CYCLES OF QUADRATIC POLYNOMIALS AND RATIONAL POINTS ON A GENUS 2 CURVE

E. V. FLYNN, BJORN POONEN, AND EDWARD F. SCHAEFER

Abstract. It has been conjectured that for N sufficiently large, there are no quadratic polynomials in $\mathbb{Q}[z]$ with rational periodic points of period N. Morton proved there were none with $N = 4$, by showing that the genus 2 algebraic curve that classifies periodic points of period 4 is birational to $X_1(16)$, whose rational points had been previously computed. We prove there are none with $N = 5$. Here the relevant curve has genus 14, but it has a genus 2 quotient, whose rational points we compute by performing a 2-descent on its Jacobian and applying a refinement of the method of Chabauty and Coleman. We hope that our computation will serve as a model for others who need to compute rational points on hyperelliptic curves. We also describe the three possible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable 5-cycles, and show that there exist $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycles for infinitely many N. Furthermore, we answer a question of Morton by showing that the genus 14 curve and its quotient are not modular. Finally, we mention some partial results for $N = 6$.

1. Introduction

Let $g(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geq 2$. We consider g as a map on $\mathbb{P}^1(\mathbb{C})$. If $x \in \mathbb{P}^1(\mathbb{C})$ and the sequence

$$x, g(x), g(g(x)), \ldots, g^{\circ n}(x), \ldots$$

is eventually periodic, then x is called a *preperiodic point* for g. If furthermore $g^{\circ n}(x) = x$, then x is called a *periodic point* of g of period n, and its orbit

$$\{x, g(x), g(g(x)), \ldots, g^{\circ(n-1)}(x)\}$$

is called an *n-cycle* if x does not actually have smaller period. Northcott [31] proved in 1950 that for fixed g, there are only finitely many preperiodic points in $\mathbb{P}^1(\mathbb{Q})$. Moreover, these can be computed effectively given g. This theorem also holds over any fixed number field, and also for morphisms of $\mathbb{P}^n$ of degree at least 2. Since

Date: July 25, 1995.

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

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

The second author is supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. Research at MSRI is supported in part by NSF grant DMS-9022140. The third author is supported by an NSA Young Investigators Grant and a Paul Locatelli Junior Faculty Fellowship.

then, the theorem (in varying degrees of generality) has been rediscovered by many authors [30], [20], [2].

It is much more difficult to obtain *uniform* results for rational functions of a given degree. Morton and Silverman [28] have proposed the following conjecture.

Conjecture 1. Let $K/\mathbb{Q}$ be a number field of degree D, and let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over K. The number of K-rational preperiodic points of ϕ can be bounded in terms of D, N, and d only.

To demonstrate the strength of this conjecture, let us remark that the case $N = 1$ and $d = 4$ would imply the recently proved strong uniform boundedness conjecture for torsion of elliptic curves [23], namely that for any D there exists $C > 0$ such that for any elliptic curve E over a number field K of degree D over $\mathbb{Q}$, $\#E(K)_{\mathrm{tors}} < C$. This is because 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 [32], which is still open.

Even the simplest cases of the conjecture seem to be difficult. Walde and Russo [37] asked whether a quadratic polynomial in $\mathbb{Q}[z]$ can have rational points of period greater than 3, and this is not known. Pairs consisting of a quadratic polynomial and a point of period N are classified by an algebraic curve, which we denote $C_1(N)$. For $N = 1, 2, 3$, this curve is birational over $\mathbb{Q}$ to $\mathbb{P}^1$, so it is easy to find a quadratic $g \in \mathbb{Q}[z]$ with a rational point of period 1, 2, or 3. Morton [26] proved that $C_1(4)$ is birational over $\mathbb{Q}$ to the modular curve $X_1(16)$, and used this to show that there are no quadratic polynomials in $\mathbb{Q}[z]$ with rational points of period 4. Our main theorem is for the case $N = 5$:

Theorem 1. *There is no quadratic polynomial $g(z) \in \mathbb{Q}[z]$ with a rational point of exact period 5.*

The curve $C_1(5)$ has genus 14, so we study it via a quotient curve $\mathcal{C} = C_0(5)$ of genus 2. In Section 9, we will use the description of endomorphism rings of quotients of the Jacobian $J_1(N)$ of $X_1(N)$ to show that there is no surjective morphism of curves over $\mathbb{C}$ from $X_1(N)$ to $C_0(5)$ or $C_1(5)$, for any $N \geq 1$. Because of this, finding the set of rational points will be more challenging than it was for $C_1(4)$. To find all the rational points on $\mathcal{C}$, we first put $\mathcal{C}$ into hyperelliptic form, and then use a 2-descent to compute the rank of its Jacobian, which turns out to be 1. The 2-descent is more difficult than the examples of descents for hyperelliptic curves worked out in the literature ([9],[13],[36]) in that $\mathcal{C}$ has no Weierstrass points defined over $\mathbb{Q}$ or even a quadratic extension; in fact, the smallest field over which all the Weierstrass points are defined is the splitting field of a sextic with Galois group S_6, the worst possible case. But because the rank is less than the genus, it is possible afterwards to apply the method of Chabauty and Coleman to bound the number of rational points on the curve. Although Coleman's original method gives at best an upper bound of 9 for the number of rational points, our refinements of the method are strong enough to show that there are at most six rational points. On the other hand, it is easy to list six rational points, so we know that we have found them all.

We will also list (in Table 2) all quadratic polynomials in $\mathbb{Q}[z]$ (up to linear conjugacy) with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable 5-cycle. Each point in such a cycle generates a degree 5 cyclic extension of $\mathbb{Q}$, which we describe. Also we prove that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycles exist for infinitely many N.

Finally, in Section 10, we describe the known $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable 6-cycles. If, as we believe, these are all, then there is no quadratic polynomial $g(z) \in \mathbb{Q}[z]$ with a rational point of exact period 6. This leads us to conjecture the following refinement of Conjecture 1 for the case of quadratic polynomials over $\mathbb{Q}$.

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

Throughout the paper, we use Mathematica (version 2.2) and the GP/PARI Calculator (version 1.39). Version 1.39 of PARI assumes the Generalized Riemann Hypothesis for certain number field calculations, but Michel Olivier has kindly verified these particular calculations for us using a newer not yet released version that makes no such assumptions.

2. Periodic points of quadratic polynomials

If $g(z) \in \mathbb{Q}[z]$ is any quadratic polynomial, then there exists a linear function $\ell(z) \in \mathbb{Q}[z]$ such that $\ell(g(\ell^{-1}(z)))$ is of the form $z^2 + c$. Therefore, for the sake of arithmetic dynamics, it will suffice to consider polynomials of the form $g(z) = z^2 + c$. If z is periodic of exact period N for g (meaning that it is periodic of period N, but not periodic of period n for any $n < N$), then z satisfies the equation

$$g^{\circ N}(z) - z = 0. \tag{1}$$

But (1) is satisfied also by points of exact period d for d dividing N, so there is a factorization

$$g^{\circ N}(z) - z = \prod_{d|N} \Phi_d(z, c)$$

where

$$\Phi_d(z, c) = \prod_{m|d} (g^{\circ m}(z) - z)^{\mu(m)} \in \mathbb{Z}[z, c] \tag{2}$$

is the polynomial whose roots z for generic c are the periodic points of exact period d. (Here μ is the Möbius μ-function.) The z-degree of $\Phi_N(z,c)$ is

$$\nu_2(N) \stackrel{\text{def}}{=} \sum_{d|N} 2^d \mu(N/d).$$

By Theorem 1 in [1], $\Phi_N(z,c)$ (where now c also is considered to be an indeterminate) is irreducible in $\mathbb{C}[z,c]$, and hence

$$\Phi_N(z,c) = 0$$

defines a geometrically irreducible algebraic curve over $\mathbb{Q}$ in the (z,c)-plane. Although the affine part of this curve is nonsingular (Proposition 1 of [1]), there is a singularity at infinity on its projective closure if $N > 2$, so we let $C_1(N)$ denote the normalization, which is a nonsingular projective curve over $\mathbb{Q}$. Every pair consisting of a polynomial $g(z) = z^2 + c$ together with a rational point of exact period N gives rise to a rational point on the affine part of $C_1(N)$. The converse is true for almost all affine rational points, but there can be exceptions, as noted in Section 1 of [29], and these can be explained by assigning multiplicities to periodic points. For example, $(z,c) = (-1/2, -3/4)$ is a point on $C_1(2)$, but $-1/2$ is actually a fixed point of $g(z) = z^2 - 3/4$ instead of a point of exact period 2. (In fact, it seems likely that there are no other such examples for quadratic polynomials over $\mathbb{Q}$; this would follow from Conjecture 2, for example.)

The curve $C_1(N)$ has an obvious automorphism σ given in the (z,c)-plane by $(z,c) \mapsto (z^2+c, c)$. (All we are saying here is that if α is a point of exact period N for $g(z) = z^2 + c$, then so is $g(\alpha)$.) This automorphism generates a group $\langle\sigma\rangle$ of order N, and we let $C_0(N)$ be the quotient curve $C_1(N)/\langle\sigma\rangle$. Then $C_0(N)$ is again a nonsingular projective curve over $\mathbb{Q}$, and its rational points correspond (with finitely many exceptions) to pairs consisting of a polynomial $g(z) = z^2 + c$, $c \in \mathbb{Q}$, with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycle. For example, $C_0(4)$ has a rational point corresponding to $g(z) = z^2 - 31/48$ with the 4-cycle

$$\begin{array}{ccc} 1/4 + \sqrt{-15}/6 & \longrightarrow & -1 + \sqrt{-15}/12 \\ \uparrow & & \downarrow \\ -1 - \sqrt{-15}/12 & \longleftarrow & 1/4 - \sqrt{-15}/6 \end{array}$$

(The notation is intended to remind the reader of the modular curves $X_0(N)$ and $X_1(N)$, which parameterize elliptic curves together with a cyclic subgroup of order N, or a point of order N, respectively.) Because field automorphisms must preserve polynomial relations over $\mathbb{Q}$, the action of an automorphism in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycle is a rotation. Thus we obtain a homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/N\mathbb{Z}$, and a point in such an N-cycle generates an abelian extension that is independent of

N	$g(C_0(N))$	$g(C_1(N))$
1	0	0
2	0	0
3	0	0
4	0	2
5	2	14
6	4	34
7	16	124
8	32	285
9	79	745
10	162	1690

TABLE 1. Genus of $C_0(N)$ and $C_1(N)$ for $N \leq 10$.

which point was chosen, since any such point can be expressed as a polynomial over $\mathbb{Q}$ in any other.

Bousch [1] derived a formula for the genus of $C_1(N)$. Later, Morton [27, Theorem C] generalized the formula to some other families of polynomials, and also derived a formula for the genus of $C_0(N)$, which is birational to his curve $\delta_N(x,c) = 0$. Here are the formulas, which are given in terms of $\nu(N) \stackrel{\text{def}}{=} \nu_2(N)/2$:

$$g(C_1(N)) = 1 + \left(\frac{N-3}{2}\right)\nu(N) - \frac{1}{2}\sum_{d|N, d\neq N} d\nu(d)\phi\left(\frac{N}{d}\right);$$

$$g(C_0(N)) = 1 + \left(\frac{1}{2} - \frac{3}{2N}\right)\nu(N) - \frac{1}{2}\sum_{d|N, d\neq N} \nu(d)\phi\left(\frac{N}{d}\right)$$

if N is odd; and

$$g(C_0(N)) = 1 + \left(\frac{1}{2} - \frac{3}{2N}\right)\nu(N) - \frac{1}{2}\sum_{d|N, d\neq N} \nu(d)\phi\left(\frac{N}{d}\right) - \frac{1}{4N}\sum_{r|N, 2|r, N/r \text{ odd}} \mu\left(\frac{N}{r}\right)2^{r/2},$$

if N is even. Table 1 gives these values for $N \leq 10$.

For $N = 1$, 2, or 3, $C_1(N)$ is in fact birational over $\mathbb{Q}$ to $\mathbb{P}^1$, so examples of quadratic polynomials in $\mathbb{Q}[x]$ with points of period 1, 2, or 3 exist in abundance. These are classified explicitly in [37]. In [26], it is proved that $C_1(4)$ is birational over $\mathbb{Q}$ to the curve

$$v^2 = u(u^2+1)(1+2u-u^2),$$

which also happens to be an equation for $X_1(16)$. Although at first this may appear to be a surprising coincidence, we can give a partial explanation: the Jacobian of a genus 2 curve with an automorphism of order 4 defined over $\mathbb{Q}$ is automatically an abelian variety of GL_2-type, and hence conjecturally is a quotient of the Jacobian

$J_1(N)$ of the modular curve $X_1(N)$ for some $N \geq 1$. (See [35].) It has been known since 1908 that (in modern terminology) no elliptic curve over $\mathbb{Q}$ has a rational point of order 16, so the only rational points of $X_1(16)$ are the rational cusps [19]. This fact is what enabled Morton [26] to prove that all rational points on $C_1(4)$ were at infinity.

Morton [26] asked whether $C_1(N)$ was modular also for $N > 4$. We will prove in Section 9 that $C_0(5)$ and $C_1(5)$ are *not* modular. The curve $C_1(5)$ is of genus 14 and is of degree 30 in the (z, c)-plane, so it is much too complicated to be studied directly. Instead we will work with $\mathcal{C} \stackrel{\text{def}}{=} C_0(5)$, which has genus 2. Of course, every rational point of $C_1(5)$ maps to a rational point of $\mathcal{C}$.

Before proceeding with the calculation of the rational points of $\mathcal{C}$, let us show that the "affine part" of $C_0(N)$ has rational points for infinitely many N. This contrasts with the modular curve situation, since for $N > 163$, the only rational points of $X_0(N)$ are the rational cusps. (The result for $X_0(N)$ involved many cases, which were worked out by several different authors. See [15] for a brief summary.)

Theorem 2. *There are infinitely many N for which there exists a quadratic polynomial $g(z) \in \mathbb{Q}[z]$ with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycle.*

Proof. For each $k \geq 1$, the image of 2 is a generator of $(\mathbb{Z}/3^k\mathbb{Z})^*$. Then under the map $g(z) = z^2$, the orbit of a primitive 3^k-th root of unity ζ is a $(2 \cdot 3^{k-1})$-cycle consisting of all primitive 3^k-th roots of unity, which is clearly $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable. (A similar argument could be used with $g(z) = z^2 - 2$ and $\zeta + \zeta^{-1}$.) □

Although the proof was disappointingly simple, it does raise an interesting question.

Question . Is it true that for sufficiently large N, if $g(z) = z^2 + c$ has a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycle, then $c = 0$ or $c = -2$?

For many N (for example, $N = 7$), not even z^2 and $z^2 - 2$ have $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycles. More precisely, it is easy to show that z^2 has a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycle if and only if $N = \phi(n)$ where n is a positive integer for which the image of 2 is a generator of $(\mathbb{Z}/n\mathbb{Z})^*$ (which forces n to an odd prime power). Similarly, $z^2 - 2$ has a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable N-cycle if and only if $N = \phi(n)/2$ where the image of 2 generates $(\mathbb{Z}/n\mathbb{Z})^*/\langle -1 \rangle$ (which forces n to be the product of at most two odd prime powers).

3. A hyperelliptic form of $\mathcal{C}$

Because $\mathcal{C}$ has genus 2, it is hyperelliptic, and more specifically is birational to a curve $\mathcal{C}$ of the form $y^2 = f(x)$, where $f(x) \in \mathbb{Q}[x]$ is of degree 5 or 6 and has distinct roots. For the future calculations, it will be necessary to find $f(x)$ explicitly. This will be the concern of this section.

Following Morton [26], we define the *trace* of an N-cycle in $\mathbb{C}$ of $g(z) = z^2 + c$ to be the sum of the elements in the cycle. Then we let $\tau_N(z, c) \in \mathbb{Z}[z, c]$ be the polynomial whose roots for generic c are the traces of all the N-cycles. The curve $\tau_N(z,c)=0$ is birational over $\mathbb{Q}$ to $C_0(N)$. (See [27].) In [26], Morton also gives an efficient method for computing $\tau_N(z,c)$ for small N.

We will start with his result for $N=5$:

$$\begin{aligned}\tau_5(z,c) = &\left(32+28c+40c^2+9c^3\right)+\left(36-24c+17c^2\right)z+\left(44+19c+19c^2\right)z^2\\ &+(11+18c)\,z^3+(3+11c)\,z^4+z^5+z^6.\end{aligned}$$

Solving the system

$$\tau_5 = \partial\tau_5/\partial z = \partial\tau_5/\partial c = 0,$$

we find that the only singularity of the curve $\tau_5(z,c)=0$ in the affine (z,c)-plane is $(-1,-4/3)$, which is a node. Therefore we substitute $z=r-1$ and $c=s-4/3$ and clear denominators to obtain a new model with the node at $(0,0)$:

$$238r^2+213r^3-15r^4-45r^5+9r^6+36rs-177r^2s-234r^3s+99r^4s+54s^2-189rs^2+171r^2s^2+81s^3=0.$$

Next we blow up the node by substituting $s=rt$, and dividing by r^2:

$$238+213r-15r^2-45r^3+9r^4+36t-177rt-234r^2t+99r^3t+54t^2-189rt^2+171r^2t^2+81rt^3=0.$$

The curve now has no affine singularities, but there must be a singularity at infinity, because a nonsingular plane curve cannot have genus 2. A calculation shows that there is a singularity at infinity on the line $r+t=0$, which we move to an axis by setting $r=q-t$:

$$238+213q-15q^2-45q^3+9q^4-177t-147qt-99q^2t+63q^3t+216t^2+144qt^2-72q^2t^2=0.$$

Now the left hand side is a quadratic in t, so the curve is birational to

$$p^2=-174303-269082q+15471q^2+115668q^3+5103q^4-30618q^5+6561q^6,$$

where the right hand side is the discriminant of that quadratic. Although this is a hyperelliptic form, it is to our advantage to simplify as much as possible before continuing. We substitute $p=192y$ and $q=-1-4x/3$, and cancel $192^2=36864$ from both sides to obtain

$$\mathcal{C}:\quad y^2=x^6+8x^5+22x^4+22x^3+5x^2+6x+1. \tag{3}$$

Let $f(x)$ be the sextic on the right hand side. Since $f(x)$ has no rational roots, the curve $\mathcal{C}$ is not birational over $\mathbb{Q}$ to a curve of the form $y^2=h(x)$ with $\deg h(x)=5$.

4. Six rational points on $\mathcal{C}$

There are a few easy to find rational points on $\mathcal{C}$. First of all, $f(0)=f(-3)=1$, so we find four affine points: $(0,1)$, $(0,-1)$, $(-3,1)$, and $(-3,-1)$. Also, since $\deg f$ is even, $\mathcal{C}$ has two points at infinity. Since the leading coefficient of $f(x)$ is a square in $\mathbb{Q}$, these points are rational. (See [4, p. 50].) 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 six points are the only rational points on $\mathcal{C}$. For now, we will describe the 5-cycles of quadratic polynomials to which they correspond.

Point	c	Conductor n	$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$
$(0,1)$	∞		
$(0,-1)$	$-16/9$	41	$\langle 3\rangle \subset (\mathbb{Z}/41\mathbb{Z})^*$
$(-3,1)$	$-64/9$	$275 = 5^2 \cdot 11$	$\langle -1, 3\rangle \subset (\mathbb{Z}/275\mathbb{Z})^*$
$(-3,-1)$	∞		
∞^+	∞		
∞^-	-2	11	$\langle -1\rangle \subset (\mathbb{Z}/11\mathbb{Z})^*$

TABLE 2. The six rational points of $\mathcal{C}$.

By tracing back through the substitutions of Section 3, we obtain two equivalent formulas for c in terms of the rational functions x and y on $\mathcal{C}$:

$$c = \frac{P_0(x) + P_1(x)y}{8x^2(3+x)^2} = \frac{64 + 110x + 325x^2 + 452x^3 + 271x^4 + 74x^5 + 8x^6}{2(P_0(x) - P_1(x)y)},$$

where

$$\begin{aligned} P_0(x) &= -9 - 24x - 95x^2 - 104x^3 - 46x^4 - 10x^5 - x^6 \\ P_1(x) &= -9 + 3x + 6x^2 + x^3. \end{aligned}$$

The second formula is determinate (i.e., the numerator and denominator do not both vanish) at the four affine rational points, and this gives the c-values shown in Table 2. At ∞^+, we have the formal expansion

$$y = x^3 + 4x^2 + 3x - 1 + 2x^{-1} + \cdots .$$

Substituting this into the first formula, we see that

$$c = x^2/4 + (\text{lower order terms})$$

so c has a pole at ∞^+. Similarly, at ∞^-, we have

$$y = -(x^3 + 4x^2 + 3x - 1 + 2x^{-1} + \cdots),$$

and substitution into the second formula shows that $c = -2$ there.

For the three values $c = -2, -16/9, -64/9$, we know there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable 5-cycle of $g(z) = z^2 + c$. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the cycle can only be a rotation, so the points of the cycle generate an abelian extension K of $\mathbb{Q}$, whose Galois group is a subgroup of $\mathbb{Z}/5\mathbb{Z}$. In Table 2, we will describe K in each case by giving its conductor (the smallest n for which K is contained in the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$) and the subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ it corresponds to under Galois theory. The quintic polynomial whose roots are the points of the cycle is a factor of $\Phi_5[z, c]$. A computation shows that for each of the three values of c above, there is a unique quintic factor in $\mathbb{Q}[z]$, and none of smaller degree, so already we know that the 5-cycles in question are not defined pointwise over $\mathbb{Q}$, and that in each case K is a degree 5 cyclic extension of $\mathbb{Q}$.

For $c = -2$, PARI tells us that the field K, which is generated by a root of this quintic, has discriminant 11^4, so the conductor of K must be a power of 11. Since $(\mathbb{Z}/11^k\mathbb{Z})^*$ is cyclic, $\mathbb{Q}(\zeta_{11^k})$ has a unique quintic subfield, namely the totally real subfield of $\mathbb{Q}(\zeta_{11})$. Thus the conductor of K equals 11, and under Galois theory K corresponds to the subgroup $\langle -1 \rangle$ of $(\mathbb{Z}/11\mathbb{Z})^*$. This is easy to explain: the 5-cycle of $z^2 - 2$ consists of all conjugates of $\zeta_{11} + \zeta_{11}^{-1}$.

For $c = -16/9$, K has discriminant 41^4, so a similar argument as for $c = -2$ shows that K is the unique quintic subfield of $\mathbb{Q}(\zeta_{41})$. Thus K has conductor 41, and corresponds to the unique subgroup of $(\mathbb{Z}/41\mathbb{Z})^*$ of index 5, which is generated by the image of 3.

For $c = -64/9$, K has discriminant $5^8 \cdot 11^4$, so the conductor of K is of the form $n = 5^k \cdot 11^l$. By Hensel's Lemma, every element of $(\mathbb{Z}/n\mathbb{Z})^*$ congruent to 1 modulo $275 = 5^2 \cdot 11$ is a 5-th power in $(\mathbb{Z}/n\mathbb{Z})^*$, and hence is in $H \stackrel{\text{def}}{=} \operatorname{Gal}(\mathbb{Q}(\zeta_n)/K)$, which has index 5 in $(\mathbb{Z}/n\mathbb{Z})^*$. Thus n divides 275. PARI tells us that the prime 3 splits completely in K, so the Frobenius element at 3 acts trivially on K, and the image of 3 lies in H. Also, the image of -1 lies in H, since H has odd index. But the subgroup generated by -1 and 3 in $(\mathbb{Z}/275\mathbb{Z})^*$ has index 5, so the images of -1 and 3 in $(\mathbb{Z}/n\mathbb{Z})^*$ generate H. Finally, this subgroup of $(\mathbb{Z}/275\mathbb{Z})^*$ does not come from a subgroup of $(\mathbb{Z}/55\mathbb{Z})^*$, so the conductor is actually 275.

5. Generalities on 2-descents on Jacobians of hyperelliptic curves

This section outlines and elaborates upon the descent method described in [4] for Jacobians of genus 2 curves over $\mathbb{Q}$. (See also [9], [13] and [36].) Later, in Section 7, we will apply the results of this section to show that the Mordell-Weil rank of the Jacobian of our curve $\mathcal{C}$ is exactly 1. We hope that the separation of the general method from the application will be useful for others who need to do 2-descents on hyperelliptic curves.

Let C be a hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$. Then C has a (singular) plane model $y^2 = f(x)$, with $f(x) \in \mathbb{Z}[x]$ a separable polynomial of even degree $d = 2g + 2$. Let J be the Jacobian of C, which is an abelian variety over $\mathbb{Q}$. We will assume $C(\mathbb{Q})$ is nonempty, so that $\operatorname{Div}^0(C)(K)$ maps onto $J(K)$ for any field extension K of $\mathbb{Q}$. (Actually, when $g = 2$, the latter is true automatically, even when $C(\mathbb{Q})$ is empty.) Without this assumption, the map $(x - T)$ below could be defined only as a map on $\operatorname{Div}^0(C)(K)$. We will call a degree 0 divisor of $\mathcal{C}$ defined over $\mathbb{Q}$ a *good divisor* if its support does not include ∞^+, ∞^- or points with y-coordinate 0.

Proposition 1. *Every divisor class of $J(K)$ contains a good divisor.*

Proof. Since C has a K-rational point, every K-rational divisor class contains a K-rational divisor (see [25, p. 168]). Every K-rational divisor has a linearly equivalent

K-rational divisor whose support avoids any given finite set of points (see [17, p. 166]). □

For a good divisor $D = \sum n_P P$, we define

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

(We use the notation $P = (x_P, y_P)$.) For any field K of characteristic 0, define $L_K = K[T]/(f(T))$.

Proposition 2. *The map $(x-T)$ is a well-defined map from $J(K)$ to the kernel of the norm from $L_K^*/L_K^{*2}K^*$ to K^*/K^{*2}.*

Proof. Let $\alpha_1, \dots, \alpha_d$ be the zeros of $f(x)$ in $\overline{K}$. We can define

$$\overline{L}_K = \overline{K}[T]/(f(T)) \cong \overline{K}[T]/(T-\alpha_1) \times \dots \times \overline{K}[T]/(T-\alpha_d) \cong \overline{K} \times \dots \times \overline{K}$$
$$\text{by } T \mapsto (\alpha_1, \dots, \alpha_d).$$

Let $\mathrm{Gal}(\overline{K}/K)$ act trivially on T; this makes $\overline{L}_K$ a $\mathrm{Gal}(\overline{K}/K)$-module and L_K is the set of $\mathrm{Gal}(\overline{K}/K)$-invariants. Then we can consider $(x-T)$ to be a $\mathrm{Gal}(\overline{K}/K)$-invariant d-tuple of functions $((x-\alpha_1), \dots, (x-\alpha_d))$ whose divisors are $(2(\alpha_1, 0) - \infty^+ - \infty^-, \dots, 2(\alpha_d, 0) - \infty^+ - \infty^-)$. We denote this d-tuple of divisors by $2(T,0) - \infty^+ - \infty^-$.

To show that $(x-T)$ is a well-defined map from $J(K)$ to $L_K^*/L_K^{*2}K^*$, we first note from Proposition 1 that every element of $J(K)$ contains a good divisor. Let D_1 and D_2 be two good divisors that are linearly equivalent. Then there is a K-defined function h with $D_1 - D_2 = \operatorname{div} h$. We have the following equalities of d-tuples:

$$(x-T)(D_1 - D_2) = (x-T)(\operatorname{div} h) = h(\operatorname{div}(x-T)) = h(2(T,0) - \infty^+ - \infty^-) =$$

$$h((T,0))^2/h(\infty^+)h(\infty^-) \in L_K^{*2}K^*.$$

Now let us show that the image of $(x-T)$ is contained in the kernel of the norm to K^*/K^{*2}. Let $D = \sum n_P P$ be a good divisor. If c is the leading coefficient of $f(x)$, then

$$N_{L_K/K}((x-T)(D)) = \prod_P \prod_{j=1}^d (x_P - \alpha_j)^{n_P} = \prod_P (y_P^2/c)^{n_P} = \left(\prod_P y_P^{n_P} \right)^2 \in K^{*2}.$$

□

Let $L = L_{\mathbb{Q}} = \mathbb{Q}[T]/((f(T)) \cong \prod_{i=1}^r L_i$, where the L_i are fields corresponding to the irreducible factors of $f(x)$. Let S be a finite set of primes of $\mathbb{Q}$ containing the primes 2, ∞, and all primes dividing the discriminant of $f(x)$. (In particular, S contains all primes dividing the leading coefficient of $f(x)$.) Suppose $l \in L^*$ maps to l_i in L_i^*. Then we say that l is *unramified outside* S if for each i, the field extension $L_i(\sqrt{l_i})/L_i$ is unramified outside of primes lying over primes of S. This property of

l depends only on the image of l in L^*/L^{*2}, and it is easy to see that the subset G of elements of L^*/L^{*2} which are unramified outside S is a subgroup. Let G' be the image of G in $L^*/L^{*2}\mathbb{Q}^*$, and let H be the kernel of the norm from G' to $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Proposition 3. *The image of the map $(x-T)$ on $J(\mathbb{Q})$ is contained in the subgroup H of $L^*/L^{*2}\mathbb{Q}^*$.*

Proof. By Proposition 2, the image of $(x-T)$ is contained in the kernel of the norm to $\mathbb{Q}^*/\mathbb{Q}^{*2}$. So it suffices to show that the image of $(x-T)$ on any good divisor $D = \sum_P n_P P$ is contained in G'.

For each $p \notin S$, fix an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$. Let v be the additive p-adic valuation on $\overline{\mathbb{Q}}_p$ with $v(p) = 1$. Since D is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable, $\prod_{v(x_P)<0} x_P^{n_P}$ is fixed by the inertia group of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and hence its valuation is an integer a_p. Moreover since the embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ is unique up to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the left, a_p is independent of the embedding.

Let $m = \prod_{p \notin S} p^{a_p} \in \mathbb{Q}^*$. We claim that $m^{-1}(x-T)(D) \in L^*/L^{*2}$ is unramified outside S (i.e., is in G), or what is the same thing, that for any $p \notin S$ and any ring homomorphism $\iota : \overline{\mathbb{Q}}[T]/(f(T)) \to \overline{\mathbb{Q}}_p$, $v(m^{-1}(x-T)(D))$ is an even integer. (We extend v to $\overline{\mathbb{Q}}[T]/(f(T))$ by applying ι when necessary.) Let $\alpha_1, \dots, \alpha_d$ be the zeros of $f(x)$ in $\overline{\mathbb{Q}}_p$, and without loss of generality assume $\iota(T) = \alpha_1$. If $v(x_P - T) > 0$, then $v(x_P - \alpha_i) = 0$ for $2 \le i \le d$, since the α_i lie in distinct residue classes of the ring of integers of $\overline{\mathbb{Q}}_p$. In this case,

$$v(x_P - T) = v\left(\prod_{i=1}^{d}(x_P - \alpha_i)\right) = v(y_P^2/c) = 2v(y_P),$$

where c is the leading coefficient of $f(x)$, which by assumption is an S-unit. Hence

$$v((x-T)(D)) = \sum_{v(x_P-T)>0} v((x_P-T)^{n_P}) + \sum_{v(x_P-T)<0} v((x_P-T)^{n_P}) \tag{4}$$

$$= 2v\left(\prod_{v(x_P-T))>0} y_P^{n_P}\right) + v(m) \tag{5}$$

since $v(x_P - T) = v(x_P)$ when either is negative. The product in (5) is again stable under the inertia group of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, so its valuation is an integer. Thus $v(m^{-1}(x-T)(D))$ is an even integer. ◻

Let $L_p = L_{\mathbb{Q}_p} = \mathbb{Q}_p[T]/(f(T))$. We have a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & J(\mathbb{Q})/\ker(x-T) & \xrightarrow{x-T} & L^*/L^{*2}\mathbb{Q}^* \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_{p\in S} J(\mathbb{Q}_p)/\ker(x-T) & \xrightarrow{x-T} & \prod_{p\in S} L_p^*/L_p^{*2}\mathbb{Q}_p^*. \end{array} \tag{6}$$

From this diagram and Proposition 3, we deduce that $x-T$ maps $J(\mathbb{Q})/\ker(x-T)$ injectively into the subgroup H' of elements of H that for each $p \in S$ map in $L_p^*/L_p^{*2}\mathbb{Q}_p^*$ into the image of $J(\mathbb{Q}_p)$ under $x-T$. The latter is something that can be calculated, and this will give bounds on the size of $J(\mathbb{Q})/\ker(x-T)$.

In order to convert these bounds into bounds on the size of $J(\mathbb{Q})/2J(\mathbb{Q})$, which will let us bound the rank of $J(\mathbb{Q})$, we need to know how $\ker(x-T)$ compares with $2J(\mathbb{Q})$. Since $(x-T)$ maps $J(\mathbb{Q})$ into an elementary 2-group, clearly $2J(\mathbb{Q}) \subseteq \ker(x-T)$. We will describe the difference between these two groups in Proposition 5 below, for the genus 2 case. The result is stated over arbitrary fields of characteristic not equal to 2, since we will need it for the completions of $\mathbb{Q}$ as well as for $\mathbb{Q}$ itself. We will make use of the following well known consequence of the Riemann-Roch theorem.

Proposition 4. *Suppose* $\deg f(x) = 6$, *so the genus of* C *is* 2. *Then any divisor class in* $J(K)$ *may be represented by a divisor of the form* $P_1 + P_2 - \infty^+ - \infty^-$ *where either* $P_1, P_2 \in C(K)$ *or* $P_1, P_2 \in C(K')$, *with* $[K' : K] = 2$ *and* P_1, P_2 *conjugate over* K. *This representation is unique (up to interchanging* P_1 *and* P_2*), except for the group identity* $\mathcal{O}$ *of* $J(K)$, *which can be represented by any divisor of the form* $(x,y) + (x,-y) - \infty^+ - \infty^-$ *or* $\infty^+ + \infty^- - \infty^+ - \infty^-$.

Proposition 5. *Suppose that* $f(x) \in K[x]$ *is a separable sextic polynomial over a field* K *with* $\mathrm{char}(K) \neq 2$, *and that the genus 2 curve* $C : y^2 = f(x)$ *has a point* P *defined over* K. *Let* J *be the Jacobian of* C. *Then the index of* $2J(K)$ *in* $\ker(x-T)$ *is*

- *1 if* $f(x)$ *has a zero in* K, *or if there is some* $\mathrm{Gal}(K^{sep}/K)$*-stable partition of the six zeros into two indistiguished 3-element subsets* $\{\{\alpha_1,\alpha_2,\alpha_3\},\{\alpha_4,\alpha_5,\alpha_6\}\}$
- *2 otherwise.*

Proof. The index of $2J(K)$ in $\ker(x-T)$ is 1 or 2 and $\ker(x-T)/2J(K)$ is generated by $[2P - \infty^+ - \infty^-]$ (see [4, lemma 5.2,theorem 5.3]). So the index is 1 exactly when $[2P - \infty^+ - \infty^-]$ is in $2J(K)$. Now $[2P - \infty^+ - \infty^-]$ is in $2J(K)$ if and only if one of the 16 divisor classes with double $[2P - \infty^+ - \infty^-]$ is in $J(K)$.

We now find these 16 divisor classes. Let $\alpha_1, \ldots, \alpha_6$ be the roots of $f(x)$ in some algebraic closure. We will use repeatedly and without further mention the fact that the divisors $2(\alpha_i, 0)$ and $\infty^+ + \infty^-$ are linearly equivalent. Since

$$2[P + (\alpha_1, 0) - \infty^+ - \infty^-] = [2P - \infty^+ - \infty^-],$$

the 16 halves of $[2P - \infty^+ - \infty^-]$ can be obtained by adding $[P + (\alpha_1, 0) - \infty^+ - \infty^-]$ to each of the 16 elements of $J[2]$. By Proposition 4, the 15 divisor classes $[(\alpha_i, 0) + (\alpha_j, 0) - \infty^+ - \infty^-]$ with $i < j$ are distinct, and each has order 2. Thus the 16 halves of $[2P - \infty^+ - \infty^-]$ are the 6 divisor classes of the form

$$[P + 2(\alpha_1, 0) + (\alpha_i, 0) - 2\infty^+ - 2\infty^-] = [P + (\alpha_i, 0) - \infty^+ - \infty^-]$$

and the 10 divisor classes of the form

$$[P + (\alpha_1, 0) + (\alpha_j, 0) + (\alpha_k, 0) - 2\infty^+ - 2\infty^-]$$

with $1 < j < k$.

The action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on the first 6 halves is the same as the action on the roots $\alpha_1, \dots, \alpha_6$. To deduce the action on the other 10 halves, note that if $1 < j < k$ and l, m, n are the other three possible indices, then

$$[P+(\alpha_l,0)+(\alpha_m,0)+(\alpha_n,0)-2\infty^+-2\infty^-] = [P+(\alpha_1,0)+(\alpha_j,0)+(\alpha_k,0)-2\infty^+-2\infty^-]$$

because the difference of the two divisors is $\mathrm{div}((x - \alpha_1)(x - \alpha_j)(x - \alpha_k)/y)$. Hence the action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on these 10 halves is the same as the action on the 10 partitions of the six roots into two indistinguished 3-element subsets.

Thus the conditions given in the proposition are necessary and sufficient for $[2P - \infty^+ - \infty^-]$ to be in $2J(K)$. By our earlier remarks, this completes the proof. □

We conclude this section with a few remarks on computing the function $(x - T)$. Although $P + Q - \infty^+ - \infty^-$ is not a good divisor, the image of $(x - T)$ on its divisor class can be found in terms of P and Q. This is described in [4, p. 50]. As an example, if P and Q are both affine and have nonzero y-coordinates, then the image of $[P + Q - \infty^+ - \infty^-]$ is $(x_P - T)(x_Q - T)$. In addition, the image of $[P + \infty^\pm - \infty^+ - \infty^-]$ is $(x_P - T)$.

6. Facts about the number field $L = \mathbb{Q}[T]/(f(T))$

From now on, we specialize to our curve $\mathcal{C}$, for which

$$f(x) = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

Let $L = \mathbb{Q}[T]/(f(T))$. (We will abuse notation by writing T for its image in L.) In this section we will record some data on L obtained from PARI, to be used later, mainly for the 2-descent. The polynomial $f(x)$ is irreducible over $\mathbb{Q}$, so L is a number field. The Galois group of the normal closure M of L is the full symmetric group S_6. The class number of L is 1. (This can be verified without using PARI, without too much difficulty, since the Minkowski bound is only about 12.2.) Two of the six zeros of $f(x)$ are real, so the unit group U has rank 3. The torsion of the unit group is only $\{\pm 1\}$, and the quotient $U/\{\pm 1\}$ is generated by the elements u_1, u_2, u_3 listed in Table 3. The discriminant of f is $2^{12} \cdot 3701$, and the prime factorizations of the ramified prime ideals (2) and (3701) in L are $(\alpha)^2$ and $(\beta_1)(\beta_2)^2(\beta_3)$, respectively,

Element	Definition	Norm
u_1	$(T^3+4T^2+3T-1)/2$	1
u_2	$(T^4+5T^3+7T^2+2T+1)/2$	1
u_3	$(T^4+6T^3+11T^2+5T)/2$	-1
-1	-1	1
α	$(T^5+8T^4+22T^3+23T^2+7T+5)/2$	2^3
β_1	$(-T^5-5T^4-5T^3+2T^2-3T+6)/2$	3701
β_2	$(T^4+7T^3+15T^2+14T+9)/2$	-3701
β_3	$(14T^5+155T^4+497T^3+439T^2-174T+143)/2$	3701^3

TABLE 3. Some elements of L.

where $\alpha, \beta_1, \beta_2, \beta_3$ are defined as in Table 3. The factorization of 2 and 3701 into irreducible *elements* of L will be given in Table 4.

Let $L_p = \mathbb{Q}_p[T]/(f(T))$ be the completion of L at a prime p of $\mathbb{Q}$. This will be a field if and only if there is only one prime of L above p, which happens when $p = 2$, for instance. For $p = 3701$, we have

$$L_{3701} \cong \mathbb{Q}_{3701} \times E \times F$$

where E is a totally ramified extension of $\mathbb{Q}_{3701}$ of degree 2, and F is the unramified extension of $\mathbb{Q}_{3701}$ of degree 3. The element T maps in $\mathbb{Q}_{3701}$ to something that is 1371 modulo 3701, and in E to something that is 1727 modulo the maximal ideal.

Finally we will need to know how 2 splits in the subfield K of M corresponding to the subgroup G of S_6 of elements that stabilize the partition $\{\{1,2,3\},\{4,5,6\}\}$ of $\{1,2,3,4,5,6\}$ into two indistinguishable subsets. Since the orbit of $\{\{1,2,3\},\{4,5,6\}\}$ under the action of S_6 consists of $\binom{6}{3}/2 = 10$ partitions, $[K:\mathbb{Q}] = (S_6 : G) = 10$. Let $\alpha_1, \ldots, \alpha_6$ be the roots of $f(x)$ in M, which we consider as a subfield of $\mathbb{C}$. Then $\alpha_1\alpha_2\alpha_3 + \alpha_4\alpha_5\alpha_6 \in K$, and its conjugates are similar sums corresponding to the other partitions. We can construct numerically the degree 10 polynomial $h(x)$ whose roots are these sums, and since these sums are the conjugates of an algebraic integer, the coefficients are integers, and we find the polynomial exactly:

$$h(x) = x^{10}+22x^9+53x^8+654x^7+2186x^6+8976x^5+38705x^4+89560x^3+244664x^2+565728x+477968.$$

This polynomial is irreducible over $\mathbb{Q}$, and it follows that $K = \mathbb{Q}(\alpha_1\alpha_2\alpha_3 + \alpha_4\alpha_5\alpha_6)$. Finally, the prime 2 factors in K as $\mathfrak{p}^4\mathfrak{q}^2$ where $\mathfrak{p}$ is of degree 1 and $\mathfrak{q}$ is of degree 3, so in particular $h(x)$ has no zeros in $\mathbb{Q}_2$.

7. THE 2-DESCENT ON $\mathcal{C}$

From now on, J will denote the Jacobian of the curve $\mathcal{C}$. We will compute the Mordell-Weil rank of J by performing the 2-descent outlined in Section 5. Since f has discriminant $2^{12} \cdot 3701$, we take $S = \{2, 3701, \infty\}$, which contains all possible primes of bad reduction for J. (In fact, our curve has good reduction at 2, because substituting $y = 2z + x^3 + x + 1$ and dividing by 4 yields the model

$$z^2 + x^3 z + xz + z = 2x^5 + 5x^4 + 5x^3 + x^2 + x,$$

which has bad reduction only at 3701. But because we are doing a 2-descent, we must include 2 in S anyway.) Let $J(\mathbb{Q})_{\mathrm{tors}}$ denote the torsion subgroup of the finitely generated abelian group $J(\mathbb{Q})$.

Proposition 6. *$J(\mathbb{Q})_{tors}$ is trivial.*

Proof. For any prime p of good reduction for J, the reduction mod p map from $J(\mathbb{Q})$ to $J(\mathbb{F}_p)$ is injective on torsion. (See [14], for example.) By [13, p. 822],

$$\#J(\mathbb{F}_p) = \frac{1}{2}\#\mathcal{C}(\mathbb{F}_{p^2}) + \frac{1}{2}(\#\mathcal{C}(\mathbb{F}_p)^2) - p.$$

This can be obtained alternatively by evaluating the characteristic polynomial at 1. (For a formula for the characteristic polynomial, see the proof of Proposition 9 in Section 9.) Using this, we find $\#J(\mathbb{F}_3) = 9$ and $\#J(\mathbb{F}_5) = 41$. But $\gcd(9, 41) = 1$, so $\#J(\mathbb{Q})_{\mathrm{tors}} = 1$. □

An immediate corollary is that $[\infty^+ - \infty^-]$ generates an infinite subgroup of $J(\mathbb{Q})$ so the rank of $J(\mathbb{Q})$ is at least 1. Also, the fact $\#J(\mathbb{F}_5) = 41$ easily implies the following:

Proposition 7. *J is not isogenous over $\mathbb{Q}$ to a product of two elliptic curves E_1, E_2 over $\mathbb{Q}$.*

Proof. If J were isogenous over $\mathbb{Q}$ to $E_1 \times E_2$, then E_1 and E_2 would have good reduction at 5 as well. Also $\#J(\mathbb{F}_5) = \#E_1(\mathbb{F}_5)\#E_2(\mathbb{F}_5)$, so $\#E_1(\mathbb{F}_5)$ and $\#E_2(\mathbb{F}_5)$ would be 1 and 41 in some order. Both of these violate Hasse's bound

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}.$$

□

In Proposition 9 of Section 9, we will prove the much stronger result that J is absolutely simple, and that J has no nontrivial endomorphisms over $\mathbb{C}$. This rules out the possibility of reducing the computation of the rank of $J(\mathbb{Q})$ to the computation of ranks of elliptic curves, so we will need to use the general method outlined in Section 5. We proceed by first calculating the groups G, G', H, H' of Section 5 for our curve.

Lemma 1. *The images of the 8 elements listed in Table 3 in L^*/L^{*2} are a basis for the $\mathbb{F}_2$-vector space G.*

Proof. If $l \in L^*$, then the field extension $L(\sqrt{l})/L$ is unramified at all finite primes of L except possibly those occuring in l and those above 2. Hence the images of the 8 elements in Table 3 are in G. On the other hand, if $l \in L^*$ maps to something in L^*/L^{*2} outside the span of these 8 elements, then there must be a prime of L not above 2, 3701 or ∞ that occurs to an odd power in the prime factorization of l, and then $L(\sqrt{l})/L$ is ramified at that prime. □

Lemma 2. *The images of u_1 and $u_3\beta_1\beta_2$ in $L^*/L^{*2}\mathbb{Q}^*$ form a basis for the $\mathbb{F}_2$-vector space H.*

Proof. If a prime p other than 2 or 3701 occurs to an odd power in the factorization of $q \in \mathbb{Q}^*$, then $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ is ramified at p, and $L/\mathbb{Q}$ is unramified at p, so $L(\sqrt{q})/L$ is ramified at any prime above p and $q \notin G$. On the other hand, by Table 4, the images of -1, 2, 3701 equal the images of -1, u_2, and $\beta_1\beta_3$ in G. Therefore $G' \subset L^*/L^{*2}\mathbb{Q}^*$ is the quotient of G by the latter three elements, and the images of $u_1, u_3, \alpha, \beta_1, \beta_2$ form a basis. By Table 3, the kernel of the norm map from G' to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is the subspace generated by u_1 and $u_3\beta_1\beta_3$. □

Lemma 3. *The last three columns of Table 4 are accurate.*

Proof. The nontrivial 2-torsion points of J over $\overline{\mathbb{Q}}_p$ are of the form $[(\alpha_i, 0) + (\alpha_j, 0) - \infty^+ - \infty^-]$, where α_i, α_j are two of the six zeros of $f(x)$. Over $\mathbb{Q}_2$, $f(x)$ is irreducible, so $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ acts transitively on the six zeros, and hence no pair can be Galois-stable. Thus $J(\mathbb{Q}_2)[2]$ is trivial.

