PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 129, Number 6, Pages 1647–1657
S 0002-9939(00)05887-1
Article electronically published on November 21, 2000

PLANE QUARTICS WITH JACOBIANS ISOMORPHIC TO A HYPERELLIPTIC JACOBIAN

EVERETT W. HOWE

(Communicated by Ron Donagi)

ABSTRACT. We show how for every integer n one can explicitly construct n distinct plane quartics and one hyperelliptic curve over $\mathbf{C}$ all of whose Jacobians are isomorphic to one another as abelian varieties without polarization. When we say that the curves can be constructed "explicitly", we mean that the coefficients of the defining equations of the curves are simple rational expressions in algebraic numbers in $\mathbf{R}$ whose minimal polynomials over $\mathbf{Q}$ can be given exactly and whose decimal approximations can be given to as many places as is necessary to distinguish them from their conjugates. We also prove a simply-stated theorem that allows one to decide whether or not two plane quartics over $\mathbf{C}$, each with a pair of commuting involutions, are isomorphic to one another.

1. INTRODUCTION

Torelli's theorem states that a curve is determined by its polarized Jacobian variety, but a century ago Humbert showed that distinct curves can have isomorphic unpolarized Jacobian varieties; thus it is natural to wonder exactly how much information about a curve is contained in its unpolarized Jacobian. In this paper we will prove that in general one cannot determine whether or not a curve over the complex numbers is hyperelliptic simply by looking at its unpolarized Jacobian. In fact, we will prove somewhat more: We will show how for every positive integer n one can explicitly construct n distinct plane quartics and one hyperelliptic curve of genus 3 such that all $n+1$ of these curves share the same unpolarized Jacobian. Our construction is apparently the first method of producing explicit exact equations for curves of genus 3 over $\mathbf{C}$ with isomorphic Jacobians. In order to state our theorem precisely, we must set some notation.

For every complex number α with $\alpha^2 \notin \{0,1\}$, we let $H(\alpha)$ denote the normalization of the curve defined by

$$V^2 = (U^2+1)^4 - 16\alpha^2U^2(U^2-1)^2.$$

The discriminant of the right-hand side of this equation is the nonzero number $2^{60}\alpha^{12}(\alpha^2-1)^4$, so $H(\alpha)$ is hyperelliptic of genus 3. For every pair of complex numbers (α,β) with $\alpha^2 \notin \{0,1\}$ and $\beta^2 \notin \{1,\alpha^2\}$, we let $C(\alpha,\beta)$ denote the plane

Received by the editors December 1, 1998 and, in revised form, October 9, 1999.
2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 14H45.
Key words and phrases. Curve, Jacobian, polarization, Torelli, quartic.

quartic curve defined by the homogeneous equation

$$X^4 + Y^4 + Z^4 + \left(-2 + 4\frac{1-\beta^2}{1-\alpha^2}\right) X^2Y^2 + \left(\frac{2\beta}{\alpha}\right) X^2Z^2 + \left(\frac{2\beta}{\alpha}\right) Y^2Z^2 = 0.$$

A computation shows that $C(\alpha, \beta)$ is nonsingular. Finally, for every positive real x we let $\mu(x)$ denote the unique $\mu \in \mathbf{R}$ such that $0 \le \mu < 1$ and such that the elliptic curve $Y^2 = (X-1)(X-\mu)(X+1)$ is complex-analytically isomorphic to the torus $\mathbf{C}/(\mathbf{Z} + ix\mathbf{Z})$. One can check that $\mu(x) = \mu(y)$ if and only if either $x = y$ or $xy = 1$, and that $\mu(x) = 0$ if and only if $x = 1$.

Theorem 1. *Let m be a positive even squarefree integer, and for every odd positive divisor d of m let $\alpha_d = \mu(\sqrt{m}/d)$. For every odd divisor $d > 1$ of m the Jacobian of the plane quartic $C(\alpha_1, \alpha_d)$ is isomorphic to the Jacobian of the hyperelliptic curve $H(\alpha_1)$ as an abelian variety without polarization. Furthermore, if d and d' are distinct odd divisors of m that are greater than 1, then $C(\alpha_1, \alpha_d)$ and $C(\alpha_1, \alpha_{d'})$ are not isomorphic to one another.*

Note that the real numbers α_d are distinct and lie strictly between 0 and 1, so the curves $C(\alpha_1, \alpha_d)$ and $H(\alpha_1)$ are defined. Moreover, the α_d can be specified without reference to transcendental functions, because if x^2 is a rational number the number $\mu(x)$ is algebraic and its minimal polynomial over $\mathbf{Q}$ can be calculated. For example, the values of $\mu(x)$ that we must calculate in order to apply the theorem with $m = 30$ are

$$\mu(\sqrt{30}) = -464325 - 328320\sqrt{2} + 268072\sqrt{3} - 207648\sqrt{5} + 189560\sqrt{6} - 146832\sqrt{10} + 119888\sqrt{15} + 84772\sqrt{30},$$

$$\mu(\sqrt{30}/3) = -464325 + 328320\sqrt{2} - 268072\sqrt{3} + 207648\sqrt{5} + 189560\sqrt{6} - 146832\sqrt{10} + 119888\sqrt{15} - 84772\sqrt{30},$$

$$\mu(\sqrt{30}/5) = -464325 + 328320\sqrt{2} - 268072\sqrt{3} - 207648\sqrt{5} + 189560\sqrt{6} + 146832\sqrt{10} - 119888\sqrt{15} + 84772\sqrt{30},$$

$$-\mu(\sqrt{30}/15) = -464325 - 328320\sqrt{2} + 268072\sqrt{3} + 207648\sqrt{5} + 189560\sqrt{6} + 146832\sqrt{10} - 119888\sqrt{15} - 84772\sqrt{30}.$$

Using these values, we find three distinct explicitly-given plane quartics whose Jacobians are all isomorphic to that of an explicitly-given hyperelliptic curve.

For our proof of Theorem 1 we will require a simple method of determining whether two plane quartics, each with a pair of commuting involutions, are isomorphic to one another. We will provide such a method in Section 2. In Section 3 we will review a construction from [9] that allows us to write down explicit equations for genus-3 curves whose Jacobians are isogenous to a product of three given elliptic curves. We will then use this construction to prove Theorem 1 in Sections 4 and 5. Finally, in Section 6 we will indicate how one may compute the minimal polynomials of the algebraic numbers $\mu(\sqrt{m}/d)$ that appear in the statement of Theorem 1.

There are a number of other papers that discuss the relationship between a curve and its unpolarized Jacobian. The fact that a curve is not determined by its unpolarized Jacobian was first observed by Humbert [10], who exhibited the period matrices for pairs of genus-2 curves over $\mathbf{C}$ with isomorphic Jacobians. The Jacobians of Humbert's curves are reducible, and Hayashida and Nishi [6, 5] showed that in fact there exist arbitrarily large sets of genus-2 curves over $\mathbf{C}$ all sharing the same reducible Jacobian. A method for producing explicit equations for the curves in such sets was given in [8]. There also exist *simple* abelian varieties over $\mathbf{C}$ of dimension 2, 3, and 4 that can be obtained in more than one way as the Jacobian of a curve (see Lange [14] for dimensions 2 and 3, and Ciliberto and van der Geer [3] for dimension 4). No explicit examples of the equations for curves giving rise

to such Jacobians are known; however, it should be possible to use the methods of van Wamelen [17, 18] to produce examples of genus 2. Over finite fields, explicit examples of distinct curves of genus 2 and 3 sharing the same reducible Jacobian can be obtained by using results of Ibukiyama, Katsura, and Oort [11] and Brock [1] or by reducing the examples in [8], and a method for producing explicit examples of distinct curves of genus 2 and 3 sharing the same irreducible Jacobian is given in [7]. The genus-3 example worked out in [7] consists of a hyperelliptic curve and a plane quartic over $\mathbf{F}_3$ with isomorphic Jacobians.

In a forthcoming paper we will explicitly construct a non-constant one-parameter family $C(t)$ of plane quartics and a non-constant one-parameter family $H(t)$ of hyperelliptic curves such that the Jacobians of $C(t)$ and $H(t)$ are isomorphic for all values of t for which the curves are nonsingular.

2. Detecting isomorphisms between plane quartics with commuting involutions

Fix a set of homogeneous coordinates X, Y, Z for $\mathbf{P}^2$, and for every triple (a, b, c) of complex numbers let $Q(a, b, c)$ denote plane quartic defined by

$$X^4 + Y^4 + Z^4 + aX^2Y^2 + bX^2Z^2 + cY^2Z^2 = 0.$$

The curve $Q(a, b, c)$ is nonsingular if and only if $a^2 + b^2 + c^2 - abc - 4$ is nonzero and none of a^2, b^2, and c^2 is equal to 4. Our goal in this section is to give a simple criterion for deciding whether two nonsingular curves $Q(a, b, c)$ and $Q(a', b', c')$ are isomorphic to one another.

The embedding of $Q(a, b, c)$ into $\mathbf{P}^2$ given by its defining equation is a canonical embedding, so every isomorphism φ from $Q(a, b, c)$ to $Q(a', b', c')$ can be extended to give an automorphism $\varphi_{\mathbf{P}^2}$ of the ambient $\mathbf{P}^2$ that takes $Q(a, b, c)$ to $Q(a', b', c')$. Using our fixed set of homogeneous coordinates, we can identify $\operatorname{Aut} \mathbf{P}^2$ with $\mathrm{PGL}(3, \mathbf{C})$, so $\varphi_{\mathbf{P}^2}$ can be represented by a 3×3 matrix, unique up to scalar multiples. We say that an isomorphism $\varphi\colon Q(a, b, c) \to Q(a', b', c')$ is *strict* if $\varphi_{\mathbf{P}^2}$ has a representative that is the product of a permutation matrix and a diagonal matrix. It is easy to see that $Q(a', b', c')$ is strictly isomorphic to $Q(a, b, c)$ if and only if the triple (a', b', c') can be obtained from (a, b, c) by permuting the order of the elements and changing the signs of an even number of elements.

