is exactly of the form required to apply Strassman's theorem as desired. The hyperelliptic involution on C then completes the proof for $U_{(-1,-1)}, U_{(0,-1)}$ and U_{∞_-} too. □

In principle, one could run the above argument to show there are only two points in the image of j within $U_{(1,\pm 3)}$. However, the reduction $(1, 0)$ is a Weierstrass point of C over $\mathbb{F}_3$ and this introduces complications. The power series $\theta_{(1,3)}(n)$ is divisible by large powers of 3, and one would have to work to a prohibitive degree of accuracy to obtain results.

Instead, we argue in the following way.

Lemma 5.16 [Poo98]. *There is a power series $\xi(t) \in \mathbb{Z}_3[\![t]\!]$ which starts*

$$\xi(t) = 1 - \frac{3}{8}t - \frac{31}{512}t^2 + \frac{105}{16384}t^3 + \frac{15269}{2097152}t^4 + \dots$$

such that if we let t range over $3\mathbb{Z}_3$, then $(\xi(t), -3 + t)$ parametrises those points of $C(\mathbb{Q}_3)$ with reduction $(1, 0) \in C(\mathbb{F}_3)$.

Proof. Since $t = y + 3$ is a uniformising parameter for C at $(1, -3)$, there is a unique power series $\xi(t) \in \mathbb{Q}[\![t]\!]$ starting as above such that $(\xi(t), -3 + t)$ is a point of C over $\mathbb{Q}[\![t]\!]$.

Now, the same t also serves as a uniformising parameter over $\mathbb{F}_3$, from which it follows that the coefficients of $\xi(t)$ are in $\mathbb{Z}_3$.

And hence whenever $t \in 3\mathbb{Z}_3$, the power series converges 3-adically and we obtain a point $(\xi(t), -3 + t) \in C(\mathbb{Q}_3)$ as desired.

It remains to justify that these are *all* the elements of $C(\mathbb{Q}_3)$ with reduction $(1, 0)$. Observe that $x = 1$ is a simple root of

$$g(x) = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$$

over $\mathbb{F}_3$. Then by Hensel's lemma, given a value $-3 + t$ for the y-coordinate, with $t \in 3\mathbb{Z}_3$, there is a *unique* $x \in \mathbb{Z}_3$ with $x \equiv 1 \pmod 3$ such that $(x, -3 + t) \in C(\mathbb{Q}_3)$. So we know that $x = \xi(t)$ from the above and the proof is complete. □

Theorem 5.17 [Poo98]**.** *The only rational points on C with reduction $(1, 0) \in C(\mathbb{F}_3)$ are $(1, \pm 3)$.*

Proof. Using lemma 5.16, the strategy is to show that if $t = 3n \in 3\mathbb{Z}_3$, then $P_t = (\xi(t), -3 + t)$ is a rational point on C only for the known values $n = 0, 2$.

If P_t is indeed rational, then the divisor class $D_t = [P_t + (1, 3)]$ lies not just in $J(\mathbb{Q}_3)$ but in $J(\mathbb{Q})$. And note that in general, the reduction of D_t in $J(\mathbb{F}_3)$ is always zero, since

$$\operatorname{div}(x - 1) = 2(1, 0) - \infty_+ - \infty_- \qquad \text{over } \mathbb{F}_3.$$

So if P_t is rational, then by the discussion following lemma 5.14, it follows that D_t is a 3-adic integer multiple of D'.

Poonen detects this by taking the formal logarithm of D_t, using the formulas in [Fly93] as in the proof of theorem 5.15. If $t = 3n$ this gives

$$\begin{aligned} L_1(D_t) &\equiv 66n + 54n^3 \pmod{3^4}, \\ L_2(D_t) &\equiv 66n + 27n^2 + 72n^3 \pmod{3^4}. \end{aligned}$$

If P_t is rational, then the determinant

$$\Delta(n) = \begin{vmatrix} L_1(D_t) & L_2(D_t) \\ l_1 & l_2 \end{vmatrix}$$

must vanish, where l_1, l_2 are as in (∗). We compute

$$\Delta(n) \equiv 54n + 27n^3 \pmod{3^4}.$$

So by Strassman's theorem, there are at most 3 values of $n \in \mathbb{Z}_3$ such that $\Delta(n) = 0$.

Two of these are the desired $n = 0, 2$. We claim there is a final zero at $n = 1$, but that the resulting point $W = (\xi(3), 0)$ on C is not rational. Indeed, the polynomial $g(x)$ is irreducible over $\mathbb{Q}$ so there are certainly no rational points on C whose y-coordinate is zero. Still,

$$\begin{aligned} 2D_3 &= 2[W + (1, 3)] \\ &= [(1, 3) + (1, 3)] + [W + W] \\ &= [(1, 3) + (1, 3)] \\ &= -[(1, -3) + (1, -3)] \\ &= -D', \end{aligned}$$

from which it follows that $\Delta(1)$ is indeed zero.

Since these are all the possible zeroes of $\Delta(n)$, we have covered all the rational points of C with the desired reduction and the proof is complete. □

We can now state with confidence the following result, which follows at once from theorems 5.15 and 5.17. This completes the proof of theorem 4.3.

Corollary 5.18. *There are exactly* 8 *rational points on the curve*

$$C \ : \ x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1,$$

and these are

$$(-1, \pm 1), \quad (0, \pm 1), \quad (1, \pm 3), \quad \infty_{\pm}.$$

References

[Cas83] J. W. S. Cassels. "The Mordell-Weil Group of Curves of Genus 2". In: *Arithmetic and Geometry*. Ed. by M. Artin and J. Tate. Progress in Mathematics. Birkhäuser, 1983, pp. 27–60. ISBN: 978-1-4757-9284-3. DOI: 10.1007/978-1-4757-9284-3_3.

[Cas86] J. W. S. Cassels. *Local Fields*. London Mathematical Society Student Texts. Cambridge University Press, 1986. ISBN: 978-0-521-31525-8. DOI: 10.1017/CBO9781139171885.

[Cha41] C. Chabauty. "Sur les points rationnels des courbes algébriques de genre supérieur à l'unité". In: *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences* 212 (1941), pp. 882–885. MR4484.

[Col85] R. F. Coleman. "Effective Chabauty". In: *Duke Mathematical Journal* 52.3 (1985), pp. 765–770. DOI: 10.1215/S0012-7094-85-05240-8.

[Cre92] J. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, 1992. ISBN: 978-0-521-41813-3. URL: https://johncremona.github.io/book/amec.html.

[Fal83] G. Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". In: *Inventiones Mathematicae* 73.3 (1983), pp. 349–366. DOI: 10.1007/BF01388432.

[Fly93] E. V. Flynn. "The group law on the jacobian of a curve of genus 2". In: *Journal für die reine und angewandte Mathematik* 439 (1993), pp. 45–70. DOI: 10.1515/crll.1993.439.45.

[FPS97] E. V. Flynn, B. Poonen, and E. F. Schaefer. "Cycles of quadratic polynomials and rational points on a genus-2 curve". In: *Duke Mathematical Journal* 90.3 (1997), pp. 435–463. DOI: 10.1215/S0012-7094-97-09011-6.

[Kat80] N. M. Katz. "Galois properties of torsion points on abelian varieties". In: *Inventiones mathematicae* 62.3 (1980), pp. 481–502. DOI: 10.1007/BF01394256.

[Maz77] B. Mazur. "Modular curves and the Eisenstein ideal". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 47.1 (1977), pp. 33–186. DOI: 10.1007/BF02684339.

[Mer96] L. Merel. "Bornes pour la torsion des courbes elliptiques sur les corps de nombres". In: *Inventiones mathematicae* 124.1 (1996), pp. 437–449. DOI: 10.1007/s002220050059.

[Mil86] J. S. Milne. "Jacobian Varieties". In: *Arithmetic Geometry*. Ed. by G. Cornell and J. H. Silverman. Springer New York, 1986, pp. 167–212. ISBN: 978-1-4613-8655-1. DOI: 10.1007/978-1-4613-8655-1_7.

[Mor92] P. Morton. "Arithmetic properties of periodic points of quadratic maps". In: *Acta Arithmetica* 62.4 (1992), pp. 343–372. URL: https://eudml.org/doc/206498.

[Mor98] P. Morton. "Arithmetic properties of periodic points of quadratic maps, II". In: *Acta Arithmetica* 87.2 (1998), pp. 89–102. URL: https://eudml.org/doc/207214.

[MS94] P. Morton and J. H. Silverman. “Rational periodic points of rational functions”. In: *International Mathematics Research Notices* (1994), pp. 97–110. DOI: 10.1155/S1073792894000127.

[Nor50] D. G. Northcott. “Periodic Points on an Algebraic Variety”. In: *Annals of Mathematics* 51.1 (1950), pp. 167–177. DOI: 10.2307/1969504.

[Poo98] B. Poonen. “The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture”. In: *Mathematische Zeitschrift* 228.1 (1998), pp. 11–29. DOI: 10.1007/PL00004405.

[Sil07] J. H. Silverman. *The Arithmetic of Dynamical Systems*. Vol. 241. Graduate Texts in Mathematics. Springer, 2007. DOI: 10.1007/978-0-387-69904-2.

[WR94] R. Walde and P. Russo. “Rational Periodic Points of $Q_c(x) = x^2 + c$”. In: *The American Mathematical Monthly* 101.4 (1994), pp. 318–331. DOI: 10.2307/2975624.