ACTA ARITHMETICA
LXXIV.3 (1996)

Arithmetic and geometry of the curve $y^3 + 1 = x^4$

by

Matthew J. Klassen and Edward F. Schaefer (Santa Clara, Calif.)

1. Introduction. In the literature on elliptic curves, the great wealth of explicit examples plays an important role in understanding many of the intricacies of the field of arithmetic geometry. For curves of higher genus, the catalog of explicit examples is only beginning to catch up with the general theory. In this paper we consider a number of themes, such as rational points, torsion points, and ramification points, and the interplay between their geometric and arithmetic significance.

Our subject (the curve in the title) is a quotient of the twelfth Fermat curve which we write as $U^{12} + W^{12} = V^{12}$ in projective coordinates over $\mathbb{Q}$. If we let $u = U/W$ and $v = V/W$ then we get the affine curve $u^{12} + 1 = v^{12}$ which admits a map of degree 12 to the curve $y^3 + 1 = x^4$, given by $(x, y) = (v^3, u^4)$. Let C be the projective completion of this curve. It is nonsingular and hence is a nonhyperelliptic curve of genus 3. From the homogeneous equation $Y^3Z + Z^4 = X^4$, we see that C has a single point on the line $Z = 0$ which we call $\infty = (0 : 1 : 0)$. Away from ∞ we let $x = X/Z$ and $y = Y/Z$ and denote $(X : Y : Z)$ by (x, y). Let J be the Jacobian variety of C, which we identify with $\mathrm{Pic}^0(C)$, and let ζ_n be a primitive nth root of unity. As a reference on Jacobian varieties see [Mi]. Our main results on J are Theorem 4.5 and Corollary 4.7:

$$(1) \qquad J(\mathbb{Q}(\zeta_{12})) \cong (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/3\mathbb{Z})^5 \quad \text{and} \quad J(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2.$$

From the first result we are able to determine completely the set of rational points on C over the field $\mathbb{Q}(\zeta_{12})$. In addition, this set turns out to be equal to two geometrically interesting finite sets of points on C. First, let W be the set of Weierstrass points on C. This is the same as the set of flexes, i.e. points where the tangent line meets the curve with order of contact 3 or 4. To define the second set, we let $f : C \to J$ be the Abel–Jacobi map which sends P to the divisor class $[P - \infty]$. Now let P be in T if $f(P)$ is a

1991 *Mathematics Subject Classification*: Primary 11G30; Secondary 11D25, 14H25, 14H45.

torsion point on J. Our main result on C is Corollary 4.6:

$$C(\mathbb{Q}(\zeta_{12})) = W = T. \tag{2}$$

Along the way to proving the above results, we give, in Section 2, a complete description of $\mathrm{Aut}(C)$, the automorphism group of C. This is used in Section 3, together with a result of Coleman, to prove the second equality in (2). The first equality in (2) follows directly from the second and the finiteness of $J(\mathbb{Q}(\zeta_{12}))$. We also use $\mathrm{Aut}(C)$ in Section 5 to find three maps of degree 2 from C to genus 1 curves which induce an isogeny $\psi : J \to A$ where A is the product of three CM elliptic curves. This isogeny is not used in our computation of Mordell–Weil groups of J. In fact, our approach is to perform a descent on J, using the endomorphism $\phi = 1 - \zeta_3$. We include the isogeny ψ for those readers who are interested in comparing our methods with those that rely more heavily on elliptic curves. If τ is an endomorphism of J, we denote its kernel by $J[\tau]$. The kernel of ψ turns out to be a subgroup of $J[2]$. For completeness, we give a description of $J[2]$, including a basis, using the bitangents of the curve C. The kernel of ϕ turns out to be a subgroup of $J[3]$. As a biproduct of the descent procedure, we also produce a basis for $J[3]$ in Lemma 4.2.

As a simple corollary of (2), we see that the only rational points on C are ∞, $(0, -1)$, $(1, 0)$, and $(-1, 0)$. We also deduce, from the finiteness of $J(\mathbb{Q})$, facts concerning points of C in other number fields. In particular, we show, in Section 4, that all solutions of the equation $y^3 + 1 = x^4$ in quadratic extensions of $\mathbb{Q}$ are in subextensions of $\mathbb{Q}(\zeta_{12})$, and we list them. Then we describe all solutions in fields of degree 3 over $\mathbb{Q}$. In particular, we list six such solutions, and show that all others arise from the intersection with C of a rational line through one of the four rational points on C.

Finally, the result (2) above was inspired by the paper of Coleman [C2, p. 205], where a similar result is stated for the Klein curve C' given by the equation $X^3Y + Y^3Z + Z^3X = 0$. Let $T(C')$ be the set of points on C' whose images under the Abel–Jacobi map, using some Weierstrass point as a basepoint, are torsion. In addition, let $W(C')$ be the set of Weierstrass points of C'. He shows that $C'(\mathbb{Q}(\zeta_7)) = W(C') = T(C')$. In this case the set has 24 elements. Also, it follows from work of Faddeev on the fourth Fermat curve, F_4, with equation $X^4 + Y^4 = Z^4$, that the set of 12 Weierstrass points $W(F_4)$ is the same as $F_4(\mathbb{Q}(\zeta_8))$. Let $T(F_4)$ be the set of points on F_4 whose images under the Abel–Jacobi map are torsion when using a Weierstrass point as a basepoint. In Section 6 we show that $F_4(\mathbb{Q}(\zeta_8)) = W(F_4) = T(F_4)$. We are not aware of any other quartics for which such a result is known. These three curves have several properties in common: each is a quotient of a Fermat curve, each has a rather large automorphism group and the Jacobian of each is isogenous to the product of three CM elliptic curves.

Acknowledgements. The first author had useful discussions on this material with Robert Coleman. The second author was supported during the preparation of this paper by a Paul Locatelli Junior Faculty Fellowship. The second author made much use of the program PARI/GP by C. Batut, D. Bernardi, H. Cohen, and M. Olivier.

2. Preliminary results and notation. Here we mention some basic facts on the geometry of C. We call P an *ordinary flex* if the tangent line meets the curve at P with order of contact 3, and a *hyperflex* if the order of contact is 4. For smooth plane quartics, it is well known that the ordinary flexes are the Weierstrass points of weight 1 and the hyperflexes are the Weierstrass points of weight 2 and no other weights are possible. For a curve of genus g, the sum of the weights over all points in W is $g^3 - g$; so in our case it is 24. In this paper we state our results in terms of Weierstrass points, partly due to the fact that this seems most common in the literature. However, throughout the text we often use the terminology of flexes since it is less cumbersome. It is a general fact (see for instance [L, p. 736]), that any automorphism of a curve of genus $g \geq 2$ preserves the set of Weierstrass points, and their respective weights.

In [V, p. 63], Vermeulen lists the possible automorphism groups of smooth plane quartic curves. The three largest groups each occur for exactly one curve, up to isomorphism over $\overline{\mathbb{Q}}$. These three curves are the Klein curve, with 168 automorphisms, the fourth Fermat curve, with 96 automorphisms, and C, with 48 automorphisms. Vermeulen lists C as $X_v^4 + Y_v^4 + 2\sqrt{-3}\,X_v^2Y_v^2 + Z_v^4 = 0$. The curves are isomorphic via

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ \frac{-1+\sqrt{3}}{\sqrt[4]{9-6\sqrt{3}}} & \frac{-1-\sqrt{3}}{\sqrt[4]{9+6\sqrt{3}}} & 0 \\ \frac{1}{\sqrt[4]{9-6\sqrt{3}}} & \frac{1}{\sqrt[4]{9+6\sqrt{3}}} & 0 \end{bmatrix} \begin{bmatrix} X_v \\ Y_v \\ Z_v \end{bmatrix}.$$

Any automorphism of a smooth plane quartic curve can be represented by $(X : Y : Z)^t \mapsto M(X : Y : Z)^t$ where $M \in \mathrm{PGL}(2)$ (see [H, p. 348]).

Proposition 2.1. *The automorphism group of C has* 48 *elements and they are represented by matrices of the following form in* $\mathrm{PGL}(2)$ *where we denote solutions of $x^3 = 1$ by α and α_i and solutions of $x^4 = 1$ by β:*

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha\beta & 0 \\ 0 & 0 & \beta \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} \frac{\sqrt{3}}{\beta} & 0 & 0 \\ 0 & -\alpha_1\alpha_2 & 2\alpha_2 \\ 0 & \alpha_1 & 1 \end{bmatrix}.$$

P r o o f. One verifies that each of these automorphisms of $\mathbb{P}^2$ preserves C and from [V], C has exactly 48 automorphisms. ∎

Let C^d be the product of d copies of C and let $C^{(d)} = S_d \backslash C^d$ be the dth symmetric product variety of C where S_d is the symmetric group on d objects. Since C has a rational point ∞, we can use this as a basepoint for the Abel–Jacobi map $f^{(d)} : C^{(d)} \to \mathrm{Pic}^0(C)$ given by $D \mapsto [D - d\infty]$ where $[\ ]$ denotes linear equivalence. We identify $C^{(d)}$ with the set of effective divisors of degree d on C.

We can give an explicit description of the Jacobian variety J via the Abel–Jacobi map $f^{(3)}$ using ∞ as a basepoint. This is a good way to think of J since $f^{(3)}$ is surjective. In fact, the map $f^{(3)}$ is almost injective as we can see in the following proposition, which is a consequence of the Riemann–Roch theorem.

PROPOSITION 2.2. *The dimension of the fiber of $f^{(3)}$ containing the divisor $D = P_1 + P_2 + P_3$ is* 0 *unless $D + Q = L.C$ for some line L and point Q in which case it is* 1.

In other words, the dimension is 1 if and only if $\omega_C \geq D$ for some canonical divisor ω_C. In this case, $[D_1] = [D_2]$ in $\mathrm{Pic}^3(C)$ means that there are lines L_1 and L_2 through Q so that $L_1.C = D_1 + Q$ and $L_2.C = D_2 + Q$. In the case of dimension 0, there will be a single effective divisor of degree 3 representing the class. The group $\mathrm{Pic}^3(C)$ is isomorphic to the group $\mathrm{Pic}^0(C)$ by $[D] \mapsto [D - 3\infty]$.

Throughout this paper we denote solutions to the equations $x^3 = 1$ and $x^4 = 1$ by α and β, respectively.

3. Torsion points on the image of C. We can embed C into J with the Abel–Jacobi map f using ∞ as a basepoint. In this section, we show that W, the set of Weierstrass points of C, is equal to T, the set of points whose images under f are torsion. For simplicity we usually refer to Weierstrass points of weight 1 as ordinary flexes and Weierstrass points of weight 2 as hyperflexes. One can find the flexes on $F(X, Y, Z) = Y^3Z + Z^4 - X^4 = 0$ by setting the determinant of the Hessian matrix of F to 0. The determinant is $-108X^2Y(Y^3 - 8Z^3)$. On the line $x = 0$ are the four hyperflexes. The line $Z = 0$ meets the curve at 4∞ and lines of the form $y = -\alpha$ meet the curve at $4(0, -\alpha)$.

So the ordinary flexes occur on the line $y = 0$ and at the points whose x- and y-coordinates satisfy $y^3 = 8$ and $x^4 = 9$. Lines of the form $x = \beta$ meet the curve at $3(\beta, 0) + \infty$ and lines of the form $\beta y - \sqrt{3}\,\alpha x + \alpha\beta = 0$ meet the curve at $3(\sqrt{3}\,\beta, 2\alpha) + (0, -\alpha)$. Using Proposition 2.2, we see that $[(\beta, 0) - \infty]$ has order 3; also $[(0, -\alpha) - \infty]$ has order 4 and thus $[(\sqrt{3}\beta, 2\alpha) - \infty]$ has order 12.

Note that the points whose x- and y-coordinates satisfy $y^3 = 8$ and $x^4 = 9$ come in three sets of four, which are the intersection divisors with lines of the form $y = 2\alpha$. The other four ordinary flexes all lie on the line $y = 0$. So the sixteen ordinary flexes come in four sets of four collinear points. Consider a fixed set of collinear ordinary flexes. If we find the fourth point of intersection with the curve of the tangent line at each ordinary flex we get the same hyperflex. In addition the four hyperflexes are collinear. The tangent lines to the hyperflexes all meet at the point $(1 : 0 : 0)$, which is not on the curve. Each line through a set of four collinear ordinary flexes also passes through $(1 : 0 : 0)$. This information is displayed in Figure 1 where the hyperflexes are large dots and the ordinary flexes are small dots.

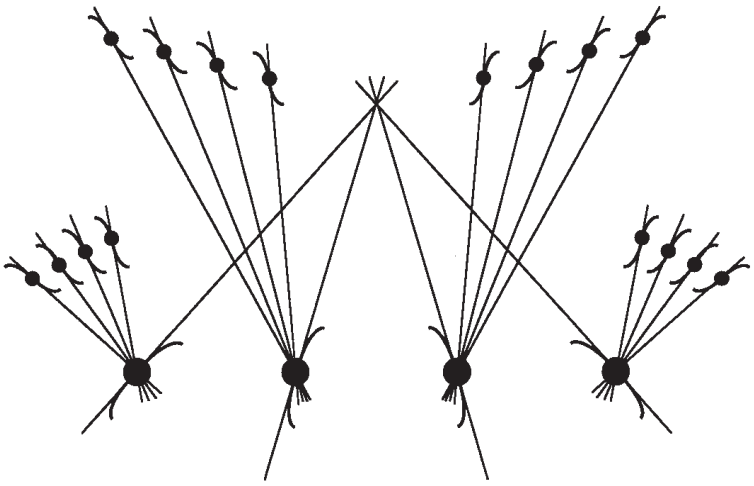

Fig. 1

Let the points P and Q on C be equivalent if the divisor class $[P - Q]$ has finite order. An equivalence class is called a *torsion packet*. To see that the 20 flexes of C form a torsion packet, we make use of the automorphism group of C.

Coleman proves the following in [C1].

THEOREM A. *Let $f : C \hookrightarrow J$ be an Albanese morphism defined over a number field K, of a smooth curve of genus g into its Jacobian. Suppose J has potential complex multiplication. Let S denote the set of primes $\mathfrak{p}$ of K satisfying*

(i) $\mathfrak{p}$ *does not divide* 2 *or* 3,
(ii) $K/\mathbb{Q}$ *is unramified at* $\mathfrak{p}$,
(iii) C *has ordinary reduction over* K.

Then the set T of torsion points of J defined over an algebraic closure of K which lie on the image of C is defined over an extension of K unramified above S. Moreover,

$$\#T \leq pg$$

where p is the smallest prime of $\mathbb{Q}$ divisible by a prime in S.

We will see in Proposition 5.1 that J is isogenous, over $\mathbb{Q}(\sqrt{3})$, to the product of three CM elliptic curves; so J has potential complex multiplication. Since ∞ is defined over $\mathbb{Q}$, f is also and it is an Albanese morphism. Thus we can let $K = \mathbb{Q}$. We also let $\mathfrak{p} = p = 13$, which is the smallest prime at which J has ordinary good reduction.

We saw above that the images of all 20 flexes of C under f are torsion. From the theorem above, the total number of torsion points on the image of C is at most 39. Let us show that there are no other torsion points on the image of C. There are 24 points on C that are not flexes and are fixed by a nontrivial automorphism. These are the points of the form $(\beta\sqrt[4]{-9 \pm 6\sqrt{3}}, \alpha(-1 \pm \sqrt{3}))$ where the two $\pm$ must agree. Each of those points is fixed by exactly two automorphisms and there are 48 automorphisms. The image of ∞ under any automorphism must also be a hyperflex. So if there were another point on C whose image were torsion, then there would be at least $48/2 = 24$ new torsion points. But $20 + 24 > 39$ so there are no more and we have the following proposition.

Proposition 3.1. $W = T$.

4. Rational points on $y^3 + 1 = x^4$ and its Jacobian. Recall that α and β denote solutions of $x^3 = 1$ and $x^4 = 1$ respectively. From Section 3, the 20 Weierstrass points of C are each defined over $\mathbb{Q}(\zeta_{12})$. These are the point ∞, and points of the form $(0, -\alpha)$, $(\beta, 0)$ or $(\beta\sqrt{3}, 2\alpha)$. We will show that there are no more points of $C(\mathbb{Q}(\zeta_{12}))$. To do this, we first describe $J(\mathbb{Q}(\zeta_{12}))$.

Lemma 4.1. *The divisor classes $[(0,-1)-\infty]$ and $[(0,-\zeta_3)-\infty]$ generate a subgroup of $J(\mathbb{Q}(\zeta_{12}))$ isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$.*

Proof. We saw in Section 3 that each of these divisor classes has order 4. From Proposition 2.2, their doubles are different. Thus these two divisor classes generate a group isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$. ∎

For simplicity, in the following discussion, and in the proofs in the remainder of this section, we will denote the field $\mathbb{Q}(\zeta_{12})$ by M. In addition, we will let $\dim N$ denote the dimension of an $\mathbb{F}_3$ vector space N. Let us describe a homomorphism on $J(M)$ that will help us find a basis for $J[3]$ in the proof of Lemma 4.2 and also enable us to compute $J(M)$ via a descent in the proof of Lemma 4.4.

Let σ be the automorphism of C given by $(X : Y : Z) \mapsto (X : \zeta_3 Y : Z)$. This automorphism of C induces an automorphism of J which we also denote by σ. The Jacobian is generated by divisor classes of the form $[P - \infty]$. If $P \in C \setminus \infty$, then $P + \sigma P + \sigma^2 P + \infty$ is the intersection divisor of C with the line $x = x(P)$. Thus the divisor $P + \sigma P + \sigma^2 P - 3\infty$ is principal. So the induced endomorphism on the Jacobian given by $1 + \sigma + \sigma^2$ equals 0. We refer to this automorphism of J as ζ_3 instead of σ and let ϕ be the endomorphism $1 - \zeta_3$. We have $\phi^2 = -3\zeta_3$ in $\mathrm{End}(J)$. Since the dimension of J is 3, $\dim J[3] = 6$ and so $\dim J[\phi] = 3$.

Let $H^1(M, J[\phi])$ denote $H^1(\mathrm{Gal}(\overline{M}/M), J[\phi])$ and δ denote the coboundary map from $J(M)$ to $H^1(M, J[\phi])$. Then we have

$$J(M)/\phi J(M) \overset{\delta}{\hookrightarrow} H^1(M, J[\phi]).$$

Let

$$L = M[T]/(T^4 - 1) \cong M \times M \times M \times M \quad \text{by } T \mapsto (-1, 1, -i, i).$$

From [KS, Thm. 5.3], the group $H^1(M, J[\phi])$ is isomorphic to the kernel of the norm from L^*/L^{*3} to M^*/M^{*3}. The composition of this isomorphism and δ is difficult to work with. But there is another map that is identical to this composition.

Let $R = \sum n_i R_i$ be a degree 0 divisor of C, defined over M, whose support does not contain ∞ or points with y-coordinate 0. We define the map $x - T$ from such divisors to L^* by $(x - T)(R) = \prod (x(R_i) - T)^{n_i}$. The map $x - T$ is well-defined from equivalence classes of such divisors to L^*/L^{*3} and every divisor class contains such a divisor (see [KS, Lemmas 5.5 and 5.6]). So $x - T$ is a homomorphism on $J(M)$. In fact, $x - T$ is the same as the composition of the isomorphism from $H^1(M, J[\phi])$ to the kernel of the norm from L^*/L^{*3} to M^*/M^{*3} and the coboundary map from $J(M)$ to $H^1(M, J[\phi])$ (see [KS, Thm. 5.4]). So $x - T$ is an injection from $J(M)/\phi J(M)$ to L^*/L^{*3}.

We would like to describe a finite subgroup containing the image of $x - T$. This will establish notation for the image of $x - T$ and also be useful in the descent. The set of bad primes of C over $\mathbb{Q}$ consists of the primes 2 and 3. Let $K = \mathbb{Q}(\zeta_3)$. There is one prime $\mathfrak{p}$ of M over 2; it is inert in K and ramifies in M. There is one prime $\mathfrak{q}$ of M over 3; it ramifies in K and then is inert up to M. Let $S = \{\mathfrak{p}, \mathfrak{q}\}$. The image of $x - T$ is known to be contained in the finite subgroup $H^1(M, J[\phi]; S)$ of $H^1(M, J[\phi])$ (see [KS, Section 5.2]). Under the above isomorphism, the group $H^1(M, J[\phi]; S)$ is isomorphic to the subgroup of L^*/L^{*3} that is unramified outside the primes over 2 and 3 and is in the kernel of the norm to M^*/M^{*3}. Let us describe this group. From above, $L^*/L^{*3} \cong (M^*/M^{*3})^4$. Since M is a

totally imaginary extension of the rationals, it has unit rank 1. We note that $i-\zeta_3$ is a fundamental unit and $(i-\zeta_3)^2 = -i\zeta_3(2+\sqrt{3})$ where $2+\sqrt{3}$ is a fundamental unit for the real quadratic subfield. The class group of the field M is trivial. Thus the subgroup of M^*/M^{*3} of elements whose cube roots produce fields unramified over M outside of the primes over 2 and 3 is $\langle i-\zeta_3, \zeta_3, 1+i, \sqrt{-3}\rangle$. We fix $\zeta_3 = (-1+\sqrt{-3})/2$ and $\sqrt{3} = \sqrt{-3}\,i$. The group $H^1(M, J[\phi]; S)$ is isomorphic to the subgroup of $\langle i-\zeta_3, \zeta_3, 1+i, \sqrt{-3}\rangle^4$ in $(M^*/M^{*3})^4$ of elements whose coordinate product is a cube. We see $\dim H^1(M, J[\phi]; S) = 12$ as any coordinate is determined by the other three. By abuse of notation, we refer to this subgroup of L^*/L^{*3} and $(M^*/M^{*3})^4$ by $H^1(M, J[\phi]; S)$.

Lemma 4.2. *A basis for* $J[3]$ *is* $[(1,0)-\infty]$, $[(-1,0)-\infty]$, $[(i,0)-\infty]$, $[4(\sqrt{3},2)-4\infty]$, $[4(\sqrt{-3},2)-4\infty]$ *and* $[(\sqrt[4]{-3}, \sqrt[3]{-4})+(-\sqrt[4]{-3}, \sqrt[3]{-4})-2\infty]$. *The first five divisor classes form a basis for* $J(\mathbb{Q}(\zeta_{12}))[3]$.

Proof. We start by showing that the first three divisor classes generate the kernel of ϕ. From Proposition 2.2, the effective divisors of degree 3 supported on ∞ and points of the form $(\beta, 0)$, represent 27 different divisor classes in $\mathrm{Pic}^3(C)$. Thus any three distinct divisor classes of the form $[(\beta,0) - \infty]$ are a basis for $J[\phi]$.

From Section 3, the divisor classes $[4(\sqrt{3},2)-4\infty]$ and $[4(\sqrt{3},2\zeta_3)-4\infty]$ have order 3. To show that these two divisor classes are independent of the elements in $J[\phi]$ and of each other, we will use the map $x-T$ on $J(M)[3]$ (or rather its image in $J(M)/\phi J(M)$). We have

$$J(M)[3] \to J(M)/\phi J(M) \overset{x-T}{\hookrightarrow} H^1(M, J[\phi]; S).$$

All of the ϕ-torsion is rational over M. In the following table we show the images of the elements of a basis for $J[\phi]$ under the map $x-T$ in $H^1(M, J[\phi]; S)$. Under the isomorphism of L^*/L^{*3} and $(M^*/M^{*3})^4$, the map $x-T$ becomes the 4-tuple of functions $(x+1, x-1, x+i, x-i)$. Above each coordinate is written $x-\beta$ to remind us how to compute that coordinate. To compute the image of $[(-1,0)-\infty]$, we can essentially ignore the ∞ and compute the image of $-1-\beta$ for $\beta = 1, -i, i$ for the second through fourth coordinates. Then we take the square of their product for the first coordinate (see [KS, Lemma 5.5]).

		$x+1$	$x-1$	$x+i$	$x-i$
$[(1,0)-\infty]$	$\mapsto$	$(1+i)^2$	$(1+i)^2$	$1+i$	$1+i$
$[(-1,0)-\infty]$	$\mapsto$	$(1+i)^2$	$(1+i)^2$	$1+i$	$1+i$
$[(i,0)-\infty]$	$\mapsto$	$1+i$	$1+i$	$(1+i)^2$	$(1+i)^2$

We see that the image has dimension 1 over $\mathbb{F}_3$. Since $\phi^2=-3\zeta_3$, the group $J(M)[\phi]/\phi(J(M)[3])$ injects into $J(M)/\phi J(M)$, which in turn injects into L^*/L^{*3}. Thus $\dim J(M)[3]=5$.

The divisor classes $[4(\sqrt{-3},2)-4\infty]$ and $[4(\sqrt{3},2)-4\infty]$ also have order 3. In the following table we show the images of $[(\sqrt{-3},2)-\infty]$, $[(\sqrt{3},2)-\infty]$ and $[(1,0)-\infty]$ in L^*/L^{*3} by the map $x-T$. To compute the image of $[(x,y)-\infty]$ where $y\neq 0$ we can simply ignore the ∞ (see [KS, Lemma 5.5]).

	$x+1$	$x-1$	$x+i$	$x-i$
$[(1,0)-\infty]\mapsto$	$(1+i)^2$	$(1+i)^2$	$1+i$	$1+i$
$[(\sqrt{-3},2)-\infty]\mapsto$	$\zeta_3^2(1+i)^2$	$\zeta_3(1+i)^2$	$\zeta_3^2(1+i)(i-\zeta_3)^2$	$\zeta_3(1+i)(i-\zeta_3)$
$[(\sqrt{3},2)-\infty]\mapsto$	$\zeta_3(1+i)(i-\zeta_3)$	$\zeta_3^2(1+i)(i-\zeta_3)^2$	$\zeta_3^2(1+i)^2$	$\zeta_3(1+i)^2$

These three images are independent. This tells us that $[(1,0)-\infty]$, $[(-1,0)-\infty]$, $[(i,0)-\infty]$, $[4(\sqrt{-3},2)-4\infty]$, and $[4(\sqrt{3},2)-4\infty]$ form a basis for $J(M)[3]$.

Let E_1 be the Jacobian of the curve $u^3+1=v^2$. A basis for $E_1[3]$ in (v,u)-coordinates is $[(1,0)-\infty]$ and $[(\sqrt{-3},\sqrt[3]{-4})-\infty]$. The map from $y^3+1=x^4$ to $u^3+1=v^2$, induced by $(v,u)=(x^2,y)$, sends the first five listed independent elements of $J[3]$ to $[(\pm1,0)-\infty]$ on E_1. The image of $[(\sqrt[4]{-3},\sqrt[3]{-4})+(-\sqrt[4]{-3},\sqrt[3]{-4})-2\infty]$ in $E_1[3]$ is $[2(\sqrt{-3},\sqrt[3]{-4})-2\infty]$ and so it must be independent of the other five basis elements of $J[3]$. ∎

Let $J(\mathbb{Q}(\zeta_{12}))_{\mathrm{tors}}$ denote the torsion subgroup of $J(\mathbb{Q}(\zeta_{12}))$.

LEMMA 4.3. *The group* $J(\mathbb{Q}(\zeta_{12}))_{\mathrm{tors}}$ *is isomorphic to* $(\mathbb{Z}/4\mathbb{Z})^2\oplus(\mathbb{Z}/3\mathbb{Z})^5$ *and is generated by the seven divisor classes listed in Lemmas* 4.1 *and* 4.2.

Proof. From Lemmas 4.1 and 4.2, $J(M)_{\mathrm{tors}}$ has at least $4^2\cdot3^5$ elements. Since $M=\mathbb{Q}(\zeta_{12})$, any prime congruent to 1 modulo 12 splits completely in M. Over $\mathbb{F}_{13}$, the characteristic polynomial of the Frobenius for J is $T^6+6T^5+39T^4+124T^3+507T^2+1014T+2197$ and over $\mathbb{F}_{37}$ it is $T^6+6T^5+75T^4+484T^3+2775T^2+8214T+50653$. By evaluating at 1 we find that $\#J(\mathbb{F}_{13})=4^2\cdot3^5$. Since the non-13 part of $J(M)_{\mathrm{tors}}$ injects into $J(\mathbb{F}_{13})$, we see that the possible non-13 part of $J(M)_{\mathrm{tors}}$ has already been realized. We also have $\#J(\mathbb{F}_{37})=4^4\cdot3^5$, so $J(M)$ has no 13-torsion and $J(M)_{\mathrm{tors}}\cong(\mathbb{Z}/4\mathbb{Z})^2\oplus(\mathbb{Z}/3\mathbb{Z})^5$. ∎

Let ϕ be the endomorphism defined in the discussion before Lemma 4.2.

LEMMA 4.4. *The ϕ-Selmer group of J over $\mathbb{Q}(\zeta_{12})$, denoted by $S^{\phi}(\mathbb{Q}(\zeta_{12}), J)$, is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$, as is $J(\mathbb{Q}(\zeta_{12}))/\phi J(\mathbb{Q}(\zeta_{12}))$. Both groups are generated by the image of $J(\mathbb{Q}(\zeta_{12}))[3]$.*

P r o o f. We compute the group $S^{\phi}(M, J)$ using the ϕ-descent described in [KS, Section 5]. The group $S^{\phi}(M, J)$ is a subgroup of $H^1(M, J[\phi])$ which contains the image of $J(M)/\phi J(M)$ under the coboundary map. It is isomorphic to the subgroup of $H^1(M, J[\phi]; S)$ that maps to the image of $(x - T)(J(M_{\mathfrak{r}})/\phi J(M_{\mathfrak{r}}))$ in $L_{\mathfrak{r}}^*/L_{\mathfrak{r}}^{*3}$ for the primes $\mathfrak{r} \in S$ where $L_{\mathfrak{r}} = M_{\mathfrak{r}}[T]/(T^4 - 1)$ (see [KS, Prop. 5.7]).

$$\begin{array}{ccc} J(M)/\phi J(M) & \overset{x-T}{\hookrightarrow} & L^*/L^{*3} \\ \downarrow & & \downarrow \\ \displaystyle\prod_{\mathfrak{r}\in S} J(M_{\mathfrak{r}})/\phi J(M_{\mathfrak{r}}) & \overset{x-T}{\hookrightarrow} & \displaystyle\prod_{\mathfrak{r}\in S} L_{\mathfrak{r}}^*/L_{\mathfrak{r}}^{*3} \end{array}$$

Let us show that the images of $[(1,0) - \infty]$, $[(\sqrt{-3}, 2) - \infty]$, and $[(\sqrt{3}, 2) - \infty]$ generate $S^{\phi}(M, J)$. Recall, from the proof of Lemma 4.2, the images of those three divisor classes in $L^*/L^{*3} \cong (M^*/M^{*3})^4$.

	$x+1$	$x-1$	$x+i$	$x-i$
$[(1,0) - \infty] \mapsto$	$(1+i)^2$	$(1+i)^2$	$1+i$	$1+i$
$[(\sqrt{-3}, 2) - \infty] \mapsto$	$\zeta_3^2(1+i)^2$	$\zeta_3(1+i)^2$	$\zeta_3^2(1+i)(i-\zeta_3)^2$	$\zeta_3(1+i)(i-\zeta_3)$
$[(\sqrt{3}, 2) - \infty] \mapsto$	$\zeta_3(1+i)(i-\zeta_3)$	$\zeta_3^2(1+i)(i-\zeta_3)^2$	$\zeta_3^2(1+i)^2$	$\zeta_3(1+i)^2$

From [Ma], if $\mathfrak{r}$ is a finite prime of M then $J(M_{\mathfrak{r}})$ has a subgroup of finite index isomorphic to three copies of the additive group of the integers of $M_{\mathfrak{r}}$. Since the residue characteristic of $M_{\mathfrak{p}}$ is 2, which is prime to 3, one can use the snake lemma to show that $\dim J(M_{\mathfrak{p}})/\phi J(M_{\mathfrak{p}}) = 3$. The group $M_{\mathfrak{p}}^*/M_{\mathfrak{p}}^{*3}$ is $\langle \zeta_3, 1+i \rangle$. The number $\sqrt{-3}$ is trivial in $M_{\mathfrak{p}}^*/M_{\mathfrak{p}}^{*3}$ and $i - \zeta_3 \equiv 1 + \zeta_3 \equiv \zeta_3^2 \pmod{M_{\mathfrak{p}}^{*3}}$.

In the following table are generators of $J(M_{\mathfrak{p}})/\phi J(M_{\mathfrak{p}})$ and their images in $L_{\mathfrak{p}}^*/L_{\mathfrak{p}}^{*3} \cong (M_{\mathfrak{p}}^*/M_{\mathfrak{p}}^{*3})^4$.

	$x+1$	$x-1$	$x+i$	$x-i$
$[(1,0) - \infty] \mapsto$	$(1+i)^2$	$(1+i)^2$	$1+i$	$1+i$
$[(\sqrt{-3}, 2) - \infty] \mapsto$	$\zeta_3^2(1+i)^2$	$\zeta_3(1+i)^2$	$1+i$	$1+i$
$[(\sqrt{3}, 2) - \infty] \mapsto$	$1+i$	$1+i$	$\zeta_3^2(1+i)^2$	$\zeta_3(1+i)^2$

Again from [Ma], and using the snake lemma, we can show that $\dim J(M_{\mathfrak{q}})/\phi J(M_{\mathfrak{q}})$ is 9 (or see [KS, Prop. 5.8]). The group $M_{\mathfrak{q}}^*/M_{\mathfrak{q}}^{*3}$ is $\langle \sqrt{-3}, 1+\sqrt{-3}, 1+i\sqrt{-3}, 1+\sqrt{-3}^2, 1+i\sqrt{-3}^2, 1+\sqrt{-3}^3 \rangle$. Let us rename

those numbers $\langle A, B, E, \Gamma, \Phi, \Delta\rangle$ (to be consistent with the notation in [KS]). The cubes are generated by $1 \pm i\sqrt{-3}^3$, and everything that is 1 modulo 9. The image of ζ_3 in $M_{\mathfrak{q}}^*/M_{\mathfrak{q}}^{*3}$ is $B^2\Gamma$ and the image of $1+i$ is Γ^2. The image of $2+\sqrt{3}$ is Γ^2E^2 and $(i-\zeta_3)^2 = -\zeta_3(2+\sqrt{3})$, so the image of $i-\zeta_3$ is BE.

In the following table are generators of $J(M_{\mathfrak{q}})/\phi J(M_{\mathfrak{q}})$ and their images in $L_{\mathfrak{q}}^*/L_{\mathfrak{q}}^{*3} \cong (M_{\mathfrak{q}}^*/M_{\mathfrak{q}}^{*3})^4$.

