Abelian Surfaces over Finite Fields as Jacobians

Daniel Maisner and Enric Nart with an Appendix by Everett W. Howe

CONTENTS

1. Introduction
2. Isogeny Classes of Abelian Surfaces Over Finite Fields
3. Curves of Genus 2 Over Finite Fields
4. Abelian Surfaces as Jacobians
5. Computational Results
Appendix by Everett W. Howe
Acknowledgments
References

For any finite field $k = \mathbb{F}_q$, we explicitly describe the k-isogeny classes of abelian surfaces defined over k and their behavior under finite field extension. In particular, we determine the absolutely simple abelian surfaces. Then, we analyze numerically what surfaces are k-isogenous to the Jacobian of a smooth projective curve of genus 2 defined over k. We prove some partial results suggested by these numerical data. For instance, we show that every absolutely simple abelian surface is k-isogenous to a Jacobian. Other facts suggested by these numerical computations are that the polynomials $t^4 + (1-2q)t^2 + q^2$ (for all q) and $t^4 + (2-2q)t^2 + q^2$ (for q odd) are never the characteristic polynomial of Frobenius of a Jacobian. These statements have been proved by E. Howe. The proof for the first polynomial is attached in an appendix.

1. INTRODUCTION

Let C be a projective smooth curve of genus 2 defined over a finite field $\mathbb{F}_q$. If $N_m := \sharp C(\mathbb{F}_{q^m})$ denotes the number of points of C over the m-th degree extension of $\mathbb{F}_q$, the zeta function of C can be written as:

$$Z(C/\mathbb{F}_q, t) = \exp\left(\sum_{m\geq 1} N_m \frac{t^m}{m}\right) = \frac{1 + a_1 t + a_2 t^2 + q a_1 t^3 + q^2 t^4}{(1-t)(1-qt)}, \quad (1\text{–}1)$$

for certain integers a_1, a_2, related to N_1, N_2 by:

$$N_1 = a_1 + q + 1, \qquad N_2 = 2a_2 - a_1^2 + q^2 + 1. \quad (1\text{–}2)$$

In this paper, we are interested in determining which rational functions appear as the zeta function of a curve C of genus 2, or equivalently, what pairs of integers a_1, a_2 satisfy (1–1) for a certain curve C, or equivalently, for what pairs of nonnegative integers (N_1, N_2) there exists a curve of genus 2 having N_1 points over $\mathbb{F}_q$ and N_2 points over $\mathbb{F}_{q^2}$.

To any curve C, as above, we can attach a more feasible object: its Jacobian, $J(C)$, which is an abelian surface over $\mathbb{F}_q$. The isogeny class of $J(C)$ is determined

2000 AMS Subject Classification: Primary 11G20, 14G15; Secondary 11G10

Keywords: Abelian surface, zeta function, finite field, Jacobian variety

1058-6458/2001 $0.50 per page
Experimental Mathematics **11**:3, page 321

by the characteristic polynomial of its Frobenius endomorphism, which is easily described in terms of a_1 and a_2:

$$f_{J(C)}(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2.$$

Thus, we can split the characterization of the zeta functions of curves of genus 2 in two steps: first characterize the pairs (a_1, a_2) arising from characteristic polynomials of abelian surfaces over $\mathbb{F}_q$ and, afterwards, determine what abelian surfaces are $\mathbb{F}_q$-isogenous to the Jacobian of a smooth projective curve defined over $\mathbb{F}_q$.

The first step is no mystery. The roots of the characteristic polynomial $f_A(t)$ of the Frobenius endomorphism of an abelian surface A are q-Weil numbers. This leads to bounds on a_1 and a_2 which determine a finite subset of $\mathbb{Z}[t]$ containing all possible polynomials of the form $f_A(t)$. Moreover, by results of Honda and Tate, the $\mathbb{F}_q$-isogeny classes of simple abelian varieties A defined over $\mathbb{F}_q$ are ruled by the q-Weil numbers, classified under the action of the absolute galois group. Combined with results of Tate [Waterhouse and Milne 69] computing the dimension of A in terms of the minimal polynomial of the corresponding q-Weil number, this makes it possible to determine explicitly all pairs (a_1, a_2) for which the polynomial $t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2$ is of the form $f_A(t)$ for a certain abelian surface A defined over $\mathbb{F}_q$. These conditions were described in [Rück 90] and [Xing 94]. In Section 2 we review these results, and we present them in a more explicit form (Theorem 2.9). In particular, we obtain a list of all simple abelian supersingular surfaces, that completes that of [Xing 96], where some cases are missing. Also, we include an exhaustive study of the behavior of the simple abelian surfaces under finite field extension, obtaining an explicit description of the absolutely simple varieties in terms of the pair (a_1, a_2) (Theorem 2.15).

The second step, to determine the Jacobians among all abelian surfaces, seems to be a very difficult question; we present a numerical analysis. In Section 3, we develop an algorithm computing all curves of genus 2 up to k-isomorphism and quadratic twist. The algorithm has been implemented in MATHEMATICA using the package FF designed by Guàrdia to work over finite fields of arbitrary degree over the prime field [Guàrdia 98]. As a by-product, we obtain the complete list of all curves of genus 2 without rational points (Theorem 3.2).

In Sections 4 and 5, we display, for any $q \leq 16$, the numerical results obtained by counting for each isogeny class of abelian surfaces over $\mathbb{F}_q$ how many nonisomorphic curves have a Jacobian belonging to the class. This is achieved by running the algorithm of Section 3 and by computing for each curve the corresponding pair (a_1, a_2). These numerical results present some regular behavior which has led us to prove some partial results, both in the positive and negative direction. For instance, we show that every absolutely simple abelian surface is k-isogenous to the Jacobian of a smooth projective curve of genus 2 (Theorem 4.3). The ordinary case has been proved in [Howe 95] and the nonordinary case is a consequence of the work [Howe 96] and our characterization of the absolutely simple surfaces.

Other facts suggested by our numerical computations are that the polynomials $t^4+(1-2q)t^2+q^2$ (for all q) and $t^4 + (2-2q)t^2 + q^2$ (for q odd) are never the characteristic polynomial of Frobenius of the Jacobian of a smooth projective curve of genus 2 defined over $\mathbb{F}_q$. These statements have been proved by E. Howe. The proof for the first polynomial is attached in an appendix and the proof for the second polynomial appears in [Howe 02]

2. ISOGENY CLASSES OF ABELIAN SURFACES OVER FINITE FIELDS

2.1 Characteristic Polynomials of Abelian Surfaces

Let A be an abelian surface defined over the finite field $\mathbb{F}_q$, where $q = p^a$, $a \geq 1$ for a certain prime number p. We denote by

$$f_A(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2 \in \mathbb{Z}[t] \qquad (2\text{–}1)$$

the characteristic polynomial of the Frobenius endomorphism of A. By abuse of language, we shall sometimes refer to $f_A(t)$ as the characteristic polynomial of A. This polynomial determines A up to $\mathbb{F}_q$-isogeny and the four roots of $f_A(t)$ in $\bar{\mathbb{Q}}$ (counting multiplicites) are q-Weil numbers; more precisely,

$$f_A(t) = (t - \pi_1)(t - \frac{q}{\pi_1})(t - \pi_2)(t - \frac{q}{\pi_2}),$$

with π_1, π_2 q-Weil numbers, not necessarily different. We recall that a q-Weil number is an algebraic integer such that its image under every complex embedding has absolute value $\sqrt{q}$. If A is simple, then $f_A(t) = h_A(t)^e$ for some irreducible polynomial $h_A(t) \in \mathbb{Z}[t]$. By results of Honda and Tate, the mapping

$$A \mapsto \pi \quad \text{root of } h_A(t),$$

is a bijection between $\mathbb{F}_q$-isogeny classes of simple abelian varieties (of any dimension) and conjugation classes of q-Weil numbers (of any degree) [Tate 69].

We review results of Rück and Xing finding necessary and sufficient conditions for a polynomial of the type (2–1) to be the characteristic polynomial of an abelian surface over $\mathbb{F}_q$. We start with well-known bounds on the size of a_1, a_2:

Lemma 2.1. *Let $f(t) \in \mathbb{Z}[t]$ be a monic polynomial of degree 4. The following conditions are equivalent:*

(i) $f(t) = (t-\pi_1)(t-\frac{q}{\pi_1})(t-\pi_2)(t-\frac{q}{\pi_2})$, *with π_1, π_2 q-Weil numbers.*

(ii) $f(t) = (t^2-\beta_1 t+q)(t^2-\beta_2 t+q)$, $\beta_i \in \mathbb{R}$, $|\beta_i| \le 2\sqrt{q}$, $i = 1, 2$.

(iii) $f(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2$, *with*

$$|a_1| \le 4\sqrt{q}, \quad 2|a_1|\sqrt{q} - 2q \le a_2 \le \frac{a_1^2}{4} + 2q. \quad (2\text{–}2)$$

Proof: The relationship $\beta_i = \pi_i + \frac{q}{\pi_i}$ shows immediately that (i) is equivalent to (ii) (cf. [Waterhouse and Milne 69, p. 59]). Analogously, (ii) is equivalent to (iii) since we can relate pairs β_1, β_2 satisfying (ii) with pairs a_1, a_2 satisfying (iii) by:

$$(x-\beta_1)(x-\beta_2) = x^2 + a_1 x + a_2 - 2q. \qquad \square$$

Definition 2.2. A polynomial $f(t) \in \mathbb{Z}[t]$ satisfying the conditions of Lemma 2.1 will be called a Weil polynomial.

Remark 2.3. The bound on $|a_1|$ can be refined to $a_1 \le 2[2\sqrt{q}]$, which is much better than $4\sqrt{q}$ for q nonsquare and large. In fact,

$$|a_1| > 2[2\sqrt{q}] \Longrightarrow 2|a_1|\sqrt{q} - 2q > \left[\frac{a_1^2}{4} + 2q\right],$$

so that in this case there is no integer a_2 satisfying (2–2).

It is easy to characterize when a Weil polynomial is irreducible:

Lemma 2.4. *Let $f(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2 \in \mathbb{Z}[t]$ be a Weil polynomial and let $\Delta = a_1^2 - 4a_2 + 8q$. Then, the following conditions are equivalent:*

(i) $f(t)$ *is irreducible in* $\mathbb{Z}[t]$.

(ii) Δ *is not a square in* $\mathbb{Z}$ *and* $|a_1| < 4\sqrt{q}$, $2|a_1|\sqrt{q} - 2q < a_2 < \frac{a_1^2}{4} + 2q$.

(iii) Δ *is not a square in* $\mathbb{Z}$ *and* $(a_1, a_2) \neq (0, -2q)$.

Proof: The equalities $|a_1| = 4\sqrt{q}$ or $a_2 = 2q + a_1^2/4$ lead to $\Delta = 0$, whereas the equality $2|a_1|\sqrt{q} - 2q = a_2$ leads to either $a_1 = 0, a_2 = -2q$ or to q a square and $\Delta = (|a_1| + 4\sqrt{q})^2$. Thus, (ii) and (iii) are equivalent.

With the notation of Lemma 2.1, Δ is the discriminant of $(x-\beta_1)(x-\beta_2)$; hence, if Δ is a square, then $\beta_1, \beta_2 \in \mathbb{Z}$ and $f(t)$ decomposes in $\mathbb{Z}[t]$. Thus, (i) implies (iii). Conversely, if $f(t)$ is not irreducible in $\mathbb{Z}[t]$, then either some π_i belongs to $\mathbb{Z}$, or some π_i is a quadratic integer with conjugate q/π_i, or π_1, π_2 are conjugate quadratic integers, $\pi_2 \neq q/\pi_1$. In the first two cases, some β_i belongs to $\mathbb{Z}$ and Δ is a square, whereas in the third case, π_1, π_2 are real and $f(t) = (t^2 - q)^2$. Thus, (iii) implies (i). $\square$

If A is a simple abelian surface defined over $\mathbb{F}_q$ whose characteristic polynomial decomposes in $\mathbb{Z}[t]$, then $f_A(t)$ has to be the square of a quadratic irreducible polynomial. The only real quadratic q-Weil numbers are $\pm\sqrt{q}$ (for a odd) and the corresponding simple abelian variety has dimension 2. We compute the dimension of the simple abelian variety associated with a pair of complex conjugate quadratic q-Weil numbers.

Proposition 2.5. *Let $\beta \in \mathbb{Z}$, with $|\beta| < 2\sqrt{q}$ and let $b = v_p(\beta)$ (taking $b = \infty$ if $\beta = 0$). Let $F(t) = t^2 - \beta t + q$ and let $d = \beta^2 - 4q$ be the discriminant of $F(t)$. Let B be the simple abelian variety defined over $\mathbb{F}_q$ with $h_B(t) = F(t)$. Then:*

$$dim(B) = \begin{cases} \frac{a}{(a,b)}, & \text{if } b < \frac{a}{2}, \\ 2, & \text{if } b \ge \frac{a}{2}, \quad d \in \mathbb{Q}_p^{*2}, \\ 1, & \text{if } b \ge \frac{a}{2}, \quad d \notin \mathbb{Q}_p^{*2}. \end{cases}$$

Proof: By [Waterhouse and Milne 69, pp. 58–59], we have $f_B(t) = h_B(t)^e$ and

$$\dim(B) = e = \text{least common denominator of } \frac{v_p(F_\nu(0))}{a},$$

where ν runs among the finite places of $\mathbb{Q}(\sqrt{d})$ lying above p and $F_\nu(t)$ denotes the corresponding factor of $F(t)$ in $\mathbb{Q}_p[t]$. If d is not a square in $\mathbb{Q}_p$, then $F(t)$ is irreducible in $\mathbb{Q}_p[t]$, $v_p(F(0)) = a$, and $e = 1$. If d is a square in $\mathbb{Q}_p$ then $F(t) = F_1(t)F_2(t)$ in $\mathbb{Q}_p[t]$ and denoting $b_i = v_p(F_i(0))$, an easy manipulation of Newton polygons shows that

$$b \ge \frac{a}{2} \Longrightarrow b_1 = b_2 = \frac{a}{2} \Longrightarrow e = 2,$$

$$b < \frac{a}{2} \Longrightarrow b_1 = b, \quad b_2 = a - b \Longrightarrow e = \frac{a}{(a,b)}.$$

$\square$

Corollary 2.6. *By adequate choice of q and β, we can find simple abelian varieties of arbitrarily large dimension with $h_B(t) = t^2 - \beta t + q$.*

Definition 2.7. We say that an integer $\beta \in \mathbb{Z}$, $|\beta| \leq 2\sqrt{q}$, is a q-Waterhouse number if there is an elliptic curve E defined over $\mathbb{F}_q$ such that $f_E(t) = t^2 - \beta t + q$. Equivalently, $\beta \in \mathbb{Z}$ is a q-Waterhouse number if either $|\beta| = 2\sqrt{q}$ or $|\beta| < 2\sqrt{q}$ and the simple abelian variety B associated to the polynomial $t^2 - \beta t + q$ has dimension 1.

Waterhouse found in [Waterhouse 69] very explicit conditions determining the q-Waterhouse numbers. We list below similar explicit conditions for the 2-dimensional case:

Corollary 2.8. *Let $\beta \in \mathbb{Z}$, $|\beta| < 2\sqrt{q}$. There exists a simple abelian surface B defined over $\mathbb{F}_q$ with $h_B(t) = t^2 - \beta t + q$ if and only if a is even and*

$$\beta = \pm\sqrt{q}, \quad p \equiv 1 \pmod 3, \text{ or } \quad \beta = 0, \quad p \equiv 1 \pmod 4.$$

Proof: Straightforward by Proposition 2.5. □

Now we can resume the explicit determination of the Weil polynomials corresponding to abelian surfaces defined over $\mathbb{F}_q$:

Theorem 2.9. *Let $f(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2 \in \mathbb{Z}[t]$ be a Weil polynomial and let*

$$\Delta = a_1^2 - 4a_2 + 8q, \quad \delta = (a_2 + 2q)^2 - 4q a_1^2.$$

Then, $f(t)$ is the characteristic polynomial of a simple abelian surface defined over $\mathbb{F}_q$ if and only if one of the following conditions holds:

(M) *Δ is not a square in $\mathbb{Z}$, $v_p(a_1) = 0$, $v_p(a_2) \geq \frac{a}{2}$ and δ is not a square in $\mathbb{Z}_p$.*

(O) *Δ is not a square in $\mathbb{Z}$ and $v_p(a_2) = 0$.*

(SS1) *(a_1, a_2) belongs to the following list:*

$(0,0)$, a odd, $p \neq 2$, or: a even, $p \not\equiv 1 \pmod 8$,

$(0,q)$, a odd,

$(0,-q)$, a odd, $p \neq 3$, or: a even, $p \not\equiv 1 \pmod{12}$,

$(\pm\sqrt{q}, q)$, a even, $p \not\equiv 1 \pmod 5$,

$(\pm\sqrt{5q}, 3q)$, a odd, $p = 5$,

$(\pm\sqrt{2q}, q)$, a odd, $p = 2$.

(SS2) *(a_1, a_2) belongs to the following list:*

$(0,-2q)$, a odd,

$(0,2q)$, a even, $p \equiv 1 \pmod 4$,

$(\pm 2\sqrt{q}, 3q)$, a even, $p \equiv 1 \pmod 3$.

Moreover, let β_1, β_2 be the roots of the quadratic polynomial $x^2 + a_1 x + (a_2 - 2q)$, with discriminant Δ. Then, $f(t) = f_A(t)$ for an abelian surface $A \sim E_1 \times E_2$ if and only if Δ is a square in $\mathbb{Z}$ and β_1, β_2 are q-Waterhouse numbers. In this case, the elliptic curves E_1, E_2 are $\mathbb{F}_q$-isogenous if and only if $\Delta = 0$.

Proof: By Lemma 2.4 in the cases (M), (O), (SS1), $f(t)$ is irreducible and the conditions determining when $f(t) = f_A(t)$ for some surface A were found in [Rück 90]. Actually, Rück wrote condition (SS1) