THE COMPLETE CLASSIFICATION OF RATIONAL PREPERIODIC POINTS OF QUADRATIC POLYNOMIALS OVER $\mathbb{Q}$: A REFINED CONJECTURE

BJORN POONEN

Abstract. We classify the graphs that can occur as the graph of rational preperiodic points of a quadratic polynomial over $\mathbb{Q}$, assuming the conjecture that it is impossible to have rational points of period 4 or higher. In particular, we show under this assumption that the number of preperiodic points is at most 9. Elliptic curves of small conductor and the genus 2 modular curves $X_1(13)$, $X_1(16)$, and $X_1(18)$ all arise as curves classifying quadratic polynomials with various combinations of preperiodic points. To complete the classification, we compute the rational points on a non-modular genus 2 curve by performing a 2-descent on its Jacobian and afterwards applying a variant of the method of Chabauty and Coleman.

1. Introduction

Let $f : \mathbb{P}^n \to \mathbb{P}^n$ be a morphism of degree $d \geq 2$ defined over a number field K. A point $P \in \mathbb{P}^n(K)$ is called *periodic* (resp. *preperiodic*) if the sequence

$$P, f(P), f(f(P)), f(f(f(P))), \ldots$$

is periodic (resp. eventually periodic). The set $\operatorname{PrePer}(f, K)$ of preperiodic points of f defined over K can be made a directed graph by drawing an arrow from P to $f(P)$ for each P. Northcott used height functions to prove that $\operatorname{PrePer}(f, K)$ is always finite. Moreover, it can be computed effectively given f. These facts have been rediscovered (in varying degrees of generality) by many authors [20], [13], [4].

It is much more difficult to obtain uniform results for morphisms of fixed degree. Morton and Silverman [19] have proposed the following conjecture.

Conjecture 1. There exists a bound $B = B(D, n, d)$ such that if $K/\mathbb{Q}$ is a number field of degree D, and $f : \mathbb{P}^n \to \mathbb{P}^n$ is a morphism of degree $d \geq 2$ defined over K, then $\# \operatorname{PrePer}(f, K) \leq B$.

Date: November 6, 1995.

1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40, 58F20.

Key words and phrases. arithmetic dynamics, periodic point, preperiodic point, descent, method of Chabauty and Coleman, uniform boundedness.

This research was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. Most of it was done at MSRI, where research is supported in part by NSF grant DMS-9022140.

As pointed out by Silverman in talks on the subject, the special case $D = 1$, $n = 1$, $d = 4$ is enough to imply the recently proven "strong uniform boundedness conjecture" [16], since torsion points of elliptic curves are exactly the preperiodic points of the multiplication-by-2 map, and their x-coordinates are preperiodic points for the degree 4 rational map that gives $x(2P)$ in terms of $x(P)$. A similar conjecture for polynomials over $\mathbb{F}_q(T)$ and its finite extensions would imply the uniform boundedness conjecture for Drinfeld modules [23], which is still open.

Thus it should come as no surprise that even the simplest cases of the conjecture seem to be difficult. For the case of quadratic polynomials over $\mathbb{Q}$, the following conjecture has been made [10]:

Conjecture 2. If $N \geq 4$, then there is no quadratic polynomial $f(z) \in \mathbb{Q}[z]$ with a rational point of exact period N.

Conjecture 2 has been verified for $N = 4$ and $N = 5$ (see [18] and [10], respectively), and [10] presents some evidence that it holds for $N = 6$ as well.

The purpose of this paper is to refine the conjecture by listing the directed graphs that occur as $\operatorname{PrePer}(f, \mathbb{Q})$ for a quadratic polynomial $f(z) \in \mathbb{Q}[z]$, assuming that Conjecture 2 holds. This list appears in Figure 1, which we will explain further in Section 3. It can be thought of as the analogue of the list of possible torsion sugroups of elliptic curves over $\mathbb{Q}$ conjectured by Levi [12] and later by Ogg [22], and finally proved by Mazur [14]. In particular, we will show that Conjecture 2 implies $\# \operatorname{PrePer}(f, \mathbb{Q}) \leq 9$.

One can decide whether a given graph can occur in much the same way that one decides whether a given group occurs as a torsion subgroup of an elliptic curve E over $\mathbb{Q}$: the pairs $(f(z), G)$ where $f(z)$ is a quadratic polynomial (up to linear conjugacy) and G is a graph of preperiodic points (of specified shape) correspond to the points on an algebraic curve, just as elliptic curves together with level structure are parameterized by points on modular curves. For example, quadratic polynomials together with a point of period N are classified by a curve $C_1(N)$ (see [10]), which may be considered the analogue of $X_1(N)$. The curve $C_1(N)$ also has a quotient $C_0(N)$ (the analogue of $X_0(N)$), whose points correspond to quadratic polynomials with a (Galois-stable) N-cycle. To decide whether a given graph occurs, it suffices to find the rational points on the corresponding curve.

There exist also some subtle (and surprising) connections between preperiodic points of quadratic polynomials and torsion points on elliptic curves. Morton [18] noticed that $C_1(4)$ was birational to $X_1(16)$, and we will show below that the curve that classifies quadratic polynomials with points of period 2 and 3 both is birational to $X_1(13)$! Similarly, the curve that classifies quadratic polynomials with points of period 1 and 3 is birational to $X_1(18)$. This is not a general phenomenon, however: $C_1(5)$ and $C_0(5)$ are not modular [10].