Over $\mathbb{Q}_{3701}$, $f(x)$ factors into polynomials of degrees $1, 2, 3$. Here the only pair of zeros that is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_{3701}/\mathbb{Q}_{3701})$ is the pair of zeros of the quadratic factor. Hence $J(\mathbb{Q}_{3701})[2]$ has one nontrivial point.

Over $\mathbb{R}$, $f(x)$ factors into polynomials of degrees $1, 1, 2, 2$. The pairs of zeros stable under complex conjugation are the pair of real zeros, and the pairs of zeros of each quadratic factor. Hence $J(\mathbb{R})[2]$ has three nontrivial points.

The multiplication-by-2 map on $J(\mathbb{Q}_p)$ is an n-to-1 map onto its image, where $n = \#J(\mathbb{Q}_p)[2]$, and locally it multiplies Haar measure by $|2|_p^2$ since $J(\mathbb{Q}_p)$ is a 2-dimensional Lie group over $\mathbb{Q}_p$. Hence the measure of $2J(\mathbb{Q}_p)$ is $|2|_p^2/n$ times the measure of $J(\mathbb{Q}_p)$, so

$$\#J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = |2|_p^{-2} \cdot \#J(\mathbb{Q}_p)[2],$$

which gives the values of the second to last column of Table 4.

From the factorization of 2 in L, we know that $f(x)$ has no roots in $\mathbb{Q}_2$. From Section 6, the polynomial $h(x)$ has no roots in $\mathbb{Q}_2$, so there is no $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-stable partition of the roots of $f(x)$ into two indistinguishable 3-element subsets. Thus by Proposition 5, $2J(\mathbb{Q}_2)$ has index 2 in the kernel of $x - T$ on $J(\mathbb{Q}_2)$. On the other hand, $f(x)$ has a zero in $\mathbb{Q}_{3701}$ and in $\mathbb{R}$, so Proposition 5 implies that the kernel of $x - T$ on $J(\mathbb{Q}_p)$ equals $2J(\mathbb{Q}_p)$ for $p = 3701$ or $p = \infty$. □

p	(e_i, f_i)	Factorization in L	$\#J(\mathbb{Q}_p)[2]$	$\#J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$	$\#J(\mathbb{Q}_p)/\ker(x-T)$
2	$(2,3)$	$\alpha^2 u_2$	1	4	2
3701	$(1,1);(2,1);(1,3)$	$\beta_1\beta_2^2\beta_3$	2	2	2
∞	$(1,1);(1,1);(2,1);(2,1)$		4	1	1

TABLE 4. The primes in S.

Next we will need to find generators for $J(\mathbb{Q}_p)/\ker(x-T)$ for each prime p in S.

Lemma 4. *The 1-dimensional $\mathbb{F}_2$-vector spaces*

$$J(\mathbb{Q}_2)/\ker(x-T) \quad \textit{and} \quad J(\mathbb{Q}_{3701})/\ker(x-T)$$

are generated by

$$[(2,\sqrt{881})-\infty^-] \in J(\mathbb{Q}_2) \quad \textit{and} \quad [(-4,\sqrt{185})-\infty^-] \in J(\mathbb{Q}_{3701}),$$

respectively.

Proof. For $p=2$, we have $881 \equiv 1 \pmod 8$, so Hensel's Lemma implies that $(2,\sqrt{881})$ is in $\mathcal{C}(\mathbb{Q}_2)$. (Fix a square root.) Thus it will suffice to show that $2-T \notin L_2^{*2}\mathbb{Q}_2^*$. Let $g(x)$ be the characteristic polynomial of $2-T$. PARI tells us that there is only one prime above 2 in the number field generated by a root of $g(x^2)$, and it follows that $L_2(\sqrt{2-T})$ is a field of degree 12, so $2-T \notin L_2^{*2}$. Similarly, for each $r \in \{\pm1,\pm2,\pm3,\pm6\}$, a set of representatives for $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, we can check that $r(2-T) \notin L_2^{*2}$, and it follows that $2-T \notin L_2^*/L_2^{*2}\mathbb{Q}_2^*$. (It should be remarked here, that it took PARI a few hours to do these calculations with degree 12 number fields. We speculate that this is because the PARI command `initalg`, which must precede the command `primedec` that computes the decomposition of primes, computes many other pieces of information that are irrelevant for our purposes. Of course, there are other methods that could be used to test if an element x of L_2^* is a square; for instance, if x is a unit, this is determined by $x \bmod 8$.)

For $p=3701$, we first verify that the Legendre symbol $\left(\frac{185}{3701}\right)$ is 1, so Hensel's Lemma implies that $(-4,\sqrt{185}) \in \mathcal{C}(\mathbb{Q}_{3701})$. To complete the proof, we must check that $-4-T \notin L_{3701}^{*2}\mathbb{Q}_{3701}^*$. This time we can avoid the PARI computations with degree 12 number fields by exploiting the decomposition of L_{3701} into fields. As before, it suffices to prove that $r(-4-T) \notin L_{3701}^{*2}$ for $r \in \{1,2,3701,2\cdot 3701\}$, which is a set of representatives for $\mathbb{Q}_{3701}^*/\mathbb{Q}_{3701}^{*2}$, since $\left(\frac{2}{3701}\right) = -1$. Now $-4-T$ maps in $\mathbb{Q}_{3701}$ to something that is $-4-1371 = -1375$ modulo 3701, and $\left(\frac{-1375}{3701}\right) = 1$, so by Hensel's Lemma, $-4-T$ maps to a square in $\mathbb{Q}_{3701}$, and $r(-4-T)$ can map to a square in $\mathbb{Q}_{3701}$ only if $r=1$. On the other hand $-4-T$ maps in E (the ramified field component of L_{3701}) to something that is $-4-1727=-1731$ modulo the maximal ideal, and $\left(\frac{-1731}{3701}\right) = -1$, so $-4-T$ does not map to a square in E, and hence $-4-T \notin L_{3701}^{*2}$. Thus $-4-T \notin L_{3701}^{*2}\mathbb{Q}_{3701}^*$, and we are done. ∎

Lemma 5. *$J(\mathbb{Q})/\ker(x-T)$ is trivial.*

Proof. By Proposition 3, diagram (6) and Lemma 4, $J(\mathbb{Q})/\ker(x-T)$ maps into the subgroup H' of H that maps in $L_2^*/L_2^{*2}\mathbb{Q}_2^*$ into the group generated by $2-T$, in $L_{3701}^*/L_{3701}^{*2}\mathbb{Q}_{3701}^*$ into the group generated by $-4-T$, and in $L_\infty^*/L_\infty^{*2}\mathbb{R}^*$ to the identity. So it will suffice to show that H' is trivial.

First of all, the β_2-adic valuation $E \to \mathbb{Z}$ induces a map $v : L_{3701}^*/L_{3701}^{*2}\mathbb{Q}_{3701}^* \to \mathbb{Z}/2\mathbb{Z}$, since the ramification index of E over $\mathbb{Q}_{3701}$ is 2. By Section 6, $-4-T$ maps in E to something that is -1731 modulo the maximal ideal, so v is trivial on the image of $-4-T$. But v maps the two generators u_1 and $u_3\beta_1\beta_2$ of H to 0 and 1, respectively, so H' is contained in the image of $\{1, u_1\}$.

The same method used in the proof of Lemma 4 to show that $2-T$ was nontrivial in $L_2^*/L_2^{*2}\mathbb{Q}_2^*$ shows that u_1 and $u_1(2-T)$ are nontrivial there, so u_1 does not map into the subgroup of $L_2^*/L_2^{*2}\mathbb{Q}_2^*$ generated by $2-T$. Thus H' is trivial. (The information from the prime ∞ was not used, but in fact it would not have helped either, since the kernel of the norm from $L_\infty^*/L_\infty^{*2}\mathbb{R}^*$ to $\mathbb{R}^*/\mathbb{R}^{*2}$ is trivial.) □

Theorem 3. *$J(\mathbb{Q}) \cong \mathbb{Z}$ as an additive group.*

Proof. By Proposition 5, $2J(\mathbb{Q})$ has index 2 in $\ker(x-T)$, so by Lemma 5, we have $\#J(\mathbb{Q})/2J(\mathbb{Q}) = 2$. By Proposition 6, $J(\mathbb{Q}) \cong \mathbb{Z}^r$ for some $r \geq 1$. Then $J(\mathbb{Q})/2J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$, so by the above, $r = 1$. □

8. Applying Chabauty's method

We recall the following consequence of Chabauty's result [5], which gives a way of deducing information about the $\mathbb{Q}$-rational points on a curve from its Jacobian.

Proposition 8. *Let C be a curve of genus g defined over $\mathbb{Q}$, whose Jacobian has Mordell-Weil rank $\leq g-1$. Then C has only finitely many $\mathbb{Q}$-rational points.*

This is a weaker result than Faltings' Theorem; however, when applicable, Chabauty's method can often be used to give good bounds for the number of points on a curve. Recent work in Coleman [6] (see also [21, 22]) has improved Chabauty's technique; however, the bounds obtained seem only rarely to resolve $\mathcal{C}(\mathbb{Q})$ completely. For our curve $\mathcal{C}$, the best bound that can be obtained from the results in [6] is that $\#\mathcal{C}(\mathbb{Q}) \leq 9$. We shall adopt a more flexible approach that will allow us to sharpen this bound to 6, as required. It is hoped that a generalisation of the following ideas to any curve of genus 2 over a number field will at some stage be presented in [11], but we make no direct use of this, and present a largely self contained account tailored to the needs of our specific example. We shall, however, need to refer to the equations in [7, 8] relating to the Jacobian and formal group. We shall first establish a few easily computed facts about $J(\mathbb{Q})$. Let $D = [\infty^+ - \infty^-] \in J(\mathbb{Q})$.

Lemma 6. *We have $J(\mathbb{Q}) = \langle E\rangle$, for some $E \in J(\mathbb{Q})$ of infinite order, and $D = k\cdot E$ with $3 \nmid k$.*

n	$n \cdot D$	$n \cdot \widetilde{D}$
0	$\mathcal{O}$	$\mathcal{O}$
1	$[\infty^+ + \infty^+]$	$[\infty^+ + \infty^+]$
2	$[(0,1) + (-3,1)]$	$[(0,1) + (0,1)]$
3	$[(0,-1) + \infty^-]$	$[(0,-1) + \infty^-]$
4	$[(0,-1) + \infty^+]$	$[(0,-1) + \infty^+]$
5	$[(-3,1) + \infty^-]$	$[(0,1) + \infty^-]$
6	$[(-3,1) + \infty^+]$	$[(0,1) + \infty^+]$
7	$[(0,-1) + (0,-1)]$	$[(0,-1) + (0,-1)]$
8	$[P + \overline{P}]$	$[\infty^- + \infty^-]$
9	$[(0,-1) + (-3,1)]$	$\mathcal{O}$
10	$[Q + \overline{Q}]$	$[\infty^+ + \infty^+]$
11	$[(-3,1) + (-3,1)]$	$[(0,1) + (0,1)]$

TABLE 5. The first 11 multiples of D and $\widetilde{D}$.

Proof. By Theorem 3, we can pick a generator E for $J(\mathbb{Q}) \cong \mathbb{Z}$. To complete the proof, we must show that $D \notin 3J(\mathbb{Q})$. Since $J(\mathbb{F}_3)$ is a cyclic group of size 9 generated by $\widetilde{D}$, the reduction of D mod 3, we find that $\widetilde{D} \notin 3J(\mathbb{F}_3)$, from which it follows that $D \notin 3J(\mathbb{Q})$, as required. □

It would be nice to have the theory of heights sufficiently well developed to determine whether $k = \pm 1$, which would give $J(\mathbb{Q}) = \langle D \rangle$. However, the method in [10] would require significant enhancements before it could realistically be applied to $\mathcal{C}$. In fact, all of our local arguments will be 3-adic and so the fact that $D \notin 3J(\mathbb{Q})$ will turn out to be sufficient for our purposes.