		$x+1$	$x-1$	$x+i$	$x-i$
$[(1,0)-\infty]$	$\mapsto$	Γ	Γ	Γ^2	Γ^2
$[(\sqrt{3},2)-\infty]$	$\mapsto$	E	$E^2\Gamma$	B	$B^2\Gamma^2$
$[(\sqrt{-3},2)-\infty]$	$\mapsto$	B	$B^2\Gamma^2$	$E^2\Gamma$	E
$[(3,y_1)-\infty]$	$\mapsto$	Γ^2	Γ	Φ	Φ^2
$[(3i,y_2)-\infty]$	$\mapsto$	Φ^2	Φ	Γ^2	Γ
$[(\sqrt{-3}^3,y_3)-\infty]$	$\mapsto$	Δ	Δ^2	1	1
$[(\sqrt{3}^3,y_4)-\infty]$	$\mapsto$	1	1	Δ	Δ^2
$[(4+4i,y_5)-\infty]$	$\mapsto$	Γ	$\Gamma^2\Phi$	Γ	$\Gamma^2\Phi^2$
$[(3+\sqrt{-3},y_6)-\infty]$	$\mapsto$	$B\Gamma^2\Delta$	$B^2\Delta$	$\Gamma\Delta^2E^2\Phi$	$\Delta^2E\Phi^2$

From the image of $J(M_{\mathfrak{q}})/\phi J(M_{\mathfrak{q}})$, we see that no $\sqrt{-3}$ appears in an element of $S^\phi(M,J)$. So in $S^\phi(M,J)$, the fourth coordinate is in $\langle i-\zeta_3, \zeta_3, 1+i\rangle$. All such possibilities occur, so it suffices to show that any element of $S^\phi(M,J)$, with a 1 as the fourth coordinate, is trivial. The subgroup of the image of $J(M_{\mathfrak{p}})/\phi J(M_{\mathfrak{p}})$, of elements with a 1 as the fourth coordinate, is $\langle(\zeta_3^2,\zeta_3,1,1)\rangle$. So in $S^\phi(M,J)$, any element with a 1 as the fourth coordinate does not contain $1+i$.

The subgroup of the image of $J(M_{\mathfrak{q}})/\phi J(M_{\mathfrak{q}})$, of elements with a 1 as the fourth coordinate, is $\langle(\Delta,\Delta^2,1,1),\ (\Delta,\Delta,\Delta,1),\ (\Phi^2\Gamma,\Phi\Gamma,\Gamma,1),\ (\Gamma,\Phi,\Gamma^2\Phi^2,1)\rangle$. We see that in the Selmer group, any element with a 1 as the fourth coordinate can not contain $i-\zeta_3$ or ζ_3 and so is trivial. So $\dim S^\phi(M,J)$ and $\dim J(M)/\phi J(M)$ are both 3 and each group is generated by the image of 3-torsion. ∎

THEOREM 4.5. $J(\mathbb{Q}(\zeta_{12})) \cong (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/3\mathbb{Z})^5$.

Proof. From Lemma 4.3, $J(M)_{\text{tors}} \cong (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/3\mathbb{Z})^5$. So it suffices to show that the Mordell–Weil rank of J over M is 0. Since $J(M)$ is a finitely generated abelian group, we can do this by showing that $J(M)/3J(M)$ is the image of $J(M)[3]$. From Lemma 4.4, $\dim J(M)/\phi J(M)$ is 3 and the group is generated by the image of $J(M)[3]$. It follows from the snake lemma that

the following sequence is exact:

$$0 \to J(M)[\phi]/\phi(J(M)[3]) \to J(M)/\phi J(M) \xrightarrow{\phi} J(M)/3J(M) \to J(M)/\phi J(M) \to 0.$$

From this exact sequence, we see that $J(M)/3J(M)$ is also generated by the image of 3-torsion and so $J(M)$ has trivial Mordell–Weil rank. ∎

Corollary 4.6. $C(\mathbb{Q}(\zeta_{12})) = W = T$.

Proof. This follows immediately from the fact that the 20 Weierstrass points are a torsion packet (Proposition 3.1) and $J(\mathbb{Q}(\zeta_{12}))$ is all torsion (Theorem 4.5). ∎

Corollary 4.7. $J(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2$.

Proof. Since we have an explicit set of generators of $J(M)$ we can compute the $\mathrm{Gal}(M/\mathbb{Q})$-invariants. We find that $J(\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})^2$ and is generated by $[(0,-1)-\infty]$, $[(-1,0)-\infty]$ and $[(1,0)-\infty]$. ∎

Corollary 4.8. *The* 36 *elements of* $J(\mathbb{Q})$ *are represented in* $\mathrm{Pic}^3(C)$ *by effective divisors supported on the following* 22 *points*: ∞, $(\pm\sqrt{3}, 2)$, *and points of the form* $(\beta, 0)$, $(0, -\alpha)$, $(\pm\sqrt{-3}, 2\alpha)$, $(\gamma, \frac{1}{2}(\gamma+1)^2)$, *or* $(\delta, \frac{1}{2}(\delta-1)^2)$, *where* γ *is a solution of* $x^3+5x^2-x+3=0$ *and* δ *is a solution of* $x^3-5x^2-x-3=0$.

Proof. Let us denote the following points on C:

$$\begin{array}{lll}
Q_1 = (0,-1), & Q_8 = (-\sqrt{3}, 2), & Q_{15} = (-\sqrt{-3}, 2\zeta_3),\\
Q_2 = (-1,0), & Q_9 = (\sqrt{3}, 2), & Q_{16} = \big(\gamma_1, \tfrac{1}{2}(\gamma_1+1)^2\big),\\
Q_3 = (1,0), & Q_{10} = (-\sqrt{-3}, 2), & Q_{17} = \big(\gamma_2, \tfrac{1}{2}(\gamma_2+1)^2\big),\\
Q_4 = (-i,0), & Q_{11} = (\sqrt{-3}, 2), & Q_{18} = \big(\gamma_3, \tfrac{1}{2}(\gamma_3+1)^2\big),\\
Q_5 = (i,0), & Q_{12} = (\sqrt{-3}, 2\zeta_3), & Q_{19} = \big(\delta_1, \tfrac{1}{2}(\delta_1-1)^2\big),\\
Q_6 = (0,-\zeta_3^2), & Q_{13} = (-\sqrt{-3}, 2\zeta_3^2), & Q_{20} = \big(\delta_2, \tfrac{1}{2}(\delta_2-1)^2\big),\\
Q_7 = (0,-\zeta_3), & Q_{14} = (\sqrt{-3}, 2\zeta_3^2), & Q_{21} = \big(\delta_3, \tfrac{1}{2}(\delta_3-1)^2\big),
\end{array}$$

where $\zeta_3 = (-1+\sqrt{-3})/2$ and $\sqrt{3} = \sqrt{-3}\,i$ and the γ_i are the roots of x^3+5x^2-x+3 and the δ_i are the roots of x^3-5x^2-x-3. We now display the group $\mathrm{Pic}^3(C)(\mathbb{Q})$. In the following table we give the divisor class of degree three corresponding to each element $j[Q_1+2\infty] + k[Q_2+2\infty] + l[Q_3+2\infty]$.

(j,k,l)	Divisor class	Order	(j,k,l)	Divisor class	Order
$(0,0,0)$	$[3\infty]$	1	$(0,2,2)$	$[Q_4 + Q_5 + \infty]$	3
$(1,0,0)$	$[Q_1 + 2\infty]$	4	$(2,0,2)$	$[Q_8 + Q_9 + Q_2]$	6
$(0,1,0)$	$[Q_2 + 2\infty]$	3	$(2,2,0)$	$[Q_8 + Q_9 + Q_3]$	6
$(0,0,1)$	$[Q_3 + 2\infty]$	3	$(2,2,2)$	$[Q_8 + Q_9 + \infty]$	6
$(2,0,0)$	$[2Q_1 + \infty]$	2	$(2,1,1)$	$[Q_{10} + Q_{11} + \infty]$	6
$(0,2,0)$	$[2Q_2 + \infty]$	3	$(2,2,1)$	$[Q_{10} + Q_{11} + Q_2]$	6
$(0,0,2)$	$[2Q_3 + \infty]$	3	$(2,1,2)$	$[Q_{10} + Q_{11} + Q_3]$	6
$(1,1,0)$	$[Q_1 + Q_2 + \infty]$	12	$(1,2,2)$	$[Q_1 + Q_4 + Q_5]$	12
$(1,0,1)$	$[Q_1 + Q_3 + \infty]$	12	$(1,2,1)$	$[Q_{16} + Q_{17} + Q_{18}]$	12
$(0,1,1)$	$[Q_2 + Q_3 + \infty]$	3	$(1,1,2)$	$[Q_{19} + Q_{20} + Q_{21}]$	12
$(1,1,1)$	$[Q_1 + Q_2 + Q_3]$	12	$(3,1,0)$	$[Q_2 + Q_6 + Q_7]$	12
$(1,2,0)$	$[Q_1 + 2Q_2]$	12	$(3,0,1)$	$[Q_3 + Q_6 + Q_7]$	12
$(1,0,2)$	$[Q_1 + 2Q_3]$	12	$(3,2,0)$	$[Q_{14} + Q_{15} + \infty]$	12
$(0,1,2)$	$[Q_2 + 2Q_3]$	3	$(3,0,2)$	$[Q_{12} + Q_{13} + \infty]$	12
$(2,1,0)$	$[2Q_1 + Q_2]$	6	$(3,1,1)$	$[Q_1 + Q_{10} + Q_{11}]$	12
$(2,0,1)$	$[2Q_1 + Q_3]$	6	$(3,2,1)$	$[Q_3 + Q_{14} + Q_{15}]$	12
$(0,2,1)$	$[2Q_2 + Q_3]$	3	$(3,1,2)$	$[Q_2 + Q_{12} + Q_{13}]$	12
$(3,0,0)$	$[3Q_1]$	4	$(3,2,2)$	$[Q_1 + Q_8 + Q_9]$	12

To obtain the above divisor classes one needs to produce certain conics that pass through specific points on our curve. We give a list of such conics and their intersection divisors.

Conic	Intersection divisor
$y = x^2 - 1$	$2Q_1 + Q_2 + Q_3 + Q_8 + Q_9 + 2\infty$
$y = -x^2 - 1$	$2Q_1 + Q_4 + Q_5 + Q_{10} + Q_{11} + 2\infty$
$x^2 + y^2 = 1$	$2Q_1 + 2Q_2 + 2Q_3 + Q_{10} + Q_{11}$
$2y = (x+1)^2$	$Q_2 + Q_{12} + Q_{13} + Q_{16} + Q_{17} + Q_{18} + 2\infty$
$2y = (x-1)^2$	$Q_3 + Q_{14} + Q_{15} + Q_{19} + Q_{20} + Q_{21} + 2\infty$
$y^2 - 3x^2 = 1$	$2Q_1 + Q_{16} + Q_{17} + Q_{18} + Q_{19} + Q_{20} + Q_{21}$ ∎

Corollary 4.9. *The only points on C with coordinates in a quadratic extension of $\mathbb{Q}$ are the ones listed in the previous corollary*; *each is a Weierstrass point. The only points on C with coordinates in a cubic extension of $\mathbb{Q}$ are the ones listed in the previous corollary and those gotten by finding the three other points of intersection of the curve with a $\mathbb{Q}$-rational line through any one of the four points of $C(\mathbb{Q})$.*

Proof. From Corollary 4.8 and Proposition 2.2, the only divisor classes in $\mathrm{Pic}^3(C)(\mathbb{Q})$ with dimension 1 are $[3\infty]$, $[2Q_2 + \infty]$, $[2Q_3 + \infty]$, and $[3Q_1]$.

Each of these four divisor classes are given by the pencil of lines through one of the four points of $C(\mathbb{Q})$. For example, we have the following equivalences of divisors:

$$\begin{aligned} 3\infty &\sim Q_1 + Q_6 + Q_7, \\ 2Q_2 + \infty &\sim Q_3 + Q_4 + Q_5, \\ 2Q_3 + \infty &\sim Q_2 + Q_4 + Q_5, \\ 3Q_1 &\sim Q_6 + Q_7 + \infty. \end{aligned}$$

From Proposition 2.2, the other 32 divisor classes in $\mathrm{Pic}^3(C)(\mathbb{Q})$ are uniquely represented. ∎

5. An isogeny from J to the product of three elliptic curves. The results in this section are largely independent of the rest of this paper and since all of the results are highly computational, we will simply give ideas of their proofs.

There is a map of degree 2 from $y^3 + 1 = x^4$ to the curve $u^3 + 1 = v^2$, whose Jacobian is an elliptic curve with j-invariant 0, given by $(u, v) = (y, x^2)$. We denote this elliptic curve by E_1. The curve $u^3 + 1 = v^2$ is isomorphic to the quotient of $y^3 + 1 = x^4$ by the automorphism given in Proposition 2.1 by the left-hand matrix with $\alpha = 1$ and $\beta = -1$. There are maps of degree 2 from $y^3 + 1 = x^4$ to the curves

$$v^2 = u^4 + \frac{3 \pm 2\sqrt{3}}{9}$$

by

$$(u, v) = \left(\frac{1}{x} \left[\left(\frac{-3 \mp \sqrt{3}}{6} \right) y \pm \frac{\sqrt{3}}{3} \right], \frac{1}{x^2} \left[\left(\frac{2 \pm \sqrt{3}}{6} \right) y^2 - \frac{1}{3} y + \left(\frac{1 \pm \sqrt{3}}{3} \right) \right] \right).$$

The Jacobians of both curves are elliptic curves with j-invariant 1728 and they are isomorphic over $\mathbb{Q}(\zeta_{12})$. We denote these elliptic curves by E_2 and E_3. The curve $v^2 = u^4 + (3 + 2\sqrt{3})/9$ is isomorphic to the quotient of the curve $y^3 + 1 = x^4$ by the automorphism given in Proposition 2.1 by the right-hand matrix with $\alpha_1 = \alpha_2 = 1$ and $\beta = -1$ and the curve $v^2 = u^4 + (3 - 2\sqrt{3})/9$ is isomorphic to the quotient by the automorphism given by the right-hand matrix with $\alpha_1 = \alpha_2 = \beta = 1$. The maps from C to each of the genus 1 curves induce maps from J to the three elliptic curves. This induces a map

$$\psi : J \to \prod_{i=1}^{3} E_i.$$

For each of the three involutions listed above, we can find a generator for the subspace of the holomorphic differentials on C fixed by that involution.

These differentials are xdx/y^2, $(y + 1 + \sqrt{3})dx/y^2$ and $(y + 1 - \sqrt{3})dx/y^2$, respectively. The image of each is a holomorphic differential on the quotient genus 1 curve. Let $d\psi$ be the induced map on tangent spaces at the origin. Showing that ψ is an isogeny is equivalent to showing that $d\psi$ is an isomorphism. This, in turn, is equivalent to showing that the map on cotangent spaces is an isomorphism. The differentials dx/y^2, xdx/y^2 and dx/y form a well-known basis for the space of holomorphic differentials on C. So it is clear that the three previous differentials are linearly independent and this provides the isomorphism and proves the following proposition.

PROPOSITION 5.1. *The map ψ is an isogeny from J to the product of three CM elliptic curves. This isogeny is defined over $\mathbb{Q}(\sqrt{3})$.*

Remark. The characteristic polynomial of the Frobenius for J over $\mathbb{F}_5$ factors into irreducible quadratic and quartic factors. So over $\mathbb{Q}$, there is no isogeny from J to the product of three elliptic curves.

We now describe the kernel of ψ. Since each of the maps from C to a genus 1 curve has degree 2, the kernel of ψ is contained in $J[2]$. The group $J[2]$ has dimension 6 as an $\mathbb{F}_2$ vector space. In [KS, Prop. 4.2] the authors show that every element of $J[2]$ is of the form $[P_i + Q_i + P_j + Q_j - 4\infty]$ such that $L_i.C = 2P_i + 2Q_i$ and $L_j.C = 2P_j + 2Q_j$ for some lines L_i and L_j and points P_i, Q_i, P_j, and Q_j. Such lines are called *bitangents* of C. If $P_i = Q_i$ then P_i is a hyperflex. From [H, p. 305], any smooth plane quartic curve has exactly 28 bitangents. For a nice discussion of the configuration of the bitangents and relations to symplectic geometry over $\mathbb{F}_2$, see [V, Chap. 1, Sect. 2–3]. We can find the bitangents other than $Z = 0$ by simultaneously solving $y^3 = x^4 - 1$ and $y = mx + b$ and forcing the resulting quartic in x to be the square of a quadratic. By doing so one finds the bitangents of the form $y = -\alpha$, which give us hyperflexes on the curve, and $y = mx + b$ where $b^3 = -(10 \pm 6\sqrt{3})$ and $m^4 = -9b^4/(1 + b^3)$, which do not. To be more explicit we have $b = -(1 \pm \sqrt{3})\alpha$ and $m = \beta b \sqrt[4]{-3 \pm 2\sqrt{3}}$, where the two $\pm$ must agree.

The 2-torsion subgroup of J is spanned by the divisor classes $[P_i + Q_i - 2\infty]$. Some subset of them forms a basis for $J[2]$. By reducing modulo 61, we found that all of the points of intersection of the bitangents with the curve are rational over $\mathbb{F}_{61}$; so we worked there to find a basis. There are many conics whose intersection divisors with C are the eight points of intersection of C with four bitangents. Using these conics, we found relations among the divisor classes $[P_i + Q_i - 2\infty]$ and thus reduced the spanning set to a basis. By lifting we get the basis presented below. The choices of roots in the following two propositions are inconsequential.

PROPOSITION 5.2. *Fix r to be some fourth root of $-3+2\sqrt{3}$. Let $b_1 = -(1+\sqrt{3})$, $b_2 = -\zeta_3(1+\sqrt{3})$ and $i^2 = -1$. Let $L_1, \ldots, L_6$ be the six lines given by $y = -1$, $y = -\zeta_3$, $y = b_1 r x + b_1$, $y = i b_1 r x + b_1$, $y = b_2 r x + b_2$, and $y = i b_2 r x + b_2$ respectively. Then the six divisor classes $[P_j + Q_j - 2\infty]$ form a basis for $J[2]$.*

To compute the kernel of ψ, we found it easier to work with Weierstrass models of the three elliptic curves. There is an isomorphism from the curve $v^2 = u^4 + k$ to $\eta^2 = \xi^3 - 4k\xi$ given by

$$(\xi, \eta) = (2(v + u^2), 4u(v + u^2)).$$

By finding the image under ψ of each element of the basis given in Proposition 5.2, in the 2-torsion of the product of the three elliptic curves, we determined the kernel of the isogeny.

PROPOSITION 5.3. *The kernel of the isogeny ψ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ and is generated by $[P_1 + Q_1 - 2\infty]$, $[P_2 + Q_2 - 2\infty]$, and $[P_3 + Q_3 + P_4 + Q_4 - 4\infty]$, in the notation of Proposition* 5.2.

6. The fourth Fermat curve. Let F_4 be given by the equation $X^4 + Y^4 = Z^4$ and let $J(F_4)$ be its Jacobian. In [F], Faddeev shows that $J(F_4)(\mathbb{Q}(\zeta_8))$ is finite. We use this result to show that the Weierstrass points form a torsion packet (as defined in Section 3). We define $W(F_4)$ to be the set of Weierstrass points on F_4 which we refer to as flexes, for simplicity. The curve F_4 has 12 hyperflexes. They are of the form $(0 : \beta : 1)$, $(\beta : 0 : 1)$ or $(1 : \gamma : 0)$ where $\gamma^4 = -1$ and $\beta^4 = 1$. Let $f : F_4 \to J(F_4)$ be the Abel–Jacobi map from F_4 to its Jacobian using $(0 : 1 : 1)$ as a basepoint. Lastly, let $T(F_4)$ be the points on F_4 whose images under f are torsion.

PROPOSITION 6.1. $F_4(\mathbb{Q}(\zeta_8)) = W(F_4) = T(F_4)$.

Proof. Since $J(F_4)$ has potential CM (see [F]), we can use Coleman's theorem, stated in Section 3. At the prime 5, $J(F_4)$ has ordinary good reduction. So the number of points on F_4 whose images are torsion is at most 15. Since $J(F_4)(\mathbb{Q}(\zeta_8))$ is finite, the image of each of the 12 flexes under the map f is torsion. The automorphism group of F_4 permutes the flexes. If there were another point on F_4 whose image under f were torsion, then there would be four other points coming from the four images of that point under the automorphisms generated by $(X : Y : Z) \mapsto (iX : Y : Z)$. But $12 + 4 > 15$ so there are no more.

The fact that $F_4(\mathbb{Q}(\zeta_8)) = T(F_4)$ follows immediately from the fact that $J(F_4)(\mathbb{Q}(\zeta_8))$ is finite. ∎

References

[C1] R. Coleman, *Torsion points on curves and p-adic Abelian integrals*, Ann. of Math. 121 (1985), 111–168.

[C2] —, *Torsion points on Abelian etale coverings of* $\mathbf{P}^1 - \{0, 1, \infty\}$, Trans. Amer. Math. Soc. 311 (1989), 185–208.

[F] D. K. Faddeev, *Group of divisor classes on the curve defined by the equation* $x^4 + y^4 = 1$, Soviet Math. Dokl. 1 (1960), 1149–1151.

[H] R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.

[KS] M. J. Klassen and E. F. Schaefer, *Group law and descent on smooth plane quartics*, preprint.

[L] J. Lewittes, *Automorphisms of compact Riemann surfaces*, Amer. J. Math. 85 (1963), 734–752.

[Ma] A. Mattuck, *Abelian varieties over p-adic ground fields*, Ann. of Math. 62 (1955), 92–119.

[Mi] J. S. Milne, *Jacobian varieties*, in: Arithmetic Geometry, G. Cornell and J. H. Silverman (eds.), Springer, New York, 1986, 167–212.

[V] A. M. Vermeulen, *Weierstrass points of weight two on curves of genus three*, Ph.D. Thesis, University of Amsterdam, 1983.

DEPARTMENT OF MATHEMATICS
SANTA CLARA UNIVERSITY
SANTA CLARA, CALIFORNIA 95053
U.S.A.
E-mail: KLASSEMA@PLU.EDU
ESCHAEFER@SCUACC.SCU.EDU

Received on 20.4.1995
and in revised form on 16.6.1995 (2775)