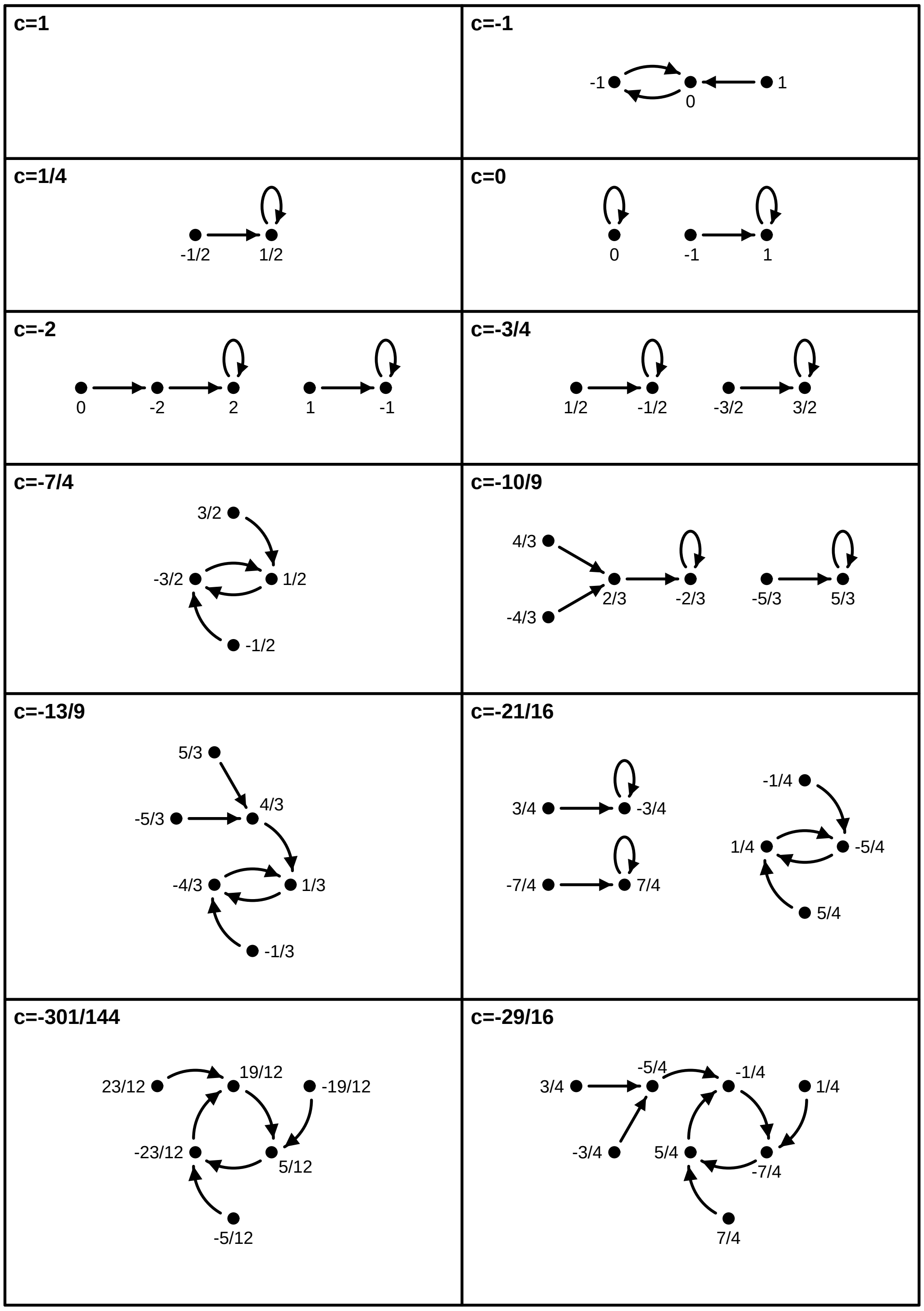

Figure 1. Finite Rational Preperiodic Points of z^2+c.

The curves whose rational points we will need to determine will all be of genus 0, 1, or 2. The genus 0 and 1 curves we encounter always have rational points "at infinity," so each is $\mathbb{P}^1$ or an elliptic curve over $\mathbb{Q}$. The conductor of each elliptic curve is small (never more than 40) and the rank is always zero (luckily), so there is no difficulty in listing the rational points in these cases. As for the genus 2 curves, all except one are recognized as modular curves, whose rational points have been previously computed. The only difficult case is the curve $C_1(3_2)$ that classifies quadratic polynomials together with a point that in two steps enters a 3-cycle. The curve $C_1(3_2)$ is not modular, it has no rational Weierstrass points, and its Jacobian J is absolutely simple, all of which rule out possible shortcuts to finding the rational points. We will need first to perform a general 2-descent on J to find its Mordell-Weil rank. The rank turns out to be 1, so to find the rational points on $C_1(3_2)$ we apply the method of Chabauty and Coleman ([6], [7]). The refinements of the method introduced in [10] are sufficient for obtaining a tight bound on the number of rational points in most of the mod 3 residue classes, but for one residue class (a Weierstrass point mod 3), those techniques would require more 3-adic precision than is easy to compute. We circumvent the problem by introducing a variant of the method.

Although it would certainly be possible to do similar calculations for other number fields K, the results obtained might not be as conclusive. Problems might arise in the application of the method of Chabauty and Coleman when computing the K-rational points of curves of genus 2 or more, because the Mordell-Weil rank may exceed the genus.

2. Periodic Points

Polynomials $f(z), g(z) \in \mathbb{Q}[z]$ are *linearly conjugate* over $\mathbb{Q}$ if there exists a linear polynomial $\ell(z)$ such that $\ell(f(\ell^{-1}(z))) = g(z)$. In this case, ℓ maps the rational preperiodic points of $f(z)$ bijectively to the rational preperiodic points of $g(z)$, also preserving the graph structure. Every quadratic polynomial in $\mathbb{Q}[z]$ is linearly conjugate over $\mathbb{Q}$ to one of the form $z^2 + c$ with $c \in \mathbb{Q}$, so from now on, we will only consider $f(z) = z^2 + c$. In the subsequent theorems for polynomials, we disregard ∞, which is always a rational fixed point.

Theorem 1. *Let $f(z) = z^2 + c$ with $c \in \mathbb{Q}$. Then*

1. *$f(z)$ has a rational point of period 1 (i.e., a rational fixed point) if and only if $c = 1/4 - \rho^2$ for some $\rho \in \mathbb{Q}$. In this case, there are exactly two, $1/2 + \rho$ and $1/2 - \rho$, unless $\rho = 0$, in which case they coincide.*
2. *$f(z)$ has a rational point of period 2 if and only if $c = -3/4 - \sigma^2$ for some $\sigma \in \mathbb{Q}$, $\sigma \neq 0$. In this case, there are exactly two, $-1/2 + \sigma$ and $-1/2 - \sigma$ (and these form a 2-cycle).*

3. *$f(z)$ 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 $\tau \in \mathbb{Q}$, $\tau \neq -1, 0$. In this case, there are exactly three,

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

and these are cyclically permuted by $f(z)$.

Proof. This is a restatement of Theorems 1 and 3 in [24], except for the claim in (3) that there can be at most one 3-cycle, which is part of Theorem 3 in [17]. □

A criterion was given in [24] for determining whether $z^2 + c$ has rational points of period 1 *and* rational points of period 2. The next theorem gives a more explicit criterion, and also shows that certain other combinations are impossible.

Theorem 2. *Let $f(z) = z^2 + c$ with $c \in \mathbb{Q}$. Then*

1. *$f(z)$ has rational points of period 1 and rational points of period 2 if and only if*

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

for some $\mu \in \mathbb{Q}$, $\mu \neq -1, 0, 1$. In this case the parameters ρ and σ of Theorem 1 are

$$\rho = -\frac{\mu^2 + 1}{\mu^2 - 1} \qquad \sigma = \frac{2\mu}{\mu^2 - 1}.$$

2. *If $f(z)$ has rational points of period 3, it cannot have any rational points of period 1 or 2.*

Proof of Theorem 2. By Theorem 1, $z^2 + c$ has rational points of period 1 and 2 if and only if

$$c = 1/4 - \rho^2 = -3/4 - \sigma^2,$$

where $\rho, \sigma \in \mathbb{Q}$ with $\sigma \neq 0$. The curve in the (ρ, σ)-plane described by this equation is a conic with a rational point $(1, 0)$, so it is birational to $\mathbb{P}^1$ over $\mathbb{Q}$, with the rational function $\mu = (1 - \rho)/\sigma$ giving the birational map. Solving for c, ρ, and σ in terms of μ gives the result. The values of μ not allowed are $-1, 1, 0, \infty$, because these correspond to the two points at infinity on the conic and the two points where $\sigma = 0$.

If z^2+c has rational points of period 1 and 3, then

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

so $(\tau, 2\tau(\tau+1)\rho)$ is a point on the hyperelliptic curve

$$C: \quad y^2 = x^6+2x^5+5x^4+10x^3+10x^2+4x+1.$$

By [9], this is also an equation for the modular curve $X_1(18)$. But $X_1(18)$ has only six rational points (these are all cusps), so the only rational points on C besides the two points at infinity (on the nonsingular model) are $(-1,1)$, $(-1,-1)$, $(0,1)$, and $(0,-1)$. These do not give rise to a valid pair (τ,ρ), since τ is not allowed to be 0 or -1 in Theorem 1. Hence it is impossible for there to exist rational points of period 1 and 3.

Similarly, if z^2+c has rational points of period 2 and 3, then

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

so $(\tau, 2\tau(\tau+1)\sigma)$ is a point on

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

This curve is $X_1(13)$, since if we the dehomogenize the model

$$x_1^2x_2^2 - x_1x_2^3 - x_1x_2x_3^2 + x_1x_3^3 + x_2^3x_3 - x_2^2x_3^2$$

of $X_1(13)$ in [2] by setting $x_3 = 1$, we find that the discriminant of the resulting quadratic in x_1 is

$$x_2^6+2x_2^5+x_2^4+2x_2^3+6x_2^2+4x_2+1.$$

The curve $X_1(13)$ also has exactly six rational points (again cusps), so the only rational points on C' besides the two points at infinity are $(-1,1)$, $(-1,-1)$, $(0,1)$, and $(0,-1)$. Again this implies that z^2+c cannot have both rational points of period 2 and 3, since τ is not allowed to be 0 or -1. $\square$

The curves were originally recognized as $X_1(13)$ and $X_1(18)$ by computing enough invariants (such as the genus, automorphism group, primes of bad reduction, and Mordell-Weil group of the Jacobian) that the result could be guessed.

3. Preperiodic Points

If m and n are positive integers, then a *point of type m_n* for $f(z)$ is a preperiodic point that enters an m-cycle after n iterations. For example, $3/4$ is a point of type 3_2 for $f(z) = z^2 - 29/16$, since its orbit is

$$3/4, -5/4, -1/4, -7/4, 5/4, -1/4, -7/4, \ldots.$$

Theorem 3. *Let $f(z) = z^2 + c$ with $c \in \mathbb{Q}$. Then*

1. *For each $m \geq 1$, x is a rational point of type m_1 for $f(z)$ if and only if $-x$ is a nonzero rational point of period m. The number of rational points of type m_1 equals the number of rational points of period m, except when $c = -1$, $m = 2$, or $c = 0$, $m = 1$, in which case there is one less.*
2. *$f(z)$ has rational points of type 1_2 if and only if*
$$c = \frac{-2(\eta^2+1)}{(\eta^2-1)^2}$$
for some $\eta \in \mathbb{Q}$, $\eta \neq -1, 1$. In this case, there are exactly 2 such points, $\frac{2\eta}{\eta^2-1}$ and $-\frac{2\eta}{\eta^2-1}$, unless $\eta = 0$ ($c = -2$), in which they coincide. The parameter ρ of Theorem 1 is
$$\rho = -\frac{\eta^2+3}{2(\eta^2-1)}.$$
3. *$f(z)$ has rational points of type 2_2 if and only if*
$$c = \frac{-\nu^4 - 2\nu^3 - 2\nu^2 + 2\nu - 1}{(\nu^2-1)^2}$$
for some $\nu \in \mathbb{Q}$, $\nu \neq -1, 0, 1$. In this case, there are exactly 2 such points, $\frac{\nu^2+1}{\nu^2-1}$ and $-\frac{\nu^2+1}{\nu^2-1}$. The parameter σ of Theorem 1 is
$$\sigma = \frac{\nu^2+4\nu-1}{2(\nu^2-1)}.$$
4. *$f(z)$ has rational points of type 3_2 if and only if $c = -29/16$. For $c = -29/16$, the rational points of type 3_2 are $3/4$ and $-3/4$.*
5. *If $f(z)$ has rational points of type m_2 with $1 \leq m \leq 3$, then there are no rational points of period $b \leq 3$ unless $b = a$.*
6. *$f(z)$ cannot have rational points of type 1_n, 2_n, or 3_n for any $n \geq 3$.*

Together, Theorems 1, 2, and 3, show that the subgraph of $\mathrm{PrePer}(z^2 + c, \mathbb{Q})$ consisting of finite rational preperiodic points that eventually end up in a cycle of length less than or equal to 3 is isomorphic to one of the graphs in Figure 1. In particular, if Conjecture 2 holds, then these are the only possibilities for the full graph $\mathrm{PrePer}(z^2 + c, \mathbb{Q})$ (with ∞ deleted), so we get the following.

Corollary 1. *If Conjecture 2 holds, then $\#\,\mathrm{PrePer}(f, \mathbb{Q}) \leq 9$ for all quadratic polynomials $f \in \mathbb{Q}[z]$.*

(The bound 9 includes the fixed point at infinity.) It should be remarked that many of the graphs in Figure 1 occur infinitely often: the only ones that are unique are the graphs for $c = -1$, $1/4$, 0, -2, and $-29/16$. Also, for each of the particular values of c in the figure, it is easy to prove unconditionally that the graph shown is the full graph of finite rational preperiodic points. In fact, this can be done even without explicit use of height functions: the rational preperiodic points are bounded in every absolute value, which means that they are multiples of $1/N$ for some fixed N and are contained in some finite interval of $\mathbb{R}$, so that one need only evaluate z^2+c at a finite number of points to compute the graph. (In [3], similar arguments are used to bound the number of preperiodic points of z^2+c in terms of the number of prime divisors of the denominator of c.)

Proof of Theorem 3. If x is a rational point of type m_1, then $f(f^m(x)) = f(x)$, but $f^m(x) \neq x$, so $f^m(x) = -x$. Since every iterate of x except x itself is periodic of period m, $-x$ must be a rational point of period m, and it must be nonzero, since otherwise x would be periodic as well. Conversely, if $-x$ is a nonzero rational point of period m, then $f(x) = f(-x)$ is also a rational point of period m, but $f^m(x) = f^{m-1}(f(x)) = f^{m-1}(f(-x)) = -x \neq x$, so x is a rational point of type m_1.

If 0 is preperiodic for z^2+c, $c \in \mathbb{Q}$, then c must be integral at each prime p, because otherwise the orbit of 0 would diverge to infinity p-adically. Thus $c \in \mathbb{Z}$. Moreover, $|c| \leq 2$, since otherwise the orbit of 0 diverges to $+\infty$ with respect to the ordinary absolute value. [This argument can be understood as follows: if 0 is preperiodic, then its orbit is bounded in every absolute value. (In fact, the converse holds as well.) In other words, 0 is in the Mandelbrot set and also in the p-adic Mandelbrot set (which is the closed unit ball in $\overline{\mathbb{Q}}_p$) for each prime p.] Checking $c = -2, -1, 0, 1, 2$, we find that 0 is preperiodic only for $c = -2, -1, 0$, and periodic only for $c = -1$ and $c = 0$, with period 2 and 1, respectively. Thus the number of rational points of type m_1 equals the number of rational points of period m, except for $c = -1$, $m = 2$, and $c = 0$, $m = 1$, when it is one less. This completes the proof of (1).

If z^2+c has a rational point r of type 1_2, then $c = 1/4 - \rho^2$ by Theorem 1, and $r^2 + c$ is the negative of one of the fixed points, since these are exactly the points of type 1_1, provided that the fixed point is not 0. Without loss of generality, we may assume $r^2 + c = -(1/2+\rho)$ with $\rho \neq -1/2$, so

$$r^2 = -(1/2+\rho) - (1/4-\rho^2) = \rho^2 - \rho - 3/4.$$

This conic in the (r,ρ)-plane has a rational point $(0, -1/2)$, so the rational function $\eta = r/(1/2+\rho)$ defines a birational map from it to $\mathbb{P}^1$. Substituting $r = (1/2+\rho)\eta$ in the equation of the conic, we solve and find

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

The values of η not allowed are $1, -1, \infty$, because these correspond to the two points at infinity on the conic, and the point where $\rho = -1/2$. But for the good values of η, $\frac{2\eta}{\eta^2-1}$ is another rational point of type 1_2, unless $\eta = 0$, in which case they coincide.

If there were yet another point s of type 1_2, then s^2+c would have to be the negative of the *other* fixed point: $s^2+c=-(1/2-\rho)$. Then

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

Letting $t=(\eta^2-1)s$, we find that we have a point on the genus 1 curve

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

Since the curve has a rational point $(\eta,t)=(1,2)$, it is birational to an elliptic curve. In fact, the following are inverse rational maps between the curve and the elliptic curve $E_{24}: y^2=x^3-x^2+x$ in Weierstrass form:

$$(\eta,t)\mapsto\left(\frac{t+2}{(\eta-1)^2},\frac{2\eta^3-2\eta^2-2\eta-6-4t}{2(\eta-1)^3}\right),$$

$$(x,y)\mapsto\left(\frac{x^2-2y-1}{x^2+1},\frac{2x^4-4x^3+8xy+4x-2}{(x^2+1)^2}\right).$$

The elliptic curve E_{24} is curve 24A4 in Cremona's tables [8] and 24A in Antwerp IV [1], and

$$E_{24}(\mathbb{Q})=\{\mathcal{O},(0,0),(1,1),(-1,1)\}.$$

These correspond to the points $(\eta,t)=(1,2),(-1,-2),(-1,2),(1,-2)$, respectively. But $\eta=1$ and $\eta=-1$ are forbidden, so there can be no further points of type 1_2.

If z^2+c has a rational point r of type 2_2, then $c=-3/4-\sigma^2$ for some nonzero $\sigma\in\mathbb{Q}$ by Theorem 1, and r^2+c is the negative of a nonzero point of period 2. Without loss of generality, we may assume $r^2+c=-(-1/2+\sigma)$ with $\sigma\neq 0,1/2$, so

$$r^2=-(-1/2+\sigma)-(-3/4-\sigma^2)=\sigma^2-\sigma+5/4.$$

This conic in the (r,σ)-plane has a rational point $(1,1/2)$, so the rational function $\nu=(r-1)/(1/2-\sigma)$ defines a birational map from it to $\mathbb{P}^1$. Substituting $r=1+(1/2-\sigma)\nu$ in the equation of the conic, we solve and find

$$\sigma=\frac{\nu^2+4\nu-1}{2(\nu^2-1)},\quad r=-\frac{\nu^2+1}{\nu^2-1},\quad c=\frac{-\nu^4-2\nu^3-2\nu^2+2\nu-1}{(\nu^2-1)^2}.$$

The values of ν not allowed are $1,-1,0,\infty$, because these correspond to the two points at infinity on the conic and the two points where $\sigma=1/2$. (Actually $-2+\sqrt{5}$ and $-2-\sqrt{5}$ are not allowed either since they correspond to the points where $\sigma=0$, but these are not rational, so we need not consider these.) For the good values of ν, $\frac{\nu^2+1}{\nu^2-1}$ is another rational point of type 2_2.

If there were yet another point s of type 2_2, then s^2+c would have to be the negative of the *other* point of period 2: $s^2+c=-(-1/2-\sigma)$. Then

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

Letting $t = (\nu^2 - 1)s$, we find that we have a point on the genus 1 curve

$$t^2 = 2(\nu^4 + 2\nu^3 - 2\nu + 1).$$

Since this curve has a rational point $(\nu, t) = (1, 2)$, it is birational to an elliptic curve. The following are inverse rational maps between the curve and the elliptic curve $E_{40} : y^2 = x^3 - 2x + 1$:

$$(\nu, t) \mapsto \left(\frac{t + 2\nu^2}{(\nu - 1)^2}, -\frac{3\nu^3 + 2\nu t + 3\nu^2 - 3\nu + 1}{(\nu - 1)^3} \right),$$
$$(x, y) \mapsto \left(\frac{x^2 - 2y}{x^2 - 4x + 2}, \frac{2x^4 - 8x^2y + 8x^3 + 8xy - 24x^2 + 24x - 8}{(x^2 - 4x + 2)^2} \right).$$

The elliptic curve E_{40} is curve 40A3 in [8] (40A in [1]), and

$$E_{40}(\mathbb{Q}) = \{\mathcal{O}, (0, 1), (1, 0), (0, -1)\}.$$

These correspond to the points $(\nu, t) = (1, 2), (-1, -2), (-1, 2), (1, -2)$, respectively. But $\nu = 1$ and $\nu = -1$ are forbidden, so there can be no further points of type 2_2.

We will postpone the discussion of points of type 3_2 until the next section. The case $a = 3$ of part (5) will follow from this, so for now we prove part (5) for $a = 1$ and $a = 2$. Note that in each of these cases, there can be no points of order 3, by Theorem 2.

If $f(z)$ has a rational point r of type 1_2 then $c = 1/4 - \rho^2$ and $r^2 + c$ is the negative of a nonzero fixed point, as before: without loss of generality $r^2 + c = -(1/2 - \rho)$. If $f(z)$ also has a rational point of period 2, then

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

for some $\mu \in \mathbb{Q}$, $\mu \neq -1, 0, 1$, and we get

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

Letting $t = 2(\mu^2 - 1)r$, we obtain a rational point on the genus 1 curve

$$t^2 = 5\mu^4 + 14\mu^2 - 3.$$

Since this curve has a rational point $(\mu, t) = (1, 4)$, it is birational to an elliptic curve. The following are inverse rational maps between the curve and the elliptic curve $E_{15} : y^2 + xy + y = x^3 + x^2$:

$$(\mu, t) \mapsto \left(\frac{t + \mu^2 + 4\mu - 1}{2(\mu - 1)^2}, -\frac{2\mu^3 + \mu t + \mu^2 + 2\mu - 1}{(\mu - 1)^3} \right),$$
$$(x, y) \mapsto \left(\frac{x^2 - 2y + x - 1}{x^2 - x - 1}, \frac{4x^4 - 12x^2y + 8x^3 - 8xy + 8x^2 + 4x - 8y - 4}{(x^2 - x - 1)^2} \right).$$

The elliptic curve E_{15} is curve 15A8 in [8] (15A in [1]), and

$$E_{15}(\mathbb{Q}) = \{\mathcal{O}, (0,0), (-1,0), (0,-1)\}.$$

These correspond to the points $(\mu, t) = (1,4), (1,-4), (-1,4), (-1,4)$, respectively. But $\mu = 1$ and $\mu = -1$ are forbidden, so it is impossible for $f(z)$ to have a rational point of type 1_2 and a rational point of period 2.

Similarly, if $f(z)$ has a rational point r of type 2_2, then $c = -3/4 - \sigma^2$ and $r^2 + c$ is the negative of a nonzero period 2 point, as before: without loss of generality $r^2 + c = -(-1/2 + \sigma)$. If $f(z)$ also has a rational point of period 1, then

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

for some $\mu \in \mathbb{Q}$, $\mu \neq -1, 0, 1$, and we get

$$r^2 = \frac{5\mu^4 - 8\mu^3 + 6\mu^2 + 8\mu + 5}{4(\mu^2 - 1)^2}.$$

Letting $t = 2(\mu^2 - 1)r$, we obtain a rational point on the genus 1 curve

$$t^2 = 5\mu^4 - 8\mu^3 + 6\mu^2 + 8\mu + 5.$$

Since this curve has a rational point $(\mu, t) = (1, 4)$, it is birational to an elliptic curve. The following are inverse rational maps between the curve and the elliptic curve $E_{17} : y^2 + xy + y = x^3 - x^2 - x$:

$$(\mu, t) \mapsto \left(\frac{t + \mu^2 + 3}{2(\mu - 1)^2}, -\frac{3\mu^3 + \mu t - 5\mu^2 + 9\mu + 1}{2(\mu - 1)^3} \right),$$
$$(x, y) \mapsto \left(\frac{x^2 - 2y - x - 1}{x^2 - x - 1}, \frac{4x^4 - 4x^2 y - 4x^3 - 8xy - 4x - 4}{(x^2 - x - 1)^2} \right).$$

The elliptic curve E_{17} is curve 17A4 in [8] (17A in [1]), and

$$E_{17}(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,-1), (0,-1)\}.$$

These correspond to the points $(\mu, t) = (1,4), (1,-4), (-1,4), (-1,-4)$, respectively. But $\mu = 1$ and $\mu = -1$ are forbidden, so it is impossible for $f(z)$ to have a rational point of type 2_2 and a rational point of period 1. This completes the proof of part (5) for $a \leq 2$.

It follows from part (4) and the calculation of preperiodic points for $z^2 - 29/16$ (which we have postponed until the next section), that $f(z)$ cannot have rational points of type 3_n for $n \geq 3$. Therefore we now prove that $f(z)$ cannot have rational points of type 1_n or 2_n for $n \geq 3$. It suffices to consider $n = 3$, since iterating f on a rational point with higher n eventually yields a point with $n = 3$. If $f(z)$ has a rational point q of type 1_3, then q^2+c is a rational point r of type 1_2, and by part (2), we have

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

where $\eta \neq -1, 1$, so

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

Letting $t = 2(\eta^2-1)q$, we obtain a rational point on the elliptic curve

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

The linear change of coordinates $\eta = 2x-1$, $t = 4y+2$ transforms this into

$$E_{11} : y^2 + y = x^3 - x^2,$$

which is curve 11A3 in [8] (11A in [1]), and which is also the modular curve $X_1(11)$. This curve has five rational points

$$\mathcal{O}, (0,0), (0,-1), (1,0), (1,-1)$$

the last four of which correspond to finite points

$$(\eta, t) = (-1, 2), (-1, -2), (1, 2), (1, -2)$$

but $\eta = 1$ and $\eta = -1$ are forbidden, so $f(z)$ cannot have rational points of type 1_3.

If $f(z)$ has a rational point q of type 2_3, then q^2+c is a rational point r of type 2_2, and by part (2), we have

$$c = \frac{-\nu^4 - 2\nu^3 - 2\nu^2 + 2\nu - 1}{(\nu^2-1)^2}, \quad r = \frac{\nu^2+1}{\nu^2-1},$$

for some $\nu \in \mathbb{Q}$, $\nu \neq -1, 0, 1$, so

$$q^2 = \frac{2(\nu^3+\nu^2-\nu+1)}{(\nu^2-1)^2}.$$

This is the same equation found in the last paragraph (with ν instead of η). Again $\nu = 1$ and $\nu = -1$ are forbidden, so $f(z)$ cannot have rational points of type 2_3. □

4. Rational points on the genus 2 curve $C_1(3_2)$

In this section, we complete the proof of Theorem 3 by proving part (4). First we find a nice model for the curve $C_1(3_2)$ which classifies z^2+c together with a point of type 3_2 If z^2+c has a rational point r of type 3_2, then r^2+c is the negative of a nonzero rational point of period 3, so by Theorem 1 we have, without loss of generality,

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

for some $\tau \in \mathbb{Q}$, $\tau \neq -1, 0$. These imply that

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

so $(\tau, 2\tau(\tau+1)r)$ is a rational point on the curve

$$\mathcal{C}: \quad y^2 = g(x)$$

where

$$g(x) \stackrel{\text{def}}{=} x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1.$$

Since $g(x)$ has no rational zeros, $\mathcal{C}$ cannot be put in the form $y^2 =$ (quintic in x) over $\mathbb{Q}$. Furthermore it can be shown using the same methods as in [10] that the Jacobian J of $\mathcal{C}$ is absolutely simple with $\operatorname{End} J = \mathbb{Z}$, so that J is not a quotient of the Jacobian of any modular curve over $\mathbb{C}$. Hence we will apply the general method of [10] to find the rational points. (We will be brief in this section; the reader is encouraged to consult [10] for more details.)

Note that $\mathcal{C}$ has six obvious affine points: $Q^+ = (-1, 1)$, $Q^- = (-1, -1)$, $R^+ = (0, 1)$, $R^- = (0, -1)$, $S^+ = (1, 3)$, and $S^- = (1, -3)$. Since $\deg g$ is even, $\mathcal{C}$ has two points at infinity (on the nonsingular model), and these are rational since the leading coefficient of $g(x)$ is a square. The rational function y/x^3 takes values 1 and -1 at these two points, which we call ∞^+ and ∞^-, respectively. We will eventually show that these eight points are the only rational points on $\mathcal{C}$. First we compute the structure of the Mordell-Weil group $J(\mathbb{Q})$. Elements of $J(\mathbb{Q})$ will be written either as $[D]$ where D is a degree zero divisor, or as $[P_1 + P_2]$ with $P_1, P_2 \in \mathcal{C}$, which is (in abuse of notation) identified with $[P_1 + P_2 - \infty^+ - \infty^-]$.

Proposition 1. $J(\mathbb{Q}) \cong \mathbb{Z}$.

Proof. The discriminant of $g(x)$ is $-2^{12} \cdot 743$, so the set of bad primes of J is contained in $S \stackrel{\text{def}}{=} \{2, 743, \infty\}$. (In fact, $\mathcal{C}$ and J have good reduction at 2, because substituting $y = 2z + x^3 + x + 1$ and dividing by 4 yields the model

$$z^2 + zx^3 + zx + z + x^4 = x^2,$$

which has bad reduction only at 743.) We compute $\#J(\mathbb{F}_3) = 27$ and $\#J(\mathbb{F}_5) = 43$, so $J(\mathbb{Q})_{\text{tors}}$ is trivial. Thus the divisor class $[\infty^+ - \infty^-]$ has infinite order, and $J(\mathbb{Q})$ has rank at least 1.

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	$(T^5 - 2T^3 + T^2 + 7T + 3)/2$	2^3
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

TABLE 1. Some elements of L.

Let L be the field $\mathbb{Q}[T]/(g(T))$, and for each prime p including ∞ let $L_p = \mathbb{Q}_p[T]/(g(T))$. PARI tells us that the splitting field of $g(x)$ over $\mathbb{Q}$ has Galois group S_6, that the class number of L is 1, and that the unit group is of rank 2, generated by u_1, u_2, and -1, where u_1 are u_2 are defined in Table 1. Furthermore the ramified primes 2 and 743 factor in L as $-\alpha^2 u_1$ and $\beta_1^2\beta_2\beta_3$, where α, β_1, β_2, β_3 are irreducible elements also defined in Table 1. We have $L_{743} \cong E \times F \times F$, where E and F are quadratic extensions of $\mathbb{Q}_{743}$ with E ramified and F unramified.

As in [10], there is a map

$$(x - T) : J(\mathbb{Q}) \to L^*/L^{*2}\mathbb{Q}^*.$$

The index of $2J(\mathbb{Q})$ in the kernel is 2 by [10, Proposition 5], since $g(x)$ has Galois group S_6. So to prove that $J(\mathbb{Q})$ has rank 1, it suffices to prove that the image is trivial. The image is contained in the subgroup H of elements in the kernel of the norm $L^*/L^{*2}\mathbb{Q}^* \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ which are "unramified outside S," by [10, Proposition 3]. In fact, it is contained in the subgroup H_0 of H consisting of elements which map in $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}$ into the image of

$$(x - T) : J(\mathbb{Q}_{743}) \to L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*.$$

(It will turn out that we will not need the information from the other primes in S.)

In our case, an $\mathbb{F}_2$-basis for the subgroup of L^*/L^{*2} unramified outside S is the set of seven elements in Table 1. The intersection with the kernel of the norm to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is spanned by $u_1, u_2, -1, \beta_2, \beta_3$. Since $u_1 = -2\alpha^{-2} \in L^{*2}\mathbb{Q}^*$, and similarly $\beta_2 \equiv \beta_3 \pmod{L^{*2}\mathbb{Q}^*}$, we find that H is spanned by (the images of) u_2 and β_2.

Let us now calculate the image of

$$(x - T) : J(\mathbb{Q}_{743}) \to L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*.$$

The 15 nonzero elements of the 2-torsion subgroup $J[2]$ are of the form $[P_1 + P_2]$ where P_1 and P_2 are distinct points on $\mathcal{C}$ of the form $(r, 0)$ with $g(r) = 0$. Since $g(x)$ factors into three quadratics over $\mathbb{Q}_{743}$, such $[P_1 + P_2]$ will be stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_{743}/\mathbb{Q}_{743})$ if and only if the two corresponding zeros of $g(x)$ are zeros of the same quadratic factor. Hence $\#J(\mathbb{Q}_{743})[2] = 3+1 = 4$. Multiplication-by-2 is locally Haar measure-preserving on $J(\mathbb{Q}_{743})$ so

$$\#J(\mathbb{Q}_{743})/2J(\mathbb{Q}_{743}) = \#J(\mathbb{Q}_{743})[2] = 4.$$

Finally, $g(x)$ has no zero in $\mathbb{Q}_{743}$, and no partition of the six zeros of $g(x)$ into two 3-element subsets can be stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_{743}/\mathbb{Q}_{743})$ because of the decomposition of L_{743}, so by [10, Proposition 5], $2J(\mathbb{Q}_{743})$ has index 2 in $\ker(x-T)$, and

$$\#(x-T)(J(\mathbb{Q}_{743})) = \#J(\mathbb{Q}_{743})/\ker(x-T) = 2. \tag{1}$$

Since the Legendre symbol $\left(\frac{33}{743}\right)$ is 1, Hensel's Lemma implies that $(2, \sqrt{33}) \in \mathcal{C}(\mathbb{Q}_{743})$. (Fix a square root.) We claim that $[(2, \sqrt{33}) - \infty^-]$ generates $J(\mathbb{Q}_{743})/\ker(x-T)$, which is equivalent to $2-T$ generating $(x-T)(J(\mathbb{Q}_{743}))$. Because of (1), it suffices to show $2-T \notin L_{743}^{*2}\mathbb{Q}_{743}^*$.

In fact, we will show more: that $2-T$, u_2 and β_2 are $\mathbb{F}_2$-independent in $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*$. If not, then since $\mathbb{Q}_{743}^*/\mathbb{Q}_{743}^{*2}$ is generated by -1 and 743, some product of -1, 743, $2-T$, u_2, and β_2 involving at least one of the last three would be in L_{743}^{*2}. Recall that $L_{743} \cong E \times F \times F$, where $F = \mathbb{Q}_{743}(i)$ is the unramified quadratic extension of $\mathbb{Q}_{743}$, $i^2 = -1$. Since -1 is a square in F, we would find that the product of some nonempty subset of $\{743, 2-T, u_2, \beta_2\}$ would map to the trivial element of $F^*/F^{*2} \times F^*/F^{*2}$. The condition that the β_3-adic valuation of the product be even forces 743 not to be part of the product. The condition that the β_2-adic valuation of the product be even forces β_2 not to be part of the product. So some $\mathbb{F}_2$-combination of $2-T$ and u_2 is a square in both F's. By factoring $g(x)$ modulo 743, we find that T maps in the first F to something congruent to $330 + 2i$ in the residue field $\mathbb{F}_{743^2}$, and in the second F to something congruent to $458 + 44i$ in the residue field. Checking the Legendre symbols at the norm from $\mathbb{F}_{743^2}$ to $\mathbb{F}_{743}$ of the image of $2-T$ and u_2 for each F, we find by Hensel's Lemma that $2-T$ is a square in the first F but not the second, and that u_2 is not a square in either F. This contradicts the existence of a relation between $2-T$ and u_2 in $F^*/F^{*2} \times F^*/F^{*2}$, and hence proves that $2-T$, u_2 and β_2 are $\mathbb{F}_2$-independent in $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*$.

But this means that $2-T$ generates the image of $J(\mathbb{Q}_{743})$ under $(x-T)$, and also that no element of H can map in $L_{743}^*/L_{743}^{*2}\mathbb{Q}_{743}^*$ into this image. Thus $J(\mathbb{Q})/\ker(x-T)$ is trivial, and the $\mathbb{F}_2$-dimension of $J(\mathbb{Q})/2J(\mathbb{Q})$ is at most 1. We have already shown that $J(\mathbb{Q})$ is torsion-free and of rank at least 1, so $J(\mathbb{Q}) \cong \mathbb{Z}$. $\square$

Since the rank of $J(\mathbb{Q})$ is 1, we can now apply the method of Chabauty and Coleman to bound the number of rational points on $\mathcal{C}$. We will work modulo powers of 3. Over $\mathbb{F}_3$, $\mathcal{C}$ has five affine points, so $\#\mathcal{C}(\mathbb{F}_3) = 7$. The mod 3 reductions of the eight known rational points Q^+, Q^-, R^+, R^-, S^+, S^-, ∞^+, ∞^- are distinct, except that R^+ and R^- both reduce to the Weierstrass point $(1, 0) \in \mathcal{C}(\mathbb{F}_3)$. To show these are all, it suffices to prove the following:

Proposition 2. *Each point in $\mathcal{C}(\mathbb{F}_3)$ is the mod 3 reduction of exactly one point in $\mathcal{C}(\mathbb{Q})$ except $(1,0)$ which is the reduction of exactly two.*

Proof. Let $D = [\infty^+ - \infty^-] = [\infty^+ + \infty^+] \in J(\mathbb{Q})$ (recall our abuse of notation), and let $\widetilde{D} \in J(\mathbb{F}_3)$ be the mod 3 reduction of D. Using the group law presented in [11] (or alternatively by intersecting $\mathcal{C}$ with carefully chosen cubics to obtain relations between divisor classes), we find that $9D = [Q^- + R^+]$ and $27D = [S^- + S^-]$. Since $\#J(\mathbb{F}_3) = 27$ and $9\widetilde{D} \neq \mathcal{O} \in J(\mathbb{F}_3)$, $J(\mathbb{F}_3)$ is cyclic of order 27 and $\widetilde{D}$ is a generator. Let $\mathcal{M}_3 \subset J(\mathbb{Q}_3)$ denote the kernel of reduction. Then $D' = 27 \cdot D = [S^- + S^-]$ is in $\mathcal{M}_3$. We do not know whether D is a generator of $J(\mathbb{Q})$, but if E is a generator and $D = n \cdot E$, then n is not divisible by 3, since $\widetilde{D} \notin 3J(\mathbb{F}_3)$. This is enough to imply that every $D_0 \in J(\mathbb{Q}) \cap \mathcal{M}_3$ is (uniquely) expressible as $n \cdot D'$, where n is a 3-*adic* integer.

Suppose $P \in \mathcal{C}(\mathbb{Q})$ has the same mod 3 reduction as Q^+. Then $[P + P]$ equals $[Q^+ + Q^+] + n \cdot D'$ for some $n \in \mathbb{Z}_3$. Using the notation and methods of [10], we find that the formal logarithm of D' satisfies

$$\ell_1 \equiv 3 \pmod{3^4}, \quad \ell_2 \equiv 75 \pmod{3^4},$$

and we compute a power series $\theta(n) \in \mathbb{Z}_3[[n]]$ which vanishes whenever $[Q^+ + Q^+] + n \cdot D'$ is of the form $[P + P]$. In our case, we find $\theta(n) \equiv 3n \pmod{3^2}$. Strassman's theorem [5, p. 62] implies that such a power series can have at most one zero in $\mathbb{Z}_3$. We already know that $n = 0$ is a zero, so it the only one. Thus $[P + P] = [Q^+ + Q^+]$, and since $J(\mathbb{Q})$ has no 2-torsion, $P = Q^+$. Applying the hyperelliptic involution, we deduce also that any $P \in \mathcal{C}(\mathbb{Q})$ with the same mod 3 reduction as Q^- must equal Q^-.

Applying the same argument with R^+ instead of Q^+, we find $\theta(n) \equiv 6n \pmod{3^2}$, so we deduce similarly that any $P \in \mathcal{C}(\mathbb{Q})$ with the same mod 3 reduction as R^+ or R^- must equal R^+ or R^-. For ∞^+ instead of Q^+, we obtain $\theta(n) \equiv 6n \pmod{3^2}$, so any $P \in \mathcal{C}(\mathbb{Q})$ with the same mod 3 reduction as ∞^+ or ∞^- must equal ∞^+ or ∞^-.

It remains to be shown that if $P \in \mathcal{C}(\mathbb{Q})$ reduces to $(1,0)$ modulo 3, then P equals S^+ or S^-. Although in theory the same technique as before could be used to bound the number of such rational points, it turns out that in this case even the terms up to degree 7 of the formal logarithm and exponential do not give sufficient 3-adic precision. (In other words, we cannot distinguish $\theta(n)$ from 0 without using a larger number of terms.) Qualitatively, the difficulty seems to be that $(1,0)$ is a Weierstrass point of $\mathcal{C}$ over $\mathbb{F}_3$, so that the image of $\mathcal{C}$ in J under $P \mapsto [P + P]$ has six branches passing the origin $\mathcal{O}$, one for each Weierstrass point, and we can therefore expect $\theta(n)$ to have a zero of multiplicity 6 and to be divisible by many factors of 3. We will circumvent the need for more precision by substituting the embedding $P \mapsto [P + S^+]$ of $\mathcal{C}$ into J for the embedding $P \mapsto [P + P]$.