Table 5 lists the first 11 multiples of D, which will be relevant to our later computations. The last column gives the corresponding multiples of $\widetilde{D}$, the reduction of D mod 3 to $J(\mathbb{F}_3)$. For simplicity, we represent multiples of D in $\mathrm{Pic}^2(\mathcal{C})$, where $\mathrm{Pic}^0(\mathcal{C}) \cong \mathrm{Pic}^2(\mathcal{C})$ by $[V] \mapsto [V + \infty^+ + \infty^-]$. In abuse of notation we will write $D = [\infty^+ - \infty^-]$ in $\mathrm{Pic}^0(\mathcal{C})$ and $D = [\infty^+ + \infty^+]$ in $\mathrm{Pic}^2(\mathcal{C})$. In the table, $P = (-2 + \frac{1}{3}\sqrt{33}, -\frac{17}{3} + \frac{10}{9}\sqrt{33})$ and $Q = (-\frac{1}{2} + \frac{1}{6}\sqrt{-87}, \frac{22}{3} + \frac{5}{9}\sqrt{-87})$, and $\overline{P}$ and $\overline{Q}$ are their algebraic conjugates.

The multiples $\ell \cdot D$, for $\ell = -1, \ldots, -11$, can be deduced from the above by using the rule that $-[(x_1, y_1) + (x_2, y_2)] = [(x_1, -y_1) + (x_2, -y_2)]$. The divisor $9 \cdot D$, which is in the kernel of reduction mod 3, will play a special role, and so we denote:

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

The following lemma is immediate from the fact that the k of Lemma 6 is coprime to 3.

Lemma 7. *Let E be as in Lemma 6, and let $E' = 9 \cdot E$. Then any member of $J(\mathbb{Q})$ can be written uniquely as $\ell \cdot D + m \cdot E'$, for some $\ell, m \in \mathbb{Z}$, with $-4 \le \ell \le 4$.*

If we now let:

$$\mathcal{M}_3 = \text{ the kernel of the reduction map from } J(\mathbb{Q}_3) \text{ to } J(\mathbb{F}_3),$$

then $\mathcal{M}_3$ contains no k-torsion, since $3 \nmid k$, and there is a well defined map $1/k$ on $\mathcal{M}_3$ that takes any $D_0 \in \mathcal{M}_3$ to the unique $E_0 \in \mathcal{M}_3$ such that $D_0 = k \cdot E_0$. We can therefore legitimately say that any divisor in $J(\mathbb{Q})$ can be written in the form:

$$\ell \cdot D + n \cdot D', \text{ with } -4 \le \ell \le 4,\ n = m/k,\ 3 \nmid k, \tag{7}$$

where it is to be understood that $1/k$ refers to the above 3-adic map on $\mathcal{M}_3$. Here, n need not be a rational integer, but must still be a 3-adic integer, which will be sufficient for our purposes.

Our next observation is that $\mathcal{C}(\mathbb{Q})$ is in 1-1 correspondence with the members of $J(\mathbb{Q})$ that have the special form: $[P+P]$. From Table 5, we see that all of the known $\mathbb{Q}$-rational points correspond to: $\pm D$, $\pm 7 \cdot D$ and $\pm 11 \cdot D$. Suppose now that we have a divisor $D_0 \in J(\mathbb{Q})$ that is of the special form $[P+P]$; we can write $D_0 = \ell \cdot D + n \cdot D'$ as in equation (7). If D_0 were in $\mathcal{M}_3$ (that is, $\ell = 0$), then $\widetilde{P}$ would have to be of the form $(x, 0)$, which is impossible since the sextic $f(x)$ has no roots in $\mathbb{F}_3$. Otherwise, the reduction of D_0, which is also the reduction of ℓD, must be of the form $[\widetilde{P} + \widetilde{P}]$, giving that $\pm 1, \pm 2$ are the only possibilities for ℓ. Suppose we can show that $D + n \cdot D'$ is of the form $[P+P]$ only when $n = 0$ and that $2 \cdot D + n \cdot D'$ is of that form only when $n = \pm 1$. Using the fact that $-[(x,y)+(x,y)] = [(x,-y)+(x,-y)]$, it would then follow that $-D + n \cdot D'$ is of that form only when $n = 0$ and that $-2 \cdot D + n \cdot D'$ is of that form only when $n = \pm 1$. This would show that $\mathcal{C}(\mathbb{Q})$ consists only of the 6 known points. We summarise the above in the following lemma.

Lemma 8. *Let $\mathcal{M}_3$ be the kernel of the reduction map from $J(\mathbb{Q}_3)$ to $J(\mathbb{F}_3)$. Let $D_1 = D = [\infty^+ + \infty^+]$ and $D_2 = 2 \cdot D = [(0,1) + (-3,1)]$. Then $D' = 9 \cdot D = [(0,-1) + (-3,1)] \in \mathcal{M}_3$. Suppose that, for $n = m/k$, $m, k \in \mathbb{Z}, 3 \nmid k$, we have $D_1 + n \cdot D'$ of the form $[P+P]$ only when $n = 0$, and $D_2 + n \cdot D'$ is of that form only when $n = \pm 1$. Then $\#\mathcal{C}(\mathbb{Q}) = 6$.*

For each D_i, $i = 1, 2$, our strategy will be to derive, to a sufficient degree of 3-adic accuracy, a power series $\theta_i(n) \in \mathbb{Z}_3[[n]]$ that must be satisfied by n whenever $D_i + n \cdot D'$ is of the form $[P+P]$. We shall show the stronger result that the known solutions to $\theta_i(N)$ give all of the solutions $n \in \mathbb{Z}_3$. The following standard theorem of Strassman is proved in [3, p.62].

Theorem 4. *Let $\theta(X) = c_0 + c_1 X + c_2 X^2 + \ldots \in \mathbb{Z}_p[[X]]$ satisfy $c_n \to 0$ in $\mathbb{Q}_p$. Define r uniquely by: $|c_r|_p \ge |c_i|_p$ for all $i \ge 0$, and $|c_r|_p > |c_i|_p$ for all $i > r$. Then there are at most r values of $x \in \mathbb{Z}_p$ such that $\theta(x) = 0$.*

In order to derive the power series $\theta_1(n)$ and $\theta_2(n)$, we shall make use of the formal group. As remarked in Section 3, $\mathcal{C}$ cannot be put in the simpler form $y^2 =$ (*quintic in* x), so instead of using the development of the formal group in [12], we must use the general $y^2 =$ (*sextic in* x) development as in [7, 8]. The derivation of the equations that we shall use for both the formal group law and the global group law are described in [8]. These equations for a general curve of genus 2, are available at: `ftp.liv.ac.uk` in the directory `~ftp/pub/genus2` by anonymous ftp. First note that for any curve of genus 2

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \quad f_i \in \mathbb{Z}, \tag{8}$$

the following functions s_1, s_2 of a point $D_0 = [(x_1, y_1) + (x_2, y_2)] \in J(\mathbb{Q})$ can be used as a pair of local parameters at $\mathcal{O}$:

$$s_1 = (G_1(x_1, x_2)y_1 - G_1(x_2, x_1)y_2)(x_1 - x_2)/(F_0(x_1, x_2) - 2y_1y_2)^2, \tag{9}$$

$$s_2 = (G_0(x_1, x_2)y_1 - G_0(x_2, x_1)y_2)(x_1 - x_2)/(F_0(x_1, x_2) - 2y_1y_2)^2, \tag{10}$$

where

$$\begin{aligned} F_0(x_1, x_2) = {} & 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1 + x_2) \\ & +2f_4(x_1x_2)^2 + f_5(x_1x_2)^2(x_1 + x_2) + 2f_6(x_1x_2)^3, \\ G_0(x_1, x_2) = {} & 4f_0 + f_1(x_1 + 3x_2) + f_2(2x_1x_2 + 2x_2^2) + f_3(3x_1x_2^2 + x_2^3) \\ & +4f_4(x_1x_2^3) + f_5(x_1^2x_2^3 + 3x_1x_2^4) + f_6(2x_1^2x_2^4 + 2x_1x_2^5), \\ G_1(x_1, x_2) = {} & f_0(2x_1 + 2x_2) + f_1(3x_1x_2 + x_2^2) + 4f_2(x_1x_2^2) + f_3(x_1^2x_2^2 + 3x_1x_2^3) \\ & +f_4(2x_1^2x_2^3 + 2x_1x_2^4) + f_5(3x_1^2x_2^4 + x_1x_2^5) + 4f_6(x_1^2x_2^5). \end{aligned}$$

The following lemma summarises the information we need from [7, 8] and introduces the standard formal exponential and logarithm maps on the formal group.

Theorem 5. *Let C be as in (8). There is a formal group law with respect to the local parameters of equation (9), given by $\mathcal{F} = \begin{pmatrix} \mathcal{F}_1 \\ \mathcal{F}_2 \end{pmatrix}$ where $\mathcal{F}_1, \mathcal{F}_2$ are power series in s_1, s_2, t_1, t_2 defined over $\mathbb{Z}$, which contain terms only of odd degree. Define the formal exponential of $\mathcal{F}$ as $E = \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}$, where E_1, E_2 are power series in $\mathbf{s}$ over $\mathbb{Q}$, by: $E(\mathbf{s}) = \mathbf{s} +$ terms of higher degree, and $E(\mathbf{s} + \mathbf{t}) = \mathcal{F}(E(\mathbf{s}), E(\mathbf{t}))$. Similarly define the formal logarithm of $\mathcal{F}$ as $L = \begin{pmatrix} L_1 \\ L_2 \end{pmatrix}$ where L_1, L_2 are power series in $\mathbf{s}$ over $\mathbb{Q}$, by: $L(E(\mathbf{s})) = \mathbf{s}$, or equivalently: $L(\mathbf{s}) = \mathbf{s} +$ terms of higher degree, and $L(\mathcal{F}(\mathbf{s}, \mathbf{t})) = L(\mathbf{s}) + L(\mathbf{t})$. Then each of E_1,E_2,L_1,L_2 can be written in the form: $\sum(a_{ij}/i!j!)s_1^i s_2^j$, where $a_{ij} \in \mathbb{Z}$ and $a_{ij} = 0$ when $i + j$ is even. Let p be a prime of good reduction, and let A, B, C be in $\mathcal{M}_p$, the kernel of reduction from $J(\mathbb{Q}_p)$ to $J(\mathbb{F}_p)$, with $C = A + B$. Suppose now that $\mathbf{s} = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$ are the local parameters corresponding* *to A, and similarly* $\mathbf{t}$, $\mathbf{u}$ *those for B, C respectively. Then each $s_i, t_i, u_i \in p\mathbb{Z}_p$ and $\mathcal{F}(\mathbf{s},\mathbf{t})$ converges in $p\mathbb{Z}_p$ with $\mathbf{u} = \mathcal{F}(\mathbf{s},\mathbf{t})$.*

The power series $\mathcal{F}$ gives a description of the group law on $\mathcal{M}_p$. It is described in [7, 8] how to compute terms of the formal group up to terms of arbitrary degree. We require here the formal group up to terms of degree 3 in $\mathbf{s}$:

$$\mathcal{F}_1 = s_1 + t_1 + 2f_4 s_1^2 t_1 + 2f_4 s_1 t_1^2 - f_1 s_2^2 t_2 - f_1 s_2 t_2^2 + (\text{degree } \geq 5)$$
$$\mathcal{F}_2 = s_2 + t_2 + 2f_2 s_2^2 t_2 + 2f_2 s_2 t_2^2 - f_5 s_1^2 t_1 - f_5 s_1 t_1^2 + (\text{degree } \geq 5)$$

