Compositio Math. 140 (2004) 581–592
DOI: 10.1112/S0010437X03000757

On the non-existence of certain curves of genus two

Everett W. Howe

Abstract

We prove that if q is a power of an odd prime, then there is no genus-2 curve over $\mathbf{F}_q$ whose Jacobian has characteristic polynomial of Frobenius equal to $x^4+(2-2q)x^2+q^2$. Our proof uses the Brauer relations in a biquadratic extension of $\mathbb{Q}$ to show that every principally polarized abelian surface over $\mathbf{F}_q$ with the given characteristic polynomial splits over $\mathbf{F}_{q^2}$ as a product of polarized elliptic curves.

1. Introduction

Recently, Maisner and Nart [MN02] compiled data on every curve of genus 2 over every finite field of cardinality at most 41. One of the facts they gleaned from analyzing the results of their computation is that for every odd prime power $q \leqslant 41$, there is no genus-2 curve over $\mathbf{F}_q$ that has exactly $q+1$ points over $\mathbf{F}_q$ and exactly q^2-4q+5 points over $\mathbf{F}_{q^2}$. With further computation they verified that the same statement holds for all odd prime powers $q \leqslant 61$, but they were unable to use any of the usual arguments (mentioned below) to explain this observed fact. The purpose of this paper is to provide a new argument that explains Maisner and Nart's observation and that shows that it holds for all odd prime powers q.

Instead of speaking about numbers of rational points, Maisner and Nart expressed their results in terms of the characteristic polynomials of the curves they enumerated. (By the *characteristic polynomial* of a curve we mean the characteristic polynomial of the Frobenius endomorphism of the Jacobian of the curve.) If for every prime power q we let f_q denote the polynomial $x^4+(2-2q)x^2+q^2$, then Maisner and Nart's observation is equivalent to the statement that for every odd prime power $q \leqslant 61$, no genus-2 curve over $\mathbf{F}_q$ has characteristic polynomial f_q. Thus, our main theorem is phrased as follows.

Theorem 1. *Let q be a power of an odd prime. There is no curve of genus 2 over $\mathbf{F}_q$ whose characteristic polynomial is equal to f_q.*

We should mention that when q is a power of 2, it is still true that there is no genus-2 curve over $\mathbf{F}_q$ with characteristic polynomial f_q, but for a trivial reason: Honda–Tate theory [Tat71] shows that if $q > 2$ is a power of 2, there is not even an abelian surface with characteristic polynomial f_q, let alone a Jacobian. The remaining case, $q = 2$, can easily be eliminated by noting that no curve can have exactly three points over $\mathbf{F}_2$ and exactly one point over $\mathbf{F}_4$.

Up until now, there seem to have been four methods of showing that the characteristic polynomial of an abelian surface does not occur as the characteristic polynomial of a genus-2 curve. Two of the methods deal directly with properties of curves.

1) For certain very small q, some characteristic polynomials can be excluded because they would require the associated curve to have a negative number of points, or fewer points over some

Received 9 April 2002, accepted in final form 19 July 2002.
2000 Mathematics Subject Classification Primary 11G20; Secondary 11G10, 11R65, 14G15, 14H25.
Keywords: curve, abelian surface, zeta function, class group, Brauer relations.

extension field than over the base field. (See, for example, [Ruc90, p. 353] and the argument we gave above for the polynomial f_2.)

2) The polynomial $x^4 + (1-2q)x^2 + q^2$ can be excluded because a curve with that characteristic polynomial would have to have an automorphism whose existence is incompatible with the number of rational points on the curve over $\mathbf{F}_{q^2}$. (See the appendix to [MN02].)

The other two methods make use of the close relationship between Jacobians of genus-2 curves and principally polarized abelian surfaces. The Jacobian of a genus-2 curve over $\mathbf{F}_q$ is a principally polarized abelian surface over $\mathbf{F}_q$, and the converse is almost true: an abelian surface over $\mathbf{F}_q$ with a principal polarization is either the Jacobian of a genus-2 curve over $\mathbf{F}_q$ or otherwise is isomorphic (over the algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$) to a product of polarized elliptic curves over $\overline{\mathbf{F}}_q$. So, to show that there is no Jacobian corresponding to a given characteristic polynomial, it suffices to show either that no principally polarized abelian surface has that characteristic polynomial, or that every principally polarized abelian surface with that characteristic polynomial is geometrically split. This leads us to the other two methods.

3) Certain polynomials of the form $x^4 + ax^3 + (a^2 - q)x^2 + aqx + q^2$ can be excluded because the associated abelian surfaces do not have principal polarizations. (See [How95, § 13].)

4) Certain polynomials of the form $x^4+(2c+1)x^3+(c^2+c+2q)x^2+(2c+1)qx+q^2$ that are associated with principally polarized abelian surfaces can be excluded because the endomorphism rings of the surfaces factor as the product of two rings in a way that forces the principally polarized surfaces to split as a product of polarized elliptic curves. (See [MN02, Theorem 3.4].)

Our proof of Theorem 1 uses polarizations, but in contrast to the last two methods it is in essence a counting argument. There are many principally polarized abelian surfaces with characteristic polynomial f_q; we compute exactly how many there are, and we compare this number to the number of geometrically split principally polarized abelian surfaces with characteristic polynomial f_q that we obtain from a simple construction. The first number turns out to be equal to the second, so we conclude that every principally polarized abelian surface with characteristic polynomial f_q splits over the algebraic closure and is hence not a Jacobian.

Lenstra *et al.* [LPP02] gave lower bounds for the number of principally polarized abelian surfaces with characteristic polynomials of a certain form. Our argument is closely related to theirs and, in fact, almost all of the ingredients of our proof of Proposition 2 (below) appear in their paper. The only reason we get an exact formula for the number of principally polarized surfaces with characteristic polynomial f_q, rather than a lower bound along the lines of [LPP02, Proposition 8.2], is that every principally polarized variety we must consider has an endomorphism ring that is Gorenstein. We recommend [LPP02] to those readers who would like to see a more general application of the arguments we give in § 4.

Maisner and Nart [MN02, § 3] raise the question of determining which isogeny classes of simple non-supersingular abelian surfaces contain Jacobians. They note that the only such isogeny classes for which the question is presently unresolved have characteristic polynomials of the form $f = x^4 + (a-2q)x^2 + q^2$ with $0 < a < 4q$, so it is natural to ask whether our argument can be applied to any other polynomials of this form. We can show that our argument also works for the case $a = 1$, but in that case there is a much simpler explanation for why the corresponding f is not the characteristic polynomial of a curve (see the appendix to [MN02]). For every other allowable value of a our argument fails, because it depends (somewhat implicitly) on the ring $\mathbb{Z}[\sqrt{-a}]$ being the full ring of integers of a field of class number one, and this only happens when $a = 1$ or 2. On the other hand, it should be possible to adapt our argument to show that except for these two cases, the characteristic polynomials given above *do* come from curves.

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

In § 2 we give a detailed outline of our proof. In § 3 we prove a technical result about the existence of a well-behaved norm map between two class groups that will be important in our argument. In § 4 we count the number of principally polarized abelian surfaces that have characteristic polynomial f_q, and in § 5 we count the number of these polarized surfaces that split over the quadratic extension of the base field. Finally, in § 6 we show that the two counts are equal, which shows that there is no curve with characteristic polynomial f_q.

2. Outline of the proof

Suppose that D is a positive squarefree integer that is congruent to 1 modulo 4. Let K be the number field $\mathbb{Q}(\sqrt{-2}, \sqrt{-D})$, let K^+ be the maximal real subfield $\mathbb{Q}(\sqrt{2D})$ of K, and let L be the imaginary quadratic subfield $\mathbb{Q}(-D)$ of K. In our notation for these fields we have intentionally suppressed the dependence on D, simply to keep the notation from getting out of hand. The number field K and its subfields will be important to our argument because if A is an abelian surface over $\mathbf{F}_q$ with characteristic polynomial f_q, and if we write $2q-1 = F^2 D$ with D squarefree, then $(\operatorname{End} A)\otimes\mathbb{Q} \cong K$. In fact, the isomorphism can be chosen so that the Frobenius endomorphism on A corresponds to the element $(F\sqrt{2D} + \sqrt{-2})/2$ of K.

Let $\mathcal{O}$ denote the ring of integers $\mathbb{Z}[\sqrt{-2}]$ of $\mathbb{Q}(\sqrt{-2})$ and let w denote the element $(\sqrt{2D} + \sqrt{-2})/2$ of K. For every odd positive integer f, let R_f be the subring $\mathcal{O} + fw\mathcal{O}$ of K, let R_f^+ be the subring $\mathbb{Z}[f\sqrt{2D}]$ of K^+, and let S_f be the subring $\mathbb{Z}[f\sqrt{-D}]$ of L. Note that when $f = 1$, these rings are the maximal orders of their quotient fields. Let U_f denote the group of units of R_f and let U_f^+ denote the group of totally positive units of R_f^+. (Recall that an element x of a number field M is *totally positive* if $\varphi(x) > 0$ for all embeddings $\varphi\colon M \to \mathbb{R}$.)

The *class group* of an order R, denoted $\operatorname{Cl} R$, is the quotient of the group of invertible fractional ideals of R by the subgroup of principal fractional ideals. The *narrow class group* of R, denoted $\operatorname{Cl}^+(R)$, is the quotient of the group of invertible fractional ideals of R by the subgroup of principal ideals that can be generated by a totally positive element of the quotient field of R.

PROPOSITION 2. *Let q be a power of an odd prime and write $2q-1 = F^2 D$, where D is squarefree. The number of principally polarized abelian surfaces (A, λ) over $\mathbf{F}_q$ (up to isomorphism over $\mathbf{F}_q$) such that A has characteristic polynomial f_q is equal to the sum*

$$\sum_{f|F} [U_f^+ : N(U_f)] \frac{\#\operatorname{Cl} R_f}{\#\operatorname{Cl}^+ R_f^+},$$

where N denotes the norm map from K to K^+.

We see that there do exist principally polarized abelian surfaces with characteristic polynomial f_q. The only way that these polarized surfaces could fail to be Jacobians is if they split geometrically as products of polarized elliptic curves. Thus, in order to prove Theorem 1 we must come up with a large enough supply of these split surfaces to account for the surfaces enumerated in Proposition 2. Maisner and Nart note that every abelian surface over $\mathbf{F}_q$ with characteristic polynomial f_q splits up to isogeny over $\mathbf{F}_{q^2}$, so it is natural to try to construct the requisite split surfaces using elliptic curves over $\mathbf{F}_{q^2}$. (In fact, it is *necessary* to use elliptic curves over $\mathbf{F}_{q^2}$, as is shown later by Proposition 10.)

Let g_q be the polynomial $x^2 + (2-2q)x + q^2$, so that $f_q(x) = g_q(x^2)$. The polynomial g_q is the characteristic polynomial of an isogeny class $\mathcal{C}$ of elliptic curves over $\mathbf{F}_{q^2}$. Suppose that E is an elliptic curve in this isogeny class and let $E^{(q)}$ be its Galois conjugate over $\mathbf{F}_q$. Then the product surface $A = E \times E^{(q)}$ has a natural principal polarization λ, namely the product polarization. It is easy to check that the obvious isomorphism $f : (A, \lambda) \to (A, \lambda)^{(q)}$ satisfies $f^{(q)} \circ f = 1$, so we can descend (A, λ) to $\mathbf{F}_q$. Let us denote this geometrically split principally polarized surface over $\mathbf{F}_q$ by $S(E)$. We find that the characteristic polynomial of Frobenius of $S(E)$ is f_q, and it is easy to

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

check that $S(E_1) \cong S(E_2)$ as polarized varieties if and only if either $E_2 \cong E_1$ or $E_2 \cong E_1^{(q)}$. Thus, if the action of $\mathrm{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$ on the isogeny class $\mathcal{C}$ breaks $\mathcal{C}$ into n_1 orbits of size 1 and n_2 orbits of size 2, we construct $n_1 + n_2$ distinct split surfaces with characteristic polynomial f_q in this manner.

Proposition 3. *Let q be a power of an odd prime and write $2q - 1 = F^2 D$, where D is squarefree. The number of elliptic curves over $\mathbf{F}_{q^2}$ with characteristic polynomial g_q is equal to the sum*

$$\sum_{f|F} \#\operatorname{Cl} S_f.$$

None of these curves is isomorphic to its Galois conjugate over $\mathbf{F}_q$, unless $D = 1$, in which case exactly one of the curves is isomorphic to its conjugate.

Let ε denote the function on the integers such that $\varepsilon(x) = 1$ if $x = 1$ and $\varepsilon(x) = 0$ otherwise. Proposition 3 shows that the number of split surfaces obtained from $\mathcal{C}$ is equal to

$$\frac{1}{2}\left(\varepsilon(D) + \sum_{f|F} \#\operatorname{Cl} S_f\right) = \sum_{f|F} \frac{\varepsilon(fD) + \#\operatorname{Cl} S_f}{2}.$$

We complete the proof of Theorem 1 by proving a purely number-theoretic result about class groups, based on the Brauer class-number relations for the extension $K/\mathbb{Q}$.

Proposition 4. *Let D be a positive squarefree integer that is congruent to 1 modulo 4 and let f be an odd positive integer. Then*

$$[U_f^+ : N(U_f)] \frac{\#\operatorname{Cl} R_f}{\#\operatorname{Cl}^+ R_f^+} = \frac{\varepsilon(fD) + \#\operatorname{Cl} S_f}{2}.$$

We prove Propositions 2, 3, and 4 in the following sections. Together with the discussion above, they provide a proof of Theorem 1.

3. The norm map on class groups

In the course of our arguments, we need to know that there is a norm map from the class group of R_f to the narrow class group of R_f^+, and that this norm map is surjective. We prove these facts in this section.

If T is an order in a number field, we let $I(T)$ denote the group of invertible fractional T-ideals. Note that $R_f = R_f^+[(\sqrt{-2} + f\sqrt{2D})/2]$ so that R_f is flat over R_f^+; it follows that the tensoring-with-R_f map from $I(R_f^+)$ to $I(R_f)$ is an injection. If $\mathfrak{A}$ is an ideal of R_f, we let $\overline{\mathfrak{A}}$ denote its complex conjugate.

Lemma 5. *Suppose that $\mathfrak{A} \in I(R_f)$. Then $\mathfrak{A}\overline{\mathfrak{A}} \in I(R_f)$ lies in the image of $I(R_f^+)$.*

Proof. Let $\operatorname{Tor} I(R_f)$ denote the torsion subgroup of $I(R_f)$. A result of Dedekind [Ded77], as reinterpreted by Sands [San91], states that the tensoring-with-R_1 map $I(R_f) \to I(R_1)$ is surjective and has kernel $\operatorname{Tor} I(R_f)$. In other words, there is an exact sequence

$$0 \to \operatorname{Tor} I(R_f) \to I(R_f) \to I(R_1) \to 0,$$

where the second map is inclusion and the third is tensoring-with-R_1. Likewise, we have a sequence

$$0 \to \operatorname{Tor} I(R_f^+) \to I(R_f^+) \to I(R_1^+) \to 0.$$

Let $\mathfrak{B}$ be the image of $\mathfrak{A}$ in $I(R_1)$. Then the usual theory of ideals in number fields shows that there is an ideal $\mathfrak{C} \in I(R_1^+)$ such that the image of $\mathfrak{C}$ in $I(R_1)$ is equal to $\mathfrak{B}\overline{\mathfrak{B}}$. Let $\mathfrak{D}$ be an element of $I(R_f^+)$ that maps to $\mathfrak{C}$. Let $\mathfrak{E} = \mathfrak{A}\overline{\mathfrak{A}}\mathfrak{D}^{-1} \in I(R_f)$. Then $\mathfrak{E}$ maps to the identity of $I(R_1)$, and hence lies in $\operatorname{Tor} I(R_f)$. We will be done if we can show that $\mathfrak{E}$ lies in the image of $\operatorname{Tor} I(R_f^+)$.

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

Let $\mathfrak{f} = fR_1$. Note that $\mathfrak{f}$ is an ideal of R_1 and of R_f. Sands shows that

$$\operatorname{Tor} I(R_f) \cong (R_1 \bmod \mathfrak{f})^*/(R_f \bmod \mathfrak{f})^*.$$

Similarly, if we let $\mathfrak{f}^+ = fR_1^+$, then

$$\operatorname{Tor} I(R_f^+) \cong (R_1^+ \bmod \mathfrak{f}^+)^*/(R_f^+ \bmod \mathfrak{f}^+)^*.$$

If we apply Galois cohomology to the sequence

$$0 \to (R_f \bmod \mathfrak{f})^* \to (R_1 \bmod \mathfrak{f})^* \to \operatorname{Tor} I(R_f) \to 0$$

and note that

$$H^1(\operatorname{Gal}(K/K^+), (R_f \bmod \mathfrak{f})^*) = H^1(\operatorname{Gal}(\mathbb{Q}(\sqrt{-2})/\mathbb{Q}), (\mathcal{O} \bmod f\mathcal{O})^*) = 0,$$

we see that every element of $\operatorname{Tor} I(R_f)$ fixed by conjugation is represented by an element of $(R_1 \bmod \mathfrak{f})^*$ that is fixed by conjugation. In particular, $\mathfrak{E}$ is represented by an element of $(R_1 \bmod \mathfrak{f})^*$ that is fixed by conjugation. However, every such element comes from $(R_1^+ \bmod \mathfrak{f}^+)^*$ because f is odd. Thus, $\mathfrak{E}$ lies in the image of $\operatorname{Tor} I(R_f^+)$, and we are done. □

Lemma 5 shows that the map $\mathfrak{A} \mapsto \mathfrak{A}\overline{\mathfrak{A}}$ can be viewed as a map from $I(R_f)$ to $I(R_f^+)$. Piecing this map together with the norm maps on $I(R_1)$ and $(R_1 \bmod \mathfrak{f})^*$, we obtain the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Tor} I(R_f) & \longrightarrow & I(R_f) & \longrightarrow & I(R_1) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \operatorname{Tor} I(R_f^+) & \longrightarrow & I(R_f^+) & \longrightarrow & I(R_1^+) & \longrightarrow & 0 \end{array}$$

This diagram gives us the following diagram of class groups, in which the vertical arrows are norm maps.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D_f & \longrightarrow & \operatorname{Cl} R_f & \longrightarrow & \operatorname{Cl} R_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & D_f^+ & \longrightarrow & \operatorname{Cl}^+ R_f^+ & \longrightarrow & \operatorname{Cl}^+ R_1^+ & \longrightarrow & 0 \end{array} \tag{1}$$

Here we have set

$$\begin{aligned} D_f &= \operatorname{Tor} I(R_f)/(U_1 \bmod \mathfrak{f}) \\ &= (R_1 \bmod \mathfrak{f})^*/((R_f \bmod \mathfrak{f})^* \cdot (U_1 \bmod \mathfrak{f})) \end{aligned}$$

and

$$\begin{aligned} D_f^+ &= \operatorname{Tor} I(R_f^+)/(U_1^+ \bmod \mathfrak{f}^+) \\ &= (R_1^+ \bmod \mathfrak{f}^+)^*/((R_f^+ \bmod \mathfrak{f}^+)^* \cdot (U_1^+ \bmod \mathfrak{f}^+)). \end{aligned}$$

We will have call to use the following basic fact about the norm from $\operatorname{Cl} R_f$ to $\operatorname{Cl}^+ R_f^+$.

LEMMA 6. *The norm map $\operatorname{Cl} R_f \to \operatorname{Cl}^+ R_f^+$ is surjective.*

Proof. Note that the prime 2 of $\mathbb{Q}$ is totally ramified in the extension $K/\mathbb{Q}$, so the field extension K/K^+ is ramified at a finite prime. It follows from class field theory that $\operatorname{Cl} R_1 \to \operatorname{Cl}^+ R_1^+$ is surjective; see [How95, Proposition 10.1], for example. Next, note that the norm map from $(R_1 \bmod \mathfrak{f})^*$ to $(R_1^+ \bmod \mathfrak{f}^+)^*$ is surjective, so that the norm from D_f to D_f^+ is also surjective. Then we see from diagram (1) that the norm map $\operatorname{Cl} R_1 \to \operatorname{Cl}^+ R_1^+$ is surjective as well. □

Remark. The existence of a norm map $\operatorname{Cl} R \to \operatorname{Cl}^+ R^+$ is proven at the beginning of § 6 of [LPP02] through an identification of the class groups with certain quotients of profinite groups.

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

4. The number of principally polarized surfaces

We make heavy use of Deligne's equivalence of categories (see [Del69]) between the category of ordinary abelian varieties over $\mathbf{F}_q$ and a certain category of modules, called *Deligne modules* in [How95]. Deligne's category equivalence was expanded upon in [How95], so that several geometric notions were translated into the category of Deligne modules. In particular, there is a notion of a polarization of a Deligne module. We will count principally polarized abelian surfaces in the isogeny class determined by f_q by counting principally polarized Deligne modules in the isogeny class determined by f_q.

We begin by reviewing the concepts of [How95]. However, we will simplify matters by restricting our discussion to Deligne modules associated to irreducible polynomials. Thus, the definitions we give below are not identical to those found in [How95], but are equivalent to the original definitions in our special case.

Let q be a power of a prime p. An *ordinary Weil q-polynomial* is a monic polynomial in $\mathbb{Z}[x]$ of even degree whose middle coefficient is coprime to q and all of whose roots in the complex numbers have magnitude $\sqrt{q}$. (For example, f_q is an ordinary Weil q-polynomial, and g_q is an ordinary Weil q^2-polynomial.) Suppose that f is an irreducible ordinary Weil q-polynomial. Let K be the number field $\mathbb{Q}[x]/(f)$, let π be the image of x in K, and let $\overline{\pi} = q/\pi$. The number field K is a totally imaginary quadratic extension of a totally real field K^+, and $\overline{\pi}$ is the complex conjugate of π. Let R be the order $\mathbb{Z}[\pi, \overline{\pi}]$ of K. A *Deligne module* associated to f is a finitely-generated non-zero sub-R-module of K. A *morphism* from a Deligne module $\mathfrak{A}$ to a Deligne module $\mathfrak{B}$ is an element α of K such that $\alpha\mathfrak{A} \subseteq \mathfrak{B}$. An *isogeny* is a non-zero morphism. The *degree* of an isogeny $\alpha : \mathfrak{A} \to \mathfrak{B}$ is the index of $\alpha\mathfrak{A}$ in $\mathfrak{B}$.

The *dual* $\hat{\mathfrak{A}}$ of a Deligne module $\mathfrak{A}$ is the complex conjugate of the dual of $\mathfrak{A}$ under the trace pairing. Suppose we pick, once and for all, a p-adic valuation ν on the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Choose a totally imaginary element ι of K with the property that for every embedding $\varphi : K \to \mathbb{C}$ with $\nu(\varphi(\pi)) > 0$ the real number $\varphi(\iota)/i$ is positive. A *polarization* of a Deligne module $\mathfrak{A}$ is an isogeny from $\mathfrak{A}$ to $\hat{\mathfrak{A}}$ of the form $\iota\alpha$, where α is a totally positive element of the field K^+. A polarization is *principal* if it is an isomorphism.

Part of the main result of [How95, § 4] is that Deligne's equivalence of categories from the category of abelian varieties over $\mathbf{F}_q$ with characteristic polynomial f to the category of Deligne modules associated to f takes isogenies to isogenies, dual varieties to dual modules, and polarizations to polarizations. Thus, to count principally polarized varieties in the isogeny class determined by f, it is sufficient to count principally polarized Deligne modules associated to f.

So, suppose that $\mathfrak{A}$ is a principally polarized Deligne module associated to f_q. Let $A = \operatorname{End}\mathfrak{A}$. Since a lattice and its trace dual have the same endomorphism ring, we see that $\operatorname{End}\hat{\mathfrak{A}}$ is the complex conjugate of $\operatorname{End}\mathfrak{A}$. Since $\mathfrak{A}$ is supposed to be isomorphic to $\hat{\mathfrak{A}}$, we see that A is stable under complex conjugation. We also know that $A \supseteq R = \mathbb{Z}[\pi, \overline{\pi}]$, and since π can be taken to be $(F\sqrt{2D} + \sqrt{-2})/2$ we see that A contains $\pi - \overline{\pi} = \sqrt{-2}$. Thus A contains $\mathcal{O}$. It follows that $A = \mathcal{O} \oplus wI$ for some ideal I of $\mathcal{O}$, and since A is stable under complex conjugation we must have $I = \overline{I}$. Thus, either $I = f\mathcal{O}$ for an integer f, or $I = f\sqrt{-2}\mathcal{O}$ for an integer f. However, A contains $\pi = (1 - F)\sqrt{-2}/2 + Fw$, and since F is odd we see that we cannot have $I = f\sqrt{-2}\mathcal{O}$. It follows that $I = f\mathcal{O}$ for some divisor of F; in other words, $A = R_f$ for some divisor f of F.

First we count the number of Deligne modules with endomorphism ring equal to R_f.

Lemma 7. *Let f be a divisor of F. The number of isomorphism classes of Deligne modules $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R_f$ is equal to $\#\operatorname{Cl} R_f$.*

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

Proof. First, we note that R_f is a Gorenstein ring because it is a complete intersection over $\mathbb{Z}$. (In fact, R_f is the quotient of $\mathbb{Z}[x,y]$ by the ideal generated by the regular sequence $(x^2+2, y^2 - fxy - f^2(D+1)/2)$, the image of x being $\sqrt{-2}$ and the image of y being fw.) Since R_f is Gorenstein, every fractional R_f-ideal $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R_f$ is actually an invertible R_f-ideal. Thus, the number of isomorphism classes of Deligne modules $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R_f$ is equal to $\#\operatorname{Cl} R_f$. □

Next, we give a method for deciding which elements of $\operatorname{Cl} R_f$ give Deligne modules that admit principal polarizations.

LEMMA 8. *Let f be a divisor of F. A Deligne module $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R_f$ has a principal polarization if and only if its class in $\operatorname{Cl} R_f$ lies in the kernel of the norm map from $\operatorname{Cl} R_f$ to $\operatorname{Cl}^+ R_f^+$. The number of isomorphism classes of Deligne modules $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R_f$ that have a principal polarization is equal to the quotient*

$$\frac{\#\operatorname{Cl} R_f}{\#\operatorname{Cl}^+ R_f^+}.$$

Proof. Before we discuss polarizations, we must pick an appropriate totally imaginary element ι of K, which requires that we pick a p-adic valuation ν on the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. To pick ν, we pick our favorite embedding φ of K into $\mathbb{C}$, pick a prime $\mathfrak{p}$ of K containing π, and choose ν to be any valuation that extends the $\mathfrak{p}$-adic valuation on $\varphi(K)$. Now the condition on ι is that $\varphi(\iota)/i$ should be positive and that $\varphi(\iota^\sigma/\iota)$ should be positive for every $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ such that $\pi^\sigma \in \mathfrak{p}$. Since $\pi^2 \in \mathbb{Q}(\sqrt{-D})$, these σ are precisely the automorphisms that fix $\mathbb{Q}(\sqrt{-D})$. Thus we can pick $\iota = \pm 1/(4\sqrt{-D})$, with the sign chosen so that $\varphi(\iota)/i$ is positive.

Suppose $\mathfrak{A}$ is a Deligne module with $\operatorname{End}\mathfrak{A} = R_f$. How can we tell whether $\mathfrak{A}$ has a principal polarization? First we note that the different of the order R_f is $4f\sqrt{-D}$, so the trace dual of $\mathfrak{A}$ is $\mathfrak{A}^{-1}/(4f\sqrt{-D})$. It follows that $\hat{\mathfrak{A}} = \overline{\mathfrak{A}}^{-1}/(4f\sqrt{-D})$. Then $\mathfrak{A}$ has a principal polarization if and only if there is a totally positive element α of K^+ such that

$$\alpha\iota\mathfrak{A} = \hat{\mathfrak{A}} = \overline{\mathfrak{A}}^{-1}/(4f\sqrt{-D}),$$

which is equivalent to

$$\mathfrak{A}\overline{\mathfrak{A}} = \left(\frac{1}{f\alpha}\right) R_f.$$

As the results of § 3 show, this last condition is equivalent to the condition that the class of $\mathfrak{A}$ in $\operatorname{Cl} R_f$ be in the kernel of the norm map from $\operatorname{Cl} R_f$ to $\operatorname{Cl}^+ R_f^+$. This proves the first statement of the lemma.

The second statement of the lemma follows immediately from the first because Lemma 6 states that the norm from $\operatorname{Cl} R_f$ to $\operatorname{Cl}^+ R_f^+$ is surjective. □

Finally, we count how many principal polarizations a Deligne module has, given that it has at least one.

LEMMA 9. *Let f be a divisor of F, and suppose $\mathfrak{A}$ is a Deligne module with $\operatorname{End}\mathfrak{A} = R_f$ that has a principal polarization. Then the number of non-isomorphic principal polarizations on $\mathfrak{A}$ is equal to $[U_f^+ : N(U_f)]$, where $N\colon U_f \to U_f^+$ is the norm map from the units of R_f to the totally positive units of R_f^+.*

Proof. Let λ be a principal polarization of $\mathfrak{A}$. Then the map $u \mapsto u\lambda$ gives a bijection between the totally positive units of R_f^+ and the principal polarizations of $\mathfrak{A}$. On the other hand, if μ_1 and μ_2

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

are principal polarizations of $\mathfrak{A}$, then $(\mathfrak{A}, \mu_1)$ and $(\mathfrak{A}, \mu_2)$ are isomorphic polarized Deligne modules if and only if there is a unit u of R_f such that $\mu_1 = u\overline{u}\mu_2$. Thus, the isomorphism classes of principal polarizations of $\mathfrak{A}$ correspond to the elements of the group $U_f^+/N(U_f)$. □

Together, Lemmas 7, 8, and 9 prove Proposition 2.

5. The number of surfaces coming from elliptic curves

In this section we count the number of elliptic curves over $\mathbf{F}_{q^2}$ in the isogeny class $\mathcal{C}$ determined by $g_q = x^2 + (2-2q)x + q^2$, and we determine the number of fixed points of the action of $\operatorname{Gal}\mathbf{F}_{q^2}/\mathbf{F}_q$ on $\mathcal{C}$.

Let ρ be a root of g_q in the field $L = \mathbb{Q}(\sqrt{-D})$ discussed above. Note that $\mathbb{Z}[\rho] = S_F$. By a classical result of Deuring [Deu41], the number of elliptic curves in $\mathcal{C}$ is given by the sum

$$\sum_{f|F} \#\operatorname{Cl} S_f,$$

and this is the main part of the statement of Proposition 3. We are left to prove the statement about the Galois action on $\mathcal{C}$.

Suppose that E is an elliptic curve in $\mathcal{C}$ that is isomorphic to its Galois conjugate $E^{(q)}$. Let $f : E \to E^{(q)}$ be an isomorphism, and consider the automorphism $g = f^{(q)} \circ f$ of E.

Since E is ordinary, the automorphism group of E is cyclic of order 2, 4, or 6. Order 6 is impossible, because then L would have to be $\mathbb{Q}(\sqrt{-3})$, whereas we know that D is congruent to 1 modulo 4. If E has an automorphism of order 4 then $D = 1$ and E has j-invariant 0; let us consider this case later, and focus for now on the case where $\operatorname{Aut} E = \{\pm 1\}$.

If $g = 1$, then we can descend E to $\mathbf{F}_q$; that is, we find that there is an elliptic curve F over $\mathbf{F}_q$ that becomes isomorphic to E when we extend the base field to $\mathbf{F}_{q^2}$. If $g = -1$, then we find something slightly different: there is an elliptic curve F over $\mathbf{F}_q$ that becomes isomorphic to E when we extend the base field to $\mathbf{F}_{q^4}$, or in other words, when we extend the base field to $\mathbf{F}_{q^2}$ the curve F becomes isomorphic to the quadratic twist of E.

Suppose that the characteristic polynomial of F over $\mathbf{F}_q$ is $x^2 - sx + q$. Then the characteristic polynomial of F over $\mathbf{F}_{q^2}$ is $x^2 + (2q - s^2)x + q^2$. Since F becomes isomorphic over $\mathbf{F}_{q^2}$ to either E or its quadratic twist, this last polynomial must be either $g_q(x)$ or $g_q(-x)$. Thus we must have either $2q - s^2 = 2 - 2q$ or $2q - s^2 = 2q - 2$. The latter condition requires $s^2 = 2$, which is clearly impossible. The former condition requires that $4q = s^2 + 2$, which cannot hold because it is impossible modulo 4. Thus, we obtain a contradiction if $\operatorname{Aut} E = \{\pm 1\}$.

If $D = 1$, then the isogeny class $\mathcal{C}$ does contain an elliptic curve E with $\operatorname{End} E = \mathbb{Z}[i]$, and this curve is unique because the class number of $\mathbb{Z}[i]$ is 1. Thus, this E is isomorphic to its Galois conjugate.

This proves Proposition 3.

While we do not need the following result for our argument, it is good to point out that the geometrically split polarized surfaces we counted above are the only possible split polarized surfaces in the isogeny class defined by f_q.

Proposition 10. *Suppose (A, λ) is a principally polarized abelian surface over a finite field k. If (A, λ) is not the polarized Jacobian of a genus-2 curve over k, then over the quadratic extension of k the polarized surface (A, λ) may be written as a product of two principally polarized elliptic curves.*

Proof. We know that over *some* finite extension ℓ of k, say of degree n, the polarized surface (A, λ) can be written as a product of polarized elliptic curves (E_1, μ_1) and (E_2, μ_2), together with

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

descent data. If we let σ be the Frobenius automorphism of the extension ℓ/k, the descent data is an isomorphism $f : E_1 \times E_2 \to E_1^\sigma \times E_2^\sigma$ that respects the polarizations $\mu_1 \times \mu_2$ and $\mu_1^\sigma \times \mu_2^\sigma$ and that satisfies the relation

$$1 = f^{\sigma^{n-1}} \circ \cdots \circ f^\sigma \circ f.$$

Using the fact that f respects the polarizations, we can show that f can be represented by a 2×2 matrix of isogenies that is either diagonal or anti-diagonal. In the former case, the descent data gives rise to descent data for (E_1, μ_1) and (E_2, μ_2) that show that (A, λ) splits already over k. In the latter case, we see that n must be even, and that $f^\sigma \circ f$ gives descent data for (A, λ) from ℓ to the quadratic extension of k. Again we find that the descent data for the surface gives descent data for the polarized elliptic curves, so (A, λ) splits over the quadratic extension of k. □

Proposition 10 is almost the same as Theorem 3.4 from [MN02], but that theorem speaks only of the splitting of A, not of (A, λ).

6. The Brauer relations

In this section we prove Proposition 4. Our proof is based on two commutative diagrams. The first diagram (2) is simply diagram (1) with the kernels C, B, and A of the vertical maps added in.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C & \to & B & \to & A & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & D_f & \to & \mathrm{Cl}\, R_f & \to & \mathrm{Cl}\, R_1 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & D_f^+ & \to & \mathrm{Cl}^+ R_f^+ & \to & \mathrm{Cl}^+ R_1^+ & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{2}$$

The second diagram (3) comes from the definitions of the groups in the left-most column of diagram (2).

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & F & \to & E & \to & C & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & G_f & \to & (R_1 \bmod \mathfrak{f})^*/(R_f \bmod \mathfrak{f})^* & \to & D_f & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & G_f^+ & \to & (R_1^+ \bmod \mathfrak{f}^+)^*/(R_f^+ \bmod \mathfrak{f}^+)^* & \to & D_f^+ & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H & \to & 0 & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array} \tag{3}$$

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

Here we have set

$$G_f = \frac{U_1 \bmod \mathfrak{f}}{(U_1 \bmod \mathfrak{f}) \cap (R_f \bmod \mathfrak{f})^*}$$

and

$$G_f^+ = \frac{U_1^+ \bmod \mathfrak{f}^+}{(U_1^+ \bmod \mathfrak{f}^+) \cap (R_f^+ \bmod \mathfrak{f}^+)^*}.$$

We denote by F and H the kernel and cokernel of the map $G_f \to G_f^+$, and we denote by E the kernel of the middle vertical map.

To prove Proposition 4, we would like to calculate $[U_f^+ : N(U_f)]\#B$. Diagram (2) shows that $\#B = \#A\#C$, and diagram (3) shows that $\#C = \#E\#H/\#F$ and that $\#H/\#F = \#G_f^+/\#G_f$. Thus, $\#B = \#A\#E\#G_f^+/\#G_f$, and we have

$$[U_f^+ : N(U_f)]\#B = \big([U_1^+ : N(U_1)]\#A\big)\big(\#E\big)\frac{[N(U_1) : N(U_f)]\#G_f^+}{[U_1^+ : U_f^+]\#G_f}. \tag{4}$$

We evaluate the right-hand side in three steps. The steps are slightly different when $D = 1$, so for now we will assume that $D > 1$.

Lemma 11. *If $D > 1$, then $[U_1^+ : N(U_1)]\#A = (\#\operatorname{Cl} S_1)/2$.*

Proof. It is easy to check that when $D > 1$ the only roots of unity in K are ± 1. Let u be a fundamental unit of K^+ that is positive under at least one of the embeddings of K^+ into $\mathbb{R}$, and let v be a fundamental unit of K. We take $v = u$ if the unit groups of K and K^+ are identical. Note that if the unit group of K strictly contains the unit group of K^+ then $N(v) = u$ and u is totally positive.

We say that we are in case 1 if $v = u$ and u is totally positive, in case 2 if $v = u$ and u is not totally positive, and in case 3 if $v \neq u$. Note that in cases 1 and 2, the regulator of K is twice that of K^+, while in case 3 the two regulators are equal.

For every number field M, let $q(M)$ denote the product of the class number and the regulator of M, divided by the number of roots of unity in M. The Brauer class number relations [FT91, § VIII.7], applied to the biquadratic extension K of $\mathbb{Q}$, show that

$$q(K)q(\mathbb{Q})^2 = q(\mathbb{Q}(\sqrt{-2}))q(K^+)q(L).$$

Since each of the fields contains exactly two roots of unity, and since we know how the regulators of K and K^+ are related to one another, we find that

$$\#\operatorname{Cl} R_1 = \begin{cases} (\#\operatorname{Cl} R_1^+)(\#\operatorname{Cl} S_1)/2 & \text{in cases 1 and 2,} \\ (\#\operatorname{Cl} R_1^+)(\#\operatorname{Cl} S_1) & \text{in case 3.} \end{cases}$$

Now, in cases 1 and 3 the narrow class number of K^+ is twice the class number of K^+, while in case 2 the narrow class number and the class number are equal. Thus, we find that

$$\#\operatorname{Cl} R_1 = \begin{cases} (\#\operatorname{Cl}^+ R_1^+)(\#\operatorname{Cl} S_1)/4 & \text{in case 1,} \\ (\#\operatorname{Cl}^+ R_1^+)(\#\operatorname{Cl} S_1)/2 & \text{in cases 2 and 3.} \end{cases}$$

Now we check that $[U_1^+ : N(U_1)]$ is 1 in cases 2 and 3, and is 2 in case 1. Thus,

$$[U_1^+ : N(U_1)]\#\operatorname{Cl} R_1 = (\#\operatorname{Cl}^+ R_1^+)(\#\operatorname{Cl} S_1)/2$$

in every case. The lemma follows. □

Lemma 12. *If $D > 1$, then $\#G_f = [N(U_1) : N(U_f)]$ and $\#G_f^+ = [U_1^+ : U_f^+]$.*

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

Proof. Recall that U_1 is generated by -1 and v. Since $-1 \in R_f$, we see that $\#G_f$ is equal to the smallest positive integer i such that $v^i \bmod \mathfrak{f}$ lies in $R_f \bmod \mathfrak{f}$. However, since $\mathfrak{f} \subset R_f$, this i is also the smallest integer such that $v^i \in R_f$, and this is clearly the index of U_f in U_1. Since the norm kills only the elements 1 and -1 in U_f and U_1, we see that i is also the index of $N(U_f)$ in $N(U_1)$.

The proof of the second equality of the lemma is similar. □

LEMMA 13. *If $D > 1$, then $\#E = \#\operatorname{Cl} S_f / \#\operatorname{Cl} S_1$.*

Proof. Since S_1^* consists only of ± 1, using arguments as in § 3 shows that

$$\frac{\#\operatorname{Cl} S_f}{\#\operatorname{Cl} S_1} = \frac{\#(S_1 \bmod fS_1)^*}{\#(S_f \bmod fS_1)^*}.$$

On the other hand, the definition of E shows that

$$\#E = \frac{\#(R_1 \bmod fR_1)^* \#(R_f^+ \bmod fR_1^+)^*}{\#(R_f \bmod fR_1)^* \#(R_1^+ \bmod fR_1^+)^*}.$$

If we note that

$$S_f \bmod fS_1 \cong \mathbb{Z} \bmod f\mathbb{Z}$$
$$R_f^+ \bmod fR_1^+ \cong \mathbb{Z} \bmod f\mathbb{Z}$$

and

$$R_f \bmod fR_1 \cong \mathcal{O} \bmod f\mathcal{O},$$

we see that what we want to show is that

$$\#(R_1/fR_1)^* (\#(\mathbb{Z}/f\mathbb{Z})^*)^2 = \#(\mathcal{O}/f\mathcal{O})^* \#(R_1^+/fR_1^+)^* \#(S_1/fS_1)^*$$

for every odd f. It clearly suffices to check this when f is a prime power. We leave the details of this computation to the reader. (However, we note as an example that if $f = p^e$ for a prime p that splits completely in K, then the two sides of the equality above are both equal to $(p-1)^6 p^{6e-6}$.) □

Combining Lemmas 11, 12, and 13 with Equation (4), we find that

$$[U_f^+ : N(U_f)] \frac{\#\operatorname{Cl} R_f}{\#\operatorname{Cl}^+ R_f^+} = \#\operatorname{Cl} S_f / 2$$

when $D > 1$, as required.

The argument when $D = 1$ is entirely similar to the argument we have just given, except that there are some complications because of the eighth roots of unity in K and the fourth roots of unity in L. We leave the details of the argument to the interested reader, but we will at least state the required variants of Lemmas 11, 12, and 13.

LEMMA 14. *If $D = 1$, then $[U_1^+ : N(U_1)] \# A = \#\operatorname{Cl} S_1$.*

LEMMA 15. *If $D = 1$ and $f > 1$, then $\#G_f = 4[N(U_1) : N(U_f)]$ and $\#G_f^+ = [U_1^+ : U_f^+]$.*

LEMMA 16. *If $D = 1$ and $f > 1$, then $\#E = 2\#\operatorname{Cl} S_f / \#\operatorname{Cl} S_1$.*

When $D = 1$ and $f = 1$, Proposition 4 is simply Lemma 14. When $D = 1$ and $f > 1$, we can combine the three lemmas above with Equation (4) to find that

$$[U_f^+ : N(U_f)] \frac{\#\operatorname{Cl} R_f}{\#\operatorname{Cl}^+ R_f^+} = \#\operatorname{Cl} S_f / 2.$$

This proves Proposition 4.

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press

Acknowledgement

The author thanks Hendrik Lenstra for helpful conversations about the techniques used in this paper.

References

Del69 P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.

Ded77 R. Dedekind, *Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers*, in *Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauß* (Braunschweig, 1877), 1–55.

Deu41 M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

FT91 A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27 (Cambridge University Press, Cambridge, 1991).

How95 E. W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), 2361–2401.

LPP02 H. W. Lenstra, Jr., J. Pila and C. Pomerance, *A hyperelliptic smoothness test, II*, Proc. London Math. Soc. (3) **84** (2002), 105–146.

MN02 D. Maisner and E. Nart with an appendix by E. W. Howe, *Abelian surfaces over finite fields as Jacobians*, Exp. Math. **11** (2002) 321–337. Appendix available at arXiv:math.NT/0111006.

Ruc90 H.-G. Rück, *Abelian surfaces and Jacobian varieties over finite fields*, Compositio Math. **76** (1990), 351–366.

San91 J. W. Sands, *Generalization of a theorem of Siegel*, Acta Arith. **58** (1991), 47–57.

Tat71 J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, exposé **352**, in *Séminaire Bourbaki 1968/69*, Lecture Notes in Mathematics, vol. 179 (Springer, Berlin, 1971), 95–110.

Everett W. Howe howeverᵃalumni.caltech.edu
Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1967, USA

https://doi.org/10.1112/S0010437X03000757 Published online by Cambridge University Press