The rational function $t = y + 3$ is a uniformizing parameter at $S^- = (1, -3)$, so there is a unique power series $\xi(t) \in \mathbb{Q}[[t]]$ which starts

$$\xi(t) = 1 - 3t/8 - 31t^2/512 + 105t^3/16384 + 15269t^4/2097152 + O(t^5)$$

such that $(\xi(t), -3 + t)$ is a point on $\mathcal{C}$ with coordinates in $\mathbb{Q}[[t]]$. Since t is also a uniformizing parameter on the the curve reduced modulo 3, $\xi(t) \in \mathbb{Z}_3[[t]]$, and hence for any $t \in 3\mathbb{Z}_3$, the power series converges to give a point P_t in $\mathcal{C}(\mathbb{Q}_3)$. This analytic parameterization gives all points in $\mathcal{C}(\mathbb{Q}_3)$ which have the same mod 3 reduction as S^-. Let $D_t = [P_t + S^+] \in \mathcal{M}_3 \subset J(\mathbb{Q}_3)$. The local parameters s_1, s_2 of [10] at D_t are again given by power series in $\mathbb{Z}_3[[t]]$:

$$\begin{aligned} s_1(t) &= t/16 + 9t^2/1024 - 111t^3/32768 - 8979t^4/4194304 + O(t^5), \\ s_2(t) &= t/16 + 21t^2/1024 + 141t^3/32768 + 1929t^4/4194304 + O(t^5). \end{aligned}$$

Using the formulas in [10], we find that the power series giving the formal logarithm at D_t for $t = 3n$ satisfy

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

If $t = 3n \in 3\mathbb{Z}_3$ is such that $P_t \in \mathcal{C}(\mathbb{Q})$, then $D_t \in J(\mathbb{Q}) \cap \mathcal{M}_3$, so its logarithm $(L_1(n), L_2(n))$ must be a 3-adic integer multiple of the logarithm (ℓ_1, ℓ_2) of D'. In particular the determinant

$$\Delta(n) \stackrel{\text{def}}{=} \begin{vmatrix} L_1(n) & L_2(n) \\ \ell_1 & \ell_2 \end{vmatrix}$$

must vanish whenever $P_t \in \mathcal{C}(\mathbb{Q})$. The power series $\Delta(n)$ satisfies

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

so by Strassman's Theorem, $\Delta(n) = 0$ for at most three values of $n \in \mathbb{Z}_3$. We already know that $\Delta(0) = \Delta(2) = 0$, since $P_0 = (1, -3)$ and $P_6 = (1, 3)$. At $n = 1$, P_3 is a Weierstrass point W defined over $\mathbb{Q}_3$ and not $\mathbb{Q}$, but $\Delta(1) = 0$ nevertheless: $2D_3 = [S^+ + S^+] + [W + W] = [S^+ + S^+] = -D'$, so the logarithm of D_3 is a multiple of the logarithm of D'. Thus $\Delta(n) \neq 0$ for $n \neq 0, 1, 2$, and it follows that any $P \in \mathcal{C}(\mathbb{Q})$ which reduces to $(1, 0) \in \mathcal{C}(\mathbb{F}_3)$ must be one of $P_0 = S^-$, $P_1 = W$, $P_2 = S^+$. Of these, only S^+ and S^- are actually rational, so we are done. $\square$

Thus there are only the eight points on $\mathcal{C}$. If $z^2 + c$ has a rational point of type 3_2 the corresponding value of $\tau = x$ must be one of $-1, 0, 1, \infty$. But $\tau = -1, 0, \infty$ do not correspond to a valid polynomial $z^2 + c$ in Theorem 1, so the only possibility is $\tau = 1$, which makes $c = -29/16$. Computing the full graph $\mathrm{PrePer}(f, \mathbb{Q})$ for $f(z) = z^2 - 29/16$ (which can be done as in the remarks following Corollary 1) completes the proof of part (4) of Theorem 3.

Acknowledgements

I thank Noam Elkies for computing an equation of $X_1(18)$ for me, and E. V. Flynn for making available his formulas for Jacobians of genus 2 curves.

References

[1] Birch, B. and Kuyk, W. (eds.), Modular functions of one variable IV, *Lecture Notes in Math.* **476**, Springer-Verlag, 1975.
[2] Billing, G. and Mahler, K., On exceptional points on cubic curves, *J. London Math. Soc.* **15** (1940), 32–43.
[3] Call, G. and Goldstine, S., Canonical heights on projective space, preprint, 1995.
[4] Call, G. and Silverman, J., Canonical heights on varieties with morphisms, *Compos. Math.* **89** (1993), 163–205.
[5] Cassels, J. W. S., *Local Fields*, London Mathematical Society Student Texts **3**, Cambridge Univ. Press, 1986.
[6] Chabauty, C., Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, *Comptes Rendus Hebdomadaires des Séances de l'Academie des Sciences, Paris* **212** (1941), 882–885.
[7] Coleman, R. F., Effective Chabauty, *Duke Math. J.* **52** (1985), 765–780.
[8] Cremona, J., *Algorithms for modular elliptic curves*, Cambridge Univ. Press, 1992.
[9] Elkies, N., private electronic communication, June 26, 1995.
[10] Flynn, E. V., Poonen, B., and Schaefer, E., Cycles of quadratic polynomials and rational points on a genus 2 curve, preprint, 1995.
[11] Flynn, E. V., The group law on the Jacobian of a curve of genus 2., *J. Reine Angew. Math.* **439** (1993), 45–69.
[12] Levi, B., Sull'equazione indeterminata del 3° ordine, *Atti del IV Congresso Internazionale dei matematici, Roma 1908* **2**, 175–177.
[13] Lewis, D., Invariant sets of morphisms on projective and affine number spaces, *Journal of Algebra* **20** (1972), 419–434.
[14] Mazur, B., Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47** (1977), 33–186.
[15] Mazur, B. and Tate, J., Points of order 13 on elliptic curves, *Invent. Math.* **22** (1973), 41–49.
[16] Merel, L., Existence d'une borne uniforme pour les nombres premiers de torsion des courbes elliptiques sur les corps de nombres, preprint, 1994.
[17] Morton, P., Arithmetic properties of periodic points of quadratic maps, *Acta Arith.* **62** (1992), 343–372.
[18] Morton, P., Arithmetic properties of periodic points of quadratic maps, II, preprint, 1995.
[19] Morton, P. and Silverman, J., Rational periodic points of rational functions, *Internat. Math. Res. Notices*, 97–110.
[20] Narkiewicz, W., On polynomial transformations in several variables, *Acta Arith.* **11** (1965), 163–168.
[21] Northcott, D., Periodic points on an algebraic variety, *Annals of Math.* **51** (1950), 167–177.
[22] Ogg, A., Rational points of finite order on elliptic curves, *Inv. Math.* **12** (1971), 105–111.
[23] Poonen, B., Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture, preprint, 1995.
[24] Walde, R. and Russo, P., Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$, *Amer. Math. Monthly* **101** (1994), 318–331.

Department of Mathematics, Princeton University, Princeton, NJ 08544-1000, USA

E-mail address: poonen@@math.princeton.edu