For any A in $\mathcal{M}_p$, with local parameter $\mathbf{s}$, note also that the power series $E(\mathbf{s})$ and $L(\mathbf{s})$ converge in $p\mathbb{Z}_p$ also, since $|s_1|_p, |s_2|_p \leq p^{-1}$ and so $|s_1^i s_2^j / i!j!|_p$ converges to 0 as $i+j \to \infty$. Once terms of the formal group have been computed, the terms of E and L may be computed inductively from their definitions. We shall again only require terms up to degree 3 in $\mathbf{s}$:

$$L_1(\mathbf{s}) = s_1 + \tfrac{1}{3}(-2f_4 s_1^3 + f_1 s_2^3) + \ldots \qquad E_1(\mathbf{s}) = s_1 + \tfrac{1}{3}(2f_4 s_1^3 - f_1 s_2^3) + \ldots$$
$$L_2(\mathbf{s}) = s_2 + \tfrac{1}{3}(-2f_2 s_2^3 + f_5 s_1^3) + \ldots \qquad E_2(\mathbf{s}) = s_2 + \tfrac{1}{3}(2f_2 s_2^3 - f_5 s_1^3) + \ldots$$

Let us now return to our specific curve $\mathcal{C}$ of equation (3). The local parameters of $D' = [(0,-1) + (-3,1)] \in \mathcal{M}_3$ are determined by substituting $x_1 = 0, y_1 = -1, x_2 = -3, y_2 = 1$ into (9), giving: $s_1 = -9/14$ and $s_2 = 426/49$, both of which have 3-adic valuation less than or equal to 3^{-1}. It is immediate that L_1,L_2 evaluated at $s_1 = -9/14$, $s_2 = 426/49$, are both 3-adic integers, and that (even after taking denominators into account) the terms up to degree 3 determine L_1,L_2 mod 3^4. This gives: $L_1 \equiv 36 \pmod{3^4}$ and $L_2 \equiv 3 \pmod{3^4}$. From the properties of E and L we see that $E(n \cdot L(\mathbf{s}))$ gives the local parameters t_1, t_2 for $T = n \cdot D' \in \mathcal{M}_3$, where n is as in (7), and so is in $\mathbb{Z}_3$. This expresses each of t_1, t_2 as members of $\mathbb{Z}_3[[n]]$, given $\pmod{3^4}$ by:

$$t_1 \equiv 36n + 27n^3 \text{ and } t_2 \equiv 3n + 9n^3 \pmod{3^4}. \tag{11}$$

Since any member of $\mathcal{M}_3$ is uniquely determined by its local parameters, this describes $T = n \cdot D'$ as a power series in n. We now wish to describe $D_1 + T$ and D_2+T, where D_1,D_2 are as specified in Lemma 8. Applying the standard global group law to the sum $[(x_1, y_1) + (x_2, y_2)] = D_1 + T$ gives (as described in [8]) expressions for $k_1, k_2, k_3 \in \mathbb{Z}[[t_1, t_2]]$ such that the triple (k_1, k_2, k_3) is the same projectively as $(1, x_1 + x_2, x_1 x_2)$. The terms up to degree 3 in $\mathbf{t}$ are:

$$k_1 = -12t_2 - 12t_1^2 + 8t_1t_2 + 36t_2^2 + 8t_1^3 - 72t_1^2t_2 - 48t_1t_2^2 - 8t_2^3 + \cdots$$
$$k_2 = 12t_1 + 48t_2 - 8t_1^2 - 104t_1t_2 - 132t_2^2 + 72t_1^3 + 648t_1^2t_2 + 408t_1t_2^2 + 104t_2^3 + \cdots$$
$$k_3 = -6 + 4t_1 - 72t_1^2 - 24t_1t_2 - 4t_2^2 - 24t_1^3 - 104t_1^2t_2 - 104t_1t_2^2 - 24t_2^3 + \cdots$$

On substituting (11) into these expressions gives each of k_1, k_2, k_3 as members of $\mathbb{Z}_3[[n]]$. Now note that if a divisor $[(x_1, y_1) + (x_2, y_2)]$ is of the form $[P + P]$ then

$\theta_1(n) = k_2^2 - 4k_1k_3 = 0$. This gives:

$$\theta_1(n) \in \mathbb{Z}_3[[n]], \text{ with } \theta_1(n) \equiv 27n \pmod{3^4},$$

where $\theta_1(n) = 0$ if $D_1 + n \cdot D'$ is of the form $[P + P]$.

Repeating the same process for D_2 first gives:

$$\begin{aligned}
k_1 &= -2 - 12t_1 - 40t_2 - 16t_1^2 + 64t_1t_2 + 100t_2^2 - 64t_1^3 - 472t_1^2t_2 - 64t_1t_2^2 - 64t_2^3 + \dots \\
k_2 &= 6 + 36t_1 + 116t_2 + 52t_1^2 - 224t_1t_2 - 392t_2^2 + 208t_1^3 + 1408t_1^2t_2 + 72t_1t_2^2 + 160t_2^3 + \dots \\
k_3 &= 4t_1 + 12t_2 + 28t_1^2 + 176t_1t_2 + 272t_2^2 + 32t_1^3 + 208t_1^2t_2 + 104t_1t_2^2 + 16t_2^3 + \dots
\end{aligned}$$

which then gives:

$$\theta_2(n) \in \mathbb{Z}_3[[n]], \text{ with } \theta_2(n) \equiv 36 + 27n + 18n^2 + 54n^3 + 27n^4 \pmod{3^4},$$

where $\theta_2(n) = 0$ if $D_2 + n \cdot D'$ is of the form $[P + P]$. We are now in a position to prove the desired result.

Theorem 6. *The curve $\mathcal{C}$ of equation (3) has only the six $\mathbb{Q}$-rational points $(0, 1)$, $(0, -1)$, $(-3, 1)$, $(-3, -1)$, ∞^+, and ∞^- listed in Table 2.*

Proof. The coefficient of n in $\theta_1(n) \in \mathbb{Z}_3[[n]]$ has 3-adic valuation strictly larger than all of the other coefficients, and so by Strassman's Theorem (Theorem 4) there is at most 1 solution, which is the known solution: $n = 0$. For $\theta_2(n)$, we further reduce mod 3^3, giving: $\theta_2(n) \equiv 9 + 18n^2$. By Strassman's Theorem, there are at most 2 solutions, which must be the 2 known solutions: $n = -1, -2$. The result now follows from Lemma 8. ∎

9. Non-modularity of $C_0(5)$ and $C_1(5)$

Recall that $C_1(4)$ turned out to be isomorphic over $\mathbb{Q}$ to the modular curve $X_1(16)$. Morton [26] asked whether $C_1(N)$ could be parameterized by modular functions also for $N > 4$. If $C_0(5)$ or $C_1(5)$ were isomorphic over $\mathbb{C}$ to $X_1(N)$ or $X_0(N)$, then N could not be a multiple of 3701, because by [16, Corollary 9.11] the genus of $X_0(3701)$ already is $(3701-5)/12 = 308$, whereas by Table 1, $C_0(5)$ and $C_1(5)$ have genus 2 and 14, respectively. Hence $C_0(5)$ or $C_1(5)$ would have potential good reduction at 3701. Using Lange's theorem [18] that potential good reduction of a geometrically connected smooth projective curve is inherited by any other such curve it surjects onto (or the more general result mentioned in the Appendix by Matignon and Youssefi to [39] that the same is true for good reduction), we find that in either case, $C_0(5)$ would have potential good reduction at 3701. But it can be shown that this contradicts the fact that the exponent of 3701 in the discriminant of $f(x)$ is 1, so neither $C_0(5)$ nor $C_1(5)$ is isomorphic over $\mathbb{C}$ to $X_0(N)$ or $X_1(N)$ for any $N \geq 1$.

We have been slightly sketchy in the previous argument, because below we will provide a complete proof for the stronger result that there is no surjective morphism from $X_1(N)$ to $C_0(5)$ or $C_1(5)$ for any $N \geq 1$, even over $\mathbb{C}$. As before, let J denote the Jacobian of $\mathcal{C} = C_0(5)$. Let $\operatorname{End} J$ denote the ring of endomorphisms of J defined over $\mathbb{C}$.

Proposition 9. *J is absolutely simple, and* $\operatorname{End} J \cong \mathbb{Z}$.

Proof. We will model our argument on that used in [33, Appendix A]. Suppose p is a prime of good reduction for J. Then reduction modulo p embeds $\operatorname{End} J$ in $\operatorname{End}_{\overline{\mathbb{F}}_p} J$, the endomorphisms defined over $\overline{\mathbb{F}}_p$ of the reduced abelian variety over $\mathbb{F}_p$ (which we will also denote J). By [24, Lemma 3], the characteristic polynomial of the Frobenius endomorphism π_p on J is

$$X^4 - tX^3 + sX^2 - ptX + p^2, \tag{12}$$

where

$$t = p + 1 - \#\mathcal{C}(\mathbb{F}_p), \qquad s = \frac{1}{2}\left[\#\mathcal{C}(\mathbb{F}_p)^2 + \#\mathcal{C}(\mathbb{F}_{p^2})\right] + p - (p+1)\#\mathcal{C}(\mathbb{F}_p).$$

Moreover, it follows from [38, Theorem 8] that if the characteristic polynomial of π_p^n is irreducible over $\mathbb{Q}$ for all $n \geq 1$, then $(\operatorname{End}_{\overline{\mathbb{F}}_p} J) \otimes \mathbb{Q} = \mathbb{Q}(\pi_p)$ is a number field of degree 4.

For $p = 3$, (12) becomes $X^4 - X^2 + 9$, so the characteristic polynomial of π_3^2 is $(X^2 - X + 9)^2$. Hence we move on to $p = 5$, for which (12) is $P(x) = X^4 + X^3 + 9X^2 + 5X + 25$. This is irreducible over $\mathbb{Q}$, so $\mathbb{Q}(\pi_5) \cong \mathbb{Q}[X]/(P(x))$ is a number field of degree 4. We wish to show that no positive power of π_5 lies in a proper subfield. PARI tells us that the Galois group of $P(X)$ is dihedral of order 8, so $\mathbb{Q}(\pi_5)$ has an automorphism σ of order 2, even though it is not Galois over $\mathbb{Q}$. By Galois theory, the (quadratic) fixed field F of σ is the only nontrivial subfield of $\mathbb{Q}(\pi_5)$. We find that $\pi_5 + \sigma(\pi_5)$ is a root of $x^2 + x = 1$, so $F = \mathbb{Q}(\sqrt{5})$. If $\pi_5^n \in F$, then $\sigma(\pi_5)/\pi_5$ would be an n-th root of unity. But PARI shows that the only roots of unity in $\mathbb{Q}(\pi_5)$ are 1 and -1, and that $\sigma(\pi_5)/\pi_5$ is neither of these. Thus we now know that $(\operatorname{End}_{\overline{\mathbb{F}}_5} J) \otimes \mathbb{Q} \cong \mathbb{Q}[X]/(P(X))$, which already is enough to imply that J is absolutely simple.

The characteristic polynomial of π_7 is $R(X) = X^4 + 2X^3 + 4X^2 + 14X + 49$, and exactly the same argument as in the previous paragraph shows $(\operatorname{End}_{\overline{\mathbb{F}}_7} J) \otimes \mathbb{Q} \cong \mathbb{Q}[X]/(R(X))$. Now $(\operatorname{End} J) \otimes \mathbb{Q}$ embeds into both number fields $\mathbb{Q}[X]/(P(X))$ and $\mathbb{Q}[X]/(R(X))$, but PARI tells us that the only nontrivial subfield $F = \mathbb{Q}(\sqrt{5})$ of $\mathbb{Q}[X]/(P(X))$ is not a subfield of $\mathbb{Q}[X]/(R(X))$, so $(\operatorname{End} J) \otimes \mathbb{Q} = \mathbb{Q}$. Thus $\operatorname{End} J = \mathbb{Z}$. ∎

Let $J_1(N)$ denote the Jacobian of $X_1(N)$. We will write $\operatorname{End}_{\mathbb{Q}} A$ for the ring of endomorphisms defined over $\mathbb{Q}$ of an abelian variety A over $\mathbb{Q}$.

Proposition 10. *Let B be an absolutely simple abelian variety over $\mathbb{C}$ which is a quotient of $J_1(N)$ over $\mathbb{C}$. Then the rank of* $\operatorname{End} B$ *over* $\mathbb{Z}$ *is* $\dim B$ *or* $2 \dim B$.

Proof. Let A be a simple abelian variety over $\mathbb{Q}$ which is a quotient of $J_1(N)$ over $\mathbb{Q}$, and which contains B in its decomposition into absolutely simple abelian varieties over $\mathbb{C}$ up to isogeny. If B is an elliptic curve with complex multiplication, the result is trivial, so assume this does not hold. Then by [34, Theorem 1], $(\operatorname{End} A) \otimes \mathbb{Q}$ is a matrix algebra $D = \mathbb{M}_n(H)$ over a division algebra H finite dimensional over its center F, and $E \stackrel{\text{def}}{=} (\operatorname{End}_{\mathbb{Q}} A) \otimes \mathbb{Q}$ is a maximal subfield of D. Moreover $[E : \mathbb{Q}] = \dim A$, and $[H : F] = r^2$ with $r = 1$ or 2. Let $f = [F : \mathbb{Q}]$. Since E is a maximal subfield of D, $[E : F] = \sqrt{[D : F]} = \sqrt{n^2 r^2} = nr$, so

$$\dim B = (\dim A)/n = [E : \mathbb{Q}]/n = [E : F]f/n = rf.$$

Finally,

$$\operatorname{rank}(\operatorname{End} B) = [(\operatorname{End} B) \otimes \mathbb{Q} : \mathbb{Q}] = [H : \mathbb{Q}] = r^2 f$$

so $\operatorname{rank}(\operatorname{End} B) = r \dim B$, and we are done. □

Theorem 7. *Let $N \geq 1$. There is no nonzero morphism of abelian varieties over $\mathbb{C}$ from $J_1(N)$ to J. Thus there is no surjective morphism of curves from $X_1(N)$ to $C_0(5)$ or $C_1(5)$.*

Proof. By Proposition 10, any 2-dimensional quotient of $J_1(N)$ must have an endomorphism ring larger than $\mathbb{Z}$. Thus the first statement follows from Proposition 9. Since $C_1(5)$ maps to $C_0(5)$, and since surjective maps on curves induce surjective maps on their Jacobians, the final statement follows from the first. □

For the modular curves $X_0(N)$ and $X_1(N)$, the Manin-Drinfeld theorem states the divisor class of the difference of two cusps is a torsion element in the Jacobian. It is natural to ask whether the same is true for $C_0(N)$ and $C_1(N)$, with cusps replaced by points with $c = \infty$. (All of these points are rational, as follows from the "q-expansions" in [26].) For $N = 4$, the result holds, simply because $C_1(4)$ is isomorphic to $X_1(16)$ and the points with $c = \infty$ correspond to cusps. But the result fails for $N = 5$, even for the quotient $C_0(5)$, since the divisor class of the difference of two of its rational points at $c = \infty$ is a nonzero element of $J(\mathbb{Q})$, and hence is not torsion, by Proposition 6.

10. Rational points and cycles of period 6

We conclude the paper with a few remarks about the next unsolved case, $N = 6$. The curve $C_0(6)$ is of genus 4 (see Table 1) and is birational to the curve given by the equation $\tau_6(x, c) = 0$, where

$$\begin{aligned}\tau_6(x,c) = {} & (-384c - 592c^2 - 256c^3) + \left(448 + 416c - 304c^2 - 256c^3\right)x + \left(196 + 552c + 480c^2 + 256c^3\right)x^2 \\ & + \left(140 - 136c + 160c^2 + 256c^3\right)x^3 + \left(175 + 16c + 112c^2\right)x^4 + \left(49 + 16c + 144c^2\right)x^5 \\ & + (14 + 8c)\,x^6 + (2 + 24c)\,x^7 - x^8 + x^9.\end{aligned}$$

(This is taken from [26].) Recall that x is the trace of a 6-cycle for $g(z) = z^2 + c$.

(x, c)	Generator of 6-cycle	K	Conductor
$(0, 0)$	ζ_9	$\mathbb{Q}(\zeta_9)$	9
$(-1, -2)$	$\zeta_{13} + \zeta_{13}^{-1}$	$\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$	13
$(1, -2)$	$\zeta_{21} + \zeta_{21}^{-1}$	$\mathbb{Q}(\zeta_{21} + \zeta_{21}^{-1})$	21
$(-3, -4)$	$(\zeta_7^2 + \zeta_7^{-2}) + \frac{1+\sqrt{5}}{2}(\zeta_7 + \zeta_7^{-1})$	$\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{5})$	35
$(-7/2, -71/48)$	$-1 + \frac{\sqrt{33}}{12}$	$\mathbb{Q}(\sqrt{33})$	33

TABLE 6. The known affine rational points on $C_0(6)$.

For each rational number $x = r/s$ with $|r|, |s| \leq 100$, we checked the polynomial $\tau_6(x, c)$ in c for rational roots. We then did the same with x and c reversed. This let us find all affine rational points on $\tau_6(x, c) = 0$ having at least one coordinate with numerator and denominator bounded by 100 (in absolute value). These are listed in Table 6. Because each of these points in fact has a coordinate with numerator and denominator bounded by 7, it seems reasonable to expect that we have found all the affine rational points. (There are also 5 points at infinity on the nonsingular model, and these are all rational.)

Each affine point on $C_0(6)$ corresponds to a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable 6-cycle, whose elements generate abelian extensions of $\mathbb{Q}$ of degree dividing 6. Table 6 lists an element of this cycle for each known point (in terms of a primitive n-th root of unity ζ_n), and also gives the abelian extension K of $\mathbb{Q}$ it generates, together with its conductor. (It is straightforward to verify these using PARI.) In particular, note that none of the cycles are defined pointwise over $\mathbb{Q}$. Therefore, if we have truly found all affine rational points on $C_0(6)$, then there is no quadratic polynomial $g(z) \in \mathbb{Q}[z]$ with a periodic point of exact period 6.

Acknowledgements

We thank Greg Call for helping us trace the history of the problem mentioned in the first paragraph, Noam Elkies for a comment that let us check that $\mathcal{C}$ actually had good reduction at 2, Qing Liu for referring us to the theorems on good reduction of curves mentioned in Section 9, Patrick Morton for sharing his preprints with us, Michel Olivier for verifiying our number field computations unconditionally using a yet to be released version of PARI, Ken Ribet for suggesting to us that the implication $(\mathrm{End}\, J = \mathbb{Z}) \implies (J$ is not a modular quotient$)$ in Section 9 should follow easily from the results in [34], and Michael Zieve for introducing us to the problems considered in this paper.

References

[1] Bousch, T., Sur quelques problèmes de dynamique holomorphe, Thèse, Université de Paris-Sud, Centre d'Orsay, 1992.

[2] Call, G. and Silverman, J., Canonical heights on varieties with morphisms, *Compos. Math.* **89** (1993), 163–205.

[3] Cassels, J. W. S., *Local Fields*, London Mathematical Society Student Texts **3**, Cambridge Univ. Press, 1986.

[4] Cassels, J. W. S., The Mordell-Weil group of curves of genus 2., in: M. Artin, J. Tate (eds.), *Arithmetic and Geometry I*, Birkhäuser, Boston, (1983), 27–60.

[5] 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.

[6] Coleman, R. F., Effective Chabauty, *Duke Math. J.* **52** (1985), 765–780.

[7] Flynn, E. V., The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field., *Math. Proc. Camb. Phil. Soc.* **107** (1990), 425–441.

[8] Flynn, E. V., The group law on the Jacobian of a curve of genus 2., *J. Reine Angew. Math.* **439** (1993), 45–69.

[9] Flynn, E. V., Descent via isogeny in dimension 2, *Acta Arith.* **66** (1994), 23–43.

[10] Flynn, E. V., An explicit theory of heights in dimension 2., to appear in *Trans. Amer. Math. Soc.*

[11] Flynn, E. V., A flexible method for applying Chabauty's Theorem., in preparation, March 1995.

[12] Grant, D., Formal Groups in Genus 2, *J. Reine Angew. Math.* **411** (1990), 96–121.

[13] Gordon, D. and Grant, D., Computing the Mordell-Weil rank of Jacobians of curves of genus two, *Trans. Amer. Math. Soc.* **337** (1993), 807–824.

[14] Katz, N., Galois properties of torsion points on abelian varieties, *Invent. Math.* **62** (1981), 481–502.

[15] Kenku, M., On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class, *J. Number Th.* **15** (1982), 199–202.

[16] Knapp, A., *Elliptic Curves*, Princeton Univ. Press, 1992.

[17] Lang, S., *Abelian Varieties*, Interscience Publishers, Inc., New York, 1959.

[18] Lange, H., Kurven mit rationaler Abbildung, *J. reine angew. Math.* **295** (1977), 80–115.

[19] Levi, B., Saggio per una teoria aritmetica della forme cubiche ternarie, *Atti Accad. Reale Sci. Torino* **43** (1908), 99–120.

[20] Lewis, D., Invariant sets of morphisms on projective and affine number spaces, *Journal of Algebra* **20** (1972), 419–434.

[21] McCallum, W. G., On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve, *Invent. Math.* **93** (1988), 637–666.

[22] McCallum, W. G., The Arithmetic of Fermat Curves, *Math. Ann.* **294** (1992), 503–511.

[23] Merel, L., Existence d'une borne uniforme pour les nombres premiers de torsion des courbes elliptiques sur les corps de nombres, preprint, 1994.

[24] Merriman, J. and Smart, N., Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point, *Math. Proc. Camb. Phil. Soc.* **114** (1993), 203–214.

[25] Milne, J. S., Jacobian Varieties, in: Cornell, G., Silverman, J.H.(eds.), *Arithmetic geometry*, 167–212, Springer-Verlag, New York, 1986.

[26] Morton, P., Arithmetic properties of periodic points of quadratic maps, II, preprint, 1995.

[27] Morton, P., On certain algebraic curves related to polynomial maps, preprint, 1995.

[28] Morton, P. and Silverman, J., Rational periodic points of rational functions, *Internat. Math. Res. Notices*, 97–110.

[29] Morton, P. and Silverman, J., Periodic points, multiplicities and dynamical units, preprint, 1993.

[30] Narkiewicz, W., On polynomial transformations in several variables, *Acta Arith.* **11** (1965), 163–168.
[31] Northcott, D., Periodic points on an algebraic variety, *Annals of Math.* **51** (1950), 167–177.
[32] Poonen, B., Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture, preprint, 1995.
[33] Pyle, E., Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$, Ph. D. thesis, Univ. of Calif. at Berkeley, 1995.
[34] Ribet, K., Endomorphism algebras of abelian varieties attached to newforms of weight 2, in Seminar on Number Theory, Paris 1979–80, *Progr. Math.* **12** (1981), 263–276.
[35] Ribet, K., Abelian varieties over $\mathbb{Q}$ and modular forms, in *1992 Proceedings of KAIST Mathematics Workshop*, Korea Advanced Institute of Science and Technology, Taejon, 1992, 53–79.
[36] Schaefer, E.F., 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995) 219–232.
[37] 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.
[38] Waterhouse, W. C. and Milne, J. S., Abelian varieties over finite fields, in *1969 Number Theory Institute, Proc. Sympos. Pure Math.* **20**, American Mathematical Society, Providence, 1971, 53–64.
[39] Youssefi, T., Inégalité relative des genres, *Manuscripta Math.* **78** (1993), 111–128.

(Flynn) Department of Pure Mathematics, University of Liverpool, P. O. Box 147, Liverpool L69 3BX, England
E-mail address: `evflynn@liverpool.ac.uk`

(Poonen) Mathematical Sciences Research Institute, Berkeley, CA 94720-5070, USA
E-mail address: `poonen@msri.org`

Santa Clara University, Santa Clara, CA 95053, USA
E-mail address: `eschaefer@scuacc.scu.edu`