Proposition 2. *An isomorphism class of nonsingular quartics of the form $Q(a', b', c')$ is equal to one of the following*:

1. *the strict isomorphism class of the curve $Q(a, b, c)$ for some a, b, and c such that a^2, b^2, and c^2 are pairwise unequal*;
2. *the union of the strict isomorphism classes of the curves $Q(a, b, b)$ and $Q(-2+16/(a+2), 2b/d, 2b/d)$ for some a and b with $b \neq 0$, where $d^2 = a+2$; or*
3. *the union of the strict isomorphism classes of the curves $Q(a, 0, 0)$ and $Q(-2 + 16/(a + 2), 0, 0,)$ and $Q(-2 + 16/(-a + 2), 0, 0,)$, for some a.*

A special case of this proposition may be found in Kuribayashi and Sekita [13], but we have been unable to find a proof of the general case in the literature. Brock uses the result of the proposition, without proof, in Chapter 3 of [1].

Our proof of the proposition depends on the following lemma. By a *V_4-subgroup* of a group G, we mean a subgroup of G isomorphic to the Klein 4-group V_4.

Lemma 3. *Let C be a nonhyperelliptic curve of genus 3. The number of strict isomorphism classes of curves $Q(a,b,c)$ that are isomorphic to C is equal to the number of conjugacy classes of V_4-subgroups of* $\operatorname{Aut} C$.

Proof. For every nonsingular curve $Q(a,b,c)$ let $A(a,b,c)$ be the subgroup of $\operatorname{Aut} Q(a,b,c)$ consisting of the automorphisms $[X:Y:Z] \mapsto [\pm X:\pm Y:\pm Z]$, so that $A(a,b,c)$ is isomorphic to V_4. If $\varphi\colon C \to Q(a,b,c)$ is an isomorphism, then $\varphi^* A(a,b,c)$ is a V_4-subgroup of $\operatorname{Aut} C$. If ψ is another isomorphism from C to the same curve $Q(a,b,c)$, then $\psi^* A(a,b,c)$ and $\varphi^* A(a,b,c)$ are conjugate subgroups of $\operatorname{Aut} C$. Furthermore, if $\psi\colon C \to Q(a',b',c')$ is the composition of φ with a strict isomorphism from $Q(a,b,c)$ to $Q(a',b',c')$, then $\varphi^* A(a,b,c) = \psi^* A(a',b',c')$. Thus we get a map Θ from the set of strict isomorphism classes of curves $Q(a,b,c)$ such that $C \cong Q(a,b,c)$ to the set of conjugacy classes of V_4-subgroups of $\operatorname{Aut} C$. We will prove that Θ is a bijection.

The canonical embedding $\Phi\colon C \to \mathbf{P}^2$ allows us to identify $\operatorname{Aut} C$ with a subgroup of $\operatorname{Aut} \mathbf{P}^2$. Suppose A is a V_4-subgroup of $\operatorname{Aut} C$. Since there is a unique embedding of V_4 into $\operatorname{Aut} \mathbf{P}^2$ up to conjugacy, we may choose coordinates X, Y, Z for $\mathbf{P}^2$ so that the image of A in $\operatorname{Aut} \mathbf{P}^2$ consists of the automorphisms $[X:Y:Z] \mapsto [\pm X:\pm Y:\pm Z]$. It is easy to see that with this choice of coordinates for $\mathbf{P}^2$, the image of C under the canonical embedding is a plane quartic defined by a homogeneous quadratic polynomial in X^2, Y^2, and Z^2. By rescaling coordinates, we find that $\Phi(C)$ is defined by a quartic of the form $Q(a,b,c)$ for some a, b, and c. By construction, the isomorphism $\varphi\colon C \to Q(a,b,c)$ obtained in this way pulls back $A(a,b,c)$ to our original group A. Thus Θ is surjective.

On the other hand, suppose $\varphi\colon C \to Q(a,b,c)$ and $\psi\colon C \to Q(a',b',c')$ are isomorphisms such that $\varphi^* A(a,b,c)$ is conjugate to $\psi^* A(a',b',c')$, say by an element $\alpha \in \operatorname{Aut} C$. By replacing ψ with the composition $\psi\alpha$, we may assume that $\varphi^* A(a,b,c)$ is equal to $\psi^* A(a',b',c')$. Let $\chi\colon Q(a,b,c) \to Q(a',b',c')$ be the isomorphism $\psi\varphi^{-1}$. Then the fact that $\chi^* A(a',b',c') = A(a,b,c)$ shows that the element $\chi_{\mathbf{P}^2}$ of $\operatorname{PGL}(3,\mathbf{C})$ can be represented by the product of a permutation matrix and a diagonal matrix. Thus $Q(a',b',c')$ is strictly isomorphic to $Q(a,b,c)$, so Θ is injective. □

Proof of Proposition 2. There are exactly seven groups containing V_4 that occur as automorphism groups of nonhyperelliptic curves of genus 3 over $\mathbf{C}$ (see [12], or Theorem 5.5 of [16], or Theorem 3.5 of [1]). These groups are V_4 itself, the dihedral group D_8 of order 8, the symmetric group S_4, a group G_{16} that is isomorphic to the central product of the quaternion group Q_8 with the cyclic group C_4 (that is, the quotient of the product $Q_8 \times C_4$ by the image of a central diagonal embedding of C_2), a group G_{48} that is isomorphic to the semidirect product of G_{16} with C_3 (where the C_3 acts in the obvious way on the quaternion group), a group G_{96} that is isomorphic to the semidirect product of the trace-0 part of $(\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z})$ with S_3 (where S_3 acts by permuting the factors), and the simple group $\operatorname{GL}(3,\mathbf{F}_2)$ of order 168.

For each of these groups G we can calculate the number N of conjugacy classes of V_4-subgroups of G. We leave these straightforward calculations to the reader; the results are presented in the first two columns of Table 1. For every automorphism group G, Vermeulen ([16], Table 5.6, pp. 63–64) lists a standard way of writing the curves with that automorphism group. For all groups in Table 1 except for D_8 and $\operatorname{GL}(3,\mathbf{F}_2)$ we list Vermeulen's standard form in column 3. For D_8 we list

G	N	Standard form	Associated form(s)
V_4	1	$Q(a,b,c)$	none
D_8	2	$Q(a,b,b)$	$Q(-2+16/(a+2), 2b/d, 2b/d)$ (where $d^2 = a+2$)
S_4	2	$Q(a,a,a)$	$Q(-2+16/(a+2), 2a/d, 2a/d)$ (where $d^2 = a+2$)
G_{16}	3	$Q(a,0,0)$	$Q(-2+16/(a+2), 0, 0)$ $Q(-2+16/(-a+2), 0, 0)$
G_{48}	1	$Q(2\sqrt{-3}, 0, 0)$	none
G_{96}	2	$Q(0,0,0)$	$Q(6,0,0)$
$\mathrm{GL}(3, \mathbf{F}_2)$	2	$Q(z,z,z)$	$Q(\overline{z}, \overline{z}, \overline{z})$

TABLE 1. Forms of curves with automorphism groups containing commuting involutions. For every possible automorphism group G that contains a V_4-subgroup we list the number N of conjugacy classes of such subgroups. Every curve C with $G \subseteq \operatorname{Aut} C$ can be put in the standard form $Q(\cdot,\cdot,\cdot)$ listed in the third column. If $Q(a,b,c)$ has automorphism group G, then the $N-1$ other strict isomorphism classes of curves $Q(a',b',c')$ isomorphic to $Q(a,b,c)$ are listed in column 4. The number z in the last row is $z = 3(-1+\sqrt{-7})/2$, and $\overline{z}$ is its complex conjugate.

a standard form easily obtained from Vermeulen's, and for $\mathrm{GL}(3, \mathbf{F}_2)$ we list the form that was apparently first obtained by Ciani [2]. Now, if a curve $Q(a,b,c)$ has automorphism group equal to G, then Lemma 3 says there there will be exactly N strict isomorphism classes of curves $Q(a',b',c')$ isomorphic to $Q(a,b,c)$. One of these classes will be represented by $Q(a,b,c)$ itself. In column 4 we list representatives of the other $N-1$ strict isomorphism classes of curves $Q(a',b',c')$ isomorphic to $Q(a,b,c)$, all of which are obtained by applying Lemma 4 (below) to elements of the strict isomorphism class of $Q(a,b,c)$. The reader may verify that the strict isomorphism classes of these N curves are distinct from one another whenever $Q(a,b,c)$ has automorphism group exactly G.

Proposition 2 follows immediately upon inspection of Table 1. □

Lemma 4. *Suppose $Q(a,b,b)$ is a nonsingular curve. Let $d \in \mathbf{C}$ satisfy $d^2 = a+2$. Then $Q(-2+16/(a+2), 2b/d, 2b/d)$ is isomorphic to $Q(a,b,b)$.*

Proof. Let $e \in \mathbf{C}$ satisfy $e^2 = d$. Then the element of $\operatorname{Aut} \mathbf{P}^2 \cong \mathrm{PGL}(3, \mathbf{C})$ represented by the matrix

$$\begin{pmatrix} e/2 & e/2 & 0 \\ e/2 & -e/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

gives an isomorphism from $Q(a,b,b)$ to $Q(-2+16/(a+2), 2b/d, 2b/d)$. □

3. Constructing curves of genus three with split Jacobians

For our proof that the curves in Theorem 1 have isomorphic Jacobians we will require some results from Section 4.1 of [9] that describe how one can explicitly construct a curve of genus 3 whose Jacobian is $(2,2,2)$-isogenous to the product of three given elliptic curves. We will review these results in this section for the convenience of the reader. Care is taken in [9] to keep track of polarizations and fields of definition, but our arguments in this paper will not involve such subtleties; therefore, for the sake of brevity and simplicity, we will present weakened versions of the relevant results of [9].

Suppose k is an algebraically closed field of characteristic not 2. For $i = 1, 2, 3$, let E_i be an elliptic curve over k given by an equation $y^2 = x(x^2 + A_i x + B_i)$, let Q_i be the 2-torsion point $(0,0)$ of E_i, and let P_i be a nonzero 2-torsion point of E_i other than Q_i. Let A be the abelian variety $E_1 \times E_2 \times E_3$ and let G be the subgroup of A generated by $(Q_1, 0, Q_3)$, $(0, Q_2, Q_3)$, and (P_1, P_2, P_3). The following propositions show how to construct a genus-3 curve over k whose Jacobian is isomorphic to A/G.

To state the propositions we must define some numbers. For each i, we let x_{P_i} denote the x-coordinate of the point P_i, we let $d_i = -(A_i + 2x_{P_i})$, and we let $\Delta_i = d_i^2 = A_i^2 - 4B_i$. Let R be the product $d_1 d_2 d_3$, and let T be the number

$$T = R\left(\frac{A_1^2}{\Delta_1} + \frac{A_2^2}{\Delta_2} + \frac{A_3^2}{\Delta_3} - 1\right) - 2A_1A_2A_3,$$

called the *twisting factor* in [9].

Proposition 5. *If $T = 0$, then A/G is isomorphic to the Jacobian of the hyperelliptic curve defined by the homogeneous equations*

$$W^2Z^2 = aX^4 + bY^4 + cZ^4,$$
$$0 = dX^2 + eY^2 + fZ^2,$$

where a, b, and c are given by

$$a = \left(\frac{RB_1}{2}\right)\left(-\frac{B_1}{\Delta_1} + \frac{B_2}{\Delta_2} + \frac{B_3}{\Delta_3}\right),$$
$$b = \left(\frac{RB_2}{2}\right)\left(\frac{B_1}{\Delta_1} - \frac{B_2}{\Delta_2} + \frac{B_3}{\Delta_3}\right),$$
$$c = \left(\frac{RB_3}{2}\right)\left(\frac{B_1}{\Delta_1} + \frac{B_2}{\Delta_2} - \frac{B_3}{\Delta_3}\right),$$

where d, e, and f are determined up to sign by the relations

$$B_2B_3d^2 = 1,$$
$$B_1B_3e^2 = 1,$$
$$B_1B_2f^2 = 1,$$

and where the signs of d, e, and f are chosen so that we have $A_1 = -aef$ and $A_2 = -bdf$ and $A_3 = -cde$.

Proof. This is a weakening of Proposition 14 of [9]. □

When the twisting factor is nonzero, we find a plane quartic with the desired Jacobian.

Proposition 6. *If $T \neq 0$, then A/G is isomorphic to the Jacobian of the plane quartic defined by*

$$B_1X^4 + B_2Y^4 + B_3Z^4 + dX^2Y^2 + eX^2Z^2 + fY^2Z^2 = 0,$$

where

$$d = \frac{1}{2}\left(-A_1A_2 + \frac{A_3R}{\Delta_3}\right),$$
$$e = \frac{1}{2}\left(-A_1A_3 + \frac{A_2R}{\Delta_2}\right),$$
$$f = \frac{1}{2}\left(-A_2A_3 + \frac{A_1R}{\Delta_1}\right).$$

Proof. This is a weakening of Proposition 15 of [9]. □

With these propositions in hand, we proceed to the proof of Theorem 1.

4. Proof that the curves in Theorem 1 have isomorphic Jacobians

We will present three lemmas that together will prove that $C(\alpha_1, \alpha_d)$ and $H(\alpha_1)$ have isomorphic Jacobians, for all odd divisors $d > 1$ of m. The proofs of the first two lemmas rely on the results of [9] that we presented in the preceding section.

For every odd positive divisor d of m let F_d be the elliptic curve given by $Y^2 = X(X^2 + 2\alpha_d X + \alpha_d^2 - 1)$. Also, let $\beta = 2\alpha_1^2 - 1$ and let F' be the elliptic curve $Y^2 = X(X^2 + 2\beta X + \beta^2 - 1)$. Let S_d, T_d, and U_d be the 2-torsion points on F_d with x-coordinates $-1 - \alpha_d$, 0, and $1 - \alpha_d$, respectively, and let S', T', and U' be the 2-torsion points on F' with x-coordinates $-1 - \beta$, 0, and $1 - \beta$, respectively. For every d, let G_d be the subgroup of $F_d \times F_d \times F'$ generated by $(T_d, 0, T')$, $(0, T_d, T')$, and (S_d, S_d, S').

Lemma 7. *The Jacobian of $H(\alpha_1)$ is isomorphic to $(F_1 \times F_1 \times F')/G_1$.*

Proof. We will find a curve whose Jacobian is isomorphic to $(F_1 \times F_1 \times F')/G_1$ by applying the construction presented in the preceding section. That construction requires that we specify three elliptic curves E_1, E_2, E_3 and 2-torsion points P_i and Q_i on each E_i. We take (E_1, P_1, Q_1) to be (F_1, S_1, T_1), we take (E_2, P_2, Q_2) to be (F_1, S_1, T_1), and we take (E_3, P_3, Q_3) to be (F', S', T'). Note that then the group G of Section 3 is equal to our group G_1.

In the notation of Section 3 we have

$$\begin{aligned} A_1 &= 2\alpha_1, \quad & B_1 &= \alpha_1^2 - 1, \quad & \Delta_1 &= 4, \quad & \text{and } d_1 &= 2, \\ A_2 &= 2\alpha_1, \quad & B_2 &= \alpha_1^2 - 1, \quad & \Delta_2 &= 4, \quad & \text{and } d_2 &= 2, \\ A_3 &= 2\beta, \quad & B_3 &= \beta^2 - 1, \quad & \Delta_3 &= 4, \quad & \text{and } d_3 &= 2, \end{aligned}$$

we have $R = 8$, and the twisting factor T is 0. Applying Proposition 5, we find that $(F_1 \times F_1 \times F')/G_1$ is isomorphic to the Jacobian of the curve defined by

$$W^2 = aX^4 + bY^4 + c,$$
$$0 = dX^2 + eY^2 + f,$$

where

$$\begin{aligned} a &= 4\alpha_1^2(\alpha_1^2-1)^2, & d &= 1/(2\alpha_1(\alpha_1^2-1)),\\ b &= 4\alpha_1^2(\alpha_1^2-1)^2, & e &= 1/(2\alpha_1(\alpha_1^2-1)),\\ c &= -8\alpha_1^2(\alpha_1^2-1)^2(2\alpha_1^2-1), & f &= -1/(\alpha_1^2-1). \end{aligned}$$

But the map from $H(\alpha_1)$ to the curve above given by

$$X = \frac{2\sqrt{2\alpha_1}U}{U^2+1}, \qquad Y = \frac{\sqrt{2\alpha_1}(U^2-1)}{U^2+1}, \qquad W = \frac{(2\sqrt{2})\alpha_1(\alpha_1^2-1)V}{(U^2+1)^2},$$

is an isomorphism, so the lemma is proven. □

Lemma 8. *If d is a divisor of m with $d > 1$, then the Jacobian of $C(\alpha_1, \alpha_d)$ is isomorphic to $(F_d \times F_d \times F')/G_d$.*

Proof. We again use the construction of Section 3. This time we take (E_1, P_1, Q_1) to be (F_d, S_d, T_d), we take (E_2, P_2, Q_2) to be (F_d, S_d, T_d), and we take (E_3, P_3, Q_3) to be (F', S', T'). Now the group G of Section 3 is equal to our group G_d. In the notation of Section 3 we have

$$\begin{aligned} A_1 &= 2\alpha_d, & B_1 &= \alpha_d^2 - 1, & \Delta_1 &= 4, & \text{and } d_1 &= 2,\\ A_2 &= 2\alpha_d, & B_2 &= \alpha_d^2 - 1, & \Delta_2 &= 4, & \text{and } d_2 &= 2,\\ A_3 &= 2\beta, & B_3 &= \beta^2 - 1, & \Delta_3 &= 4, & \text{and } d_3 &= 2, \end{aligned}$$

we have $R = 8$, and the twisting factor T is $8(\beta-1)(\beta-2\alpha_d^2+1)$. We see that T is nonzero, because $\beta = 2\alpha_1^2 - 1 < 1$ and because $\alpha_1 \neq \pm\alpha_d$. We can therefore apply Proposition 6 to find that $(F_d \times F_d \times F')/G_d$ is isomorphic to the Jacobian of the nonsingular plane quartic

$$B_1X^4 + B_2Y^4 + B_3Z^4 + dX^2Y^2 + eX^2Z^2 + fY^2Z^2 = 0$$

where

$$d = 2(1-\alpha_d^2) - 4(1-\alpha_1^2) \qquad \text{and} \qquad e = f = 4\alpha_d(1-\alpha_1^2).$$

If we multiply the equation for the quartic by -1, replace X with $X/(1-\alpha_d^2)^{1/4}$, replace Y with $Y/(1-\alpha_d^2)^{1/4}$, and replace Z with $Z/(1-\beta^2)^{1/4}$, we find that this plane quartic is isomorphic to the curve given by

$$X^4 + Y^4 + Z^4 + d'X^2Y^2 + e'X^2Z^2 + e'Y^2Z^2 = 0,$$

where

$$d' = -2 + 4\frac{1-\alpha_1^2}{1-\alpha_d^2} \qquad \text{and} \qquad e' = -2\frac{\alpha_d}{\alpha_1}\sqrt{\frac{1-\alpha_1^2}{1-\alpha_d^2}}.$$

Finally, by applying Lemma 4 we find that this last curve is isomorphic to $C(\alpha_1, \alpha_d)$. □

Lemma 9. *For every odd positive divisor d of m we have*

$$(F_1 \times F_1 \times F')/G_1 \cong (F_d \times F_d \times F')/G_d$$

as abelian varieties without polarization.

Proof. By shifting X-coordinates by α_1, we see that F_1 is isomorphic to the curve $Y^2 = (X-1)(X-\alpha_1)(X+1)$. Since $\alpha_1 = \mu(\sqrt{m})$, the definition of μ shows that F_1 is complex-analytically isomorphic to the torus $\mathbf{C}/\Lambda_1$, where $\Lambda_1 = \mathbf{Z} + i\sqrt{m}\mathbf{Z}$. This isomorphism is given by sending a point P on F_1 to the image in $\mathbf{Z}/\Lambda_1$ of the integral from ∞ to P of $k\ dX/Y$ for some constant k that is either real or pure imaginary. Since $1/Y$ is pure imaginary for real values of X less than $-1-\alpha_1$ and real for real values of X between $-1-\alpha_1$ and 0, we see that S_1 corresponds to either $1/2+\Lambda_1$ or $i\sqrt{m}/2+\Lambda_1$ and that T_1 corresponds to $(1+i\sqrt{m})/2+\Lambda_1$. Similarly, if we let Λ_d be the lattice $d\mathbf{Z}+i\sqrt{m}\mathbf{Z}$, there is a complex-analytic isomorphism from F_d to $\mathbf{C}/\Lambda_d$ that takes S_d to either $d/2+\Lambda_d$ or $i\sqrt{m}/2+\Lambda_d$ and that takes T_d to $(d+i\sqrt{m})/2+\Lambda_d$.

Let u and v be integers such that $ud+v(m/d)=1$ and such that v is a multiple of 4. One can easily check that the matrix

$$\begin{pmatrix} ud & 2i\sqrt{m} \\ iv\sqrt{m}/2 & d \end{pmatrix}$$

gives an automorphism of $\mathbf{C}\times\mathbf{C}$ that takes $\Lambda_1\times\Lambda_1$ to $\Lambda_d\times\Lambda_d$. Thus, this matrix gives an isomorphism from $(\mathbf{C}/\Lambda_1)\times(\mathbf{C}/\Lambda_1)$ to $(\mathbf{C}/\Lambda_d)\times(\mathbf{C}/\Lambda_d)$, which we may interpret as an isomorphism $\varphi\colon F_1\times F_1 \to F_d\times F_d$. Furthermore, using the matrix interpretation of φ, it is easy to check that $\varphi((T_1,0)) = (T_d,0)$, that $\varphi((0,T_1)) = (0,T_d)$, and that $\varphi((S_1,S_1))$ is either (S_d,S_d) or (U_d,U_d). But then $\varphi\times 1_{F'}$ is an isomorphism from $F_1\times F_1\times F'$ to $F_d\times F_d\times F'$ that takes G_1 to G_d, and we are done. □

5. Proof that the plane quartics in Theorem 1 are distinct

To prove that distinct values of d give us distinct curves $C(\alpha_1,\alpha_d)$, we will need the following lemma.

Lemma 10. *For every odd divisor $d>1$ of m we have $\alpha_1 > \alpha_d$.*

Proof. The j-invariant of the elliptic curve $Y^2=(X-1)(X-\mu)(X+1)$ is

$$2^6(\mu^2+3)^3/(\mu^2-1)^2,$$

and this is an increasing function of μ for $\mu\in[0,1)$. Likewise, the function from $\mathbf{R}_{>0}$ to $\mathbf{R}$ that takes x to the j-invariant of the lattice $\mathbf{Z}+ix\mathbf{Z}$ is increasing for $x\in[1,\infty)$. Thus, the function $\mu\colon \mathbf{R}_{>0}\to\mathbf{R}$ defined in the introduction is increasing for $x\in[1,\infty)$. Suppose $d>1$ is an odd divisor of m, so that $1<d<m$. If $d\le\sqrt{m}$, then $1\le\sqrt{m}/d<\sqrt{m}$ and we have $\mu(\sqrt{m}/d)<\mu(\sqrt{m})$. If $d>\sqrt{m}$, then $1<d/\sqrt{m}<\sqrt{m}$, and by using the fact that $\mu(x)=\mu(1/x)$ we find that $\mu(\sqrt{m}/d)=\mu(d/\sqrt{m})<\mu(\sqrt{m})$. □

Suppose d and d' are divisors of m, each greater than 1, such that $C(\alpha_1,\alpha_d)$ and $C(\alpha_1,\alpha_{d'})$ are isomorphic to one another. Each of these curves is of the form $Q(a,b,b)$ with b nonzero, so we can apply Proposition 2 to find that we must have either

$$\frac{1-\alpha_d^2}{1-\alpha_1^2} = \frac{1-\alpha_{d'}^2}{1-\alpha_1^2} \qquad \text{or} \qquad \left(\frac{1-\alpha_d^2}{1-\alpha_1^2}\right)\left(\frac{1-\alpha_{d'}^2}{1-\alpha_1^2}\right) = 1.$$

The second equality is impossible because Lemma 10 shows that the two factors on the left-hand side are both greater than 1. Thus the first equality holds, and since

the α's are positive we find that $\alpha_d = \alpha_{d'}$ and hence $d = d'$. Thus distinct values of d give distinct curves, and we have proven Theorem 1.

6. Explicitly calculating the equations for the curves

Let m be a positive even squarefree integer, let K be the field $\mathbf{Q}(\sqrt{-m})$, let $\mathfrak{O} = \mathbf{Z}[\sqrt{-m}]$ be the ring of integers of K, and for every odd positive divisor d of m let $\mathfrak{A}_d$ be the ideal $(d, \sqrt{-m})$ of $\mathfrak{O}$. The ideals $\mathfrak{A}_d$ represent distinct 2-torsion elements of the class group of K, and every 2-torsion element is represented by an $\mathfrak{A}_d$. By choosing one of the two embeddings $K \hookrightarrow \mathbf{C}$ we can think of the $\mathfrak{A}_d$ as lattices in $\mathbf{C}$. It is well known that the j-invariants of the lattices $\mathfrak{A}_d$ are conjugate algebraic integers, and by using Algorithm 7.6.1 (p. 408) of [4] we can compute the minimal polynomial $f \in \mathbf{Z}[x]$ of these integers. In fact, since the $\mathfrak{A}_d$ represent the 2-torsion elements of the class group, we see from statement 5.4.3 (p. 124) of [15] that the j-invariants $j(\mathfrak{A}_d)$ are precisely the real roots of f.

Now, the j-invariant of the elliptic curve $Y^2 = (X-1)(X-\mu)(X+1)$ is

$$2^6(\mu^2+3)^3/(\mu^2-1)^2,$$

so the numbers $\alpha_d = \mu(\sqrt{m}/d)$ of Theorem 1 are zeros of the rational function $f\left(2^6(x^2+3)^3/(x^2-1)^2\right)$. Suppose we write this rational function as $g(x)/h(x)$, where g and h are coprime elements of $\mathbf{Z}[x]$ and h is monic. Then $g(\alpha_d) = 0$ for each positive odd divisor d of m, and in fact the α_d are precisely the real roots of g that lie between 0 and 1. Thus we can specify the α_d precisely, by specifying g and by specifying each α_d to enough decimal places to distinguish it from the other α_d's.

Suppose for example that $m = 6$. One calculates (using PARI/GP, for example) that

$$\begin{aligned} g = 2^{12}(x^4 - 36x^2 + 36)(x^4 + 276x^3 + 342x^2 - 396x - 207) \\ \times (x^4 - 276x^3 + 342x^2 + 396x - 207). \end{aligned}$$

The roots of g between 0 and 1 are roots of the last two factors, and we find that

$$\begin{aligned} \mu(\sqrt{6}) &= -69 - 48\sqrt{2} + 40\sqrt{3} + 28\sqrt{6} \approx \quad 0.9854941, \\ -\mu(\sqrt{6}/3) &= -69 + 48\sqrt{2} + 40\sqrt{3} - 28\sqrt{6} \approx -0.4214295 \end{aligned}$$

(where we list $-\mu(\sqrt{6}/3)$ instead of $\mu(\sqrt{6}/3)$ to emphasize the fact that the two given values are conjugate algebraic integers).

Likewise, if we take $m = 30$ we find the values of $\mu(\sqrt{30}/d)$ given in the introduction.

Acknowledgements

The author thanks I. M. Isaacs for providing succinct descriptions for some of the groups appearing in the proof of Proposition 2.

References

[1] B. W. Brock: *Superspecial curves of genera two and three*, doctoral dissertation, Princeton University, 1993.

[2] E. Ciani: I varii tipi possibili di quartiche piane più volte omologico-armoniche, *Rend. Circ. Mat. Palermo* **13** (1899), 347–373.

[3] C. Ciliberto and G. van der Geer: Non-isomorphic curves of genus four with isomorphic (non-polarized) jacobians, pp. 129–133 in: *Classification of Algebraic Varieties* (C. Ciliberto, E. L. Livorni, and A. J. Sommese, eds.), Contemp. Math. **162**, Amer. Math. Soc., Providence, RI, 1994. MR **95d:**14026

[4] H. Cohen: *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. **138**, Springer-Verlag, Berlin, 1993. MR **94i:**11105

[5] T. Hayashida: A class number associated to the product of an elliptic curve with itself, *J. Math. Soc. Japan* **20** (1968), 26–43. MR **38:**2125

[6] T. Hayashida and M. Nishi: Existence of curves of genus two on a product of two elliptic curves, *J. Math. Soc. Japan* **17** (1965), 1–16. MR **34:**1318

[7] E. W. Howe: Constructing distinct curves with isomorphic Jacobians, *J. Number Theory* **56** (1996), 381–390. MR **97d:**11101

[8] E. W. Howe: Constructing distinct curves with isomorphic Jacobians in characteristic zero, *Internat. Math. Res. Notices* **1995**, 173–180. MR **96f:**14030

[9] E. W. Howe, F. Leprévost, and B. Poonen: Large torsion subgroups of split Jacobians of curves of genus two or three, *Forum Math.* **12** (2000), 315–364. CMP 2000:10

[10] G. Humbert: Sur les fonctiones abéliennes singulières (deuxième mémoire), *J. Math. Pures Appl. (5)* **6** (1900), 279–386.

[11] T. Ibukiyama, T. Katsura, and F. Oort: Supersingular curves of genus two and class numbers, *Compositio Math.* **57** (1986), 127–152. MR **87f:**14026

[12] A. Kuribayashi and K. Komiya: On Weierstrass points and automorphisms of curves of genus three, pp. 253–299 in: *Algebraic Geometry: Proceedings, Copenhagen 1978* (K. Lønsted, ed.), Lecture Notes in Math. **732**, Springer, Berlin, 1979. MR **81c:**14016

[13] A. Kuribayashi and E. Sekita: On a family of Riemann surfaces I, *Bull. Fac. Sci. Engrg. Chuo Univ. Ser. I Math.* **22** (1979), 107–139. MR **81i:**14018

[14] H. Lange: Abelian varieties with several principal polarizations, *Duke Math. J.* **55** (1987), 617–628. MR **88i:**14039

[15] G. Shimura: *Introduction to the Arithmetic Theory of Automorphic Functions,* Iwanami Shoten, Publishers, and Princeton University Press, Princeton, NJ, 1971. MR **47:**3318

[16] A. M. Vermeulen: *Weierstrass points of weight two on curves of genus three*, doctoral dissertation, Universiteit van Amsterdam, 1983. MR **84j:**14036

[17] P. van Wamelen: Examples of genus two CM curves defined over the rationals, *Math. Comp.* **68** (1999), 307–320. MR **99c:**11079

[18] P. van Wamelen: Proving that a genus 2 curve has complex multiplication, *Math. Comp.* **68** (1999), 1663–1677. MR **2000a:**14033

Center for Communications Research, 4320 Westerra Court, San Diego, California 92121-1967

E-mail address: however@alumni.caltech.edu

URL: http://alumni.caltech.edu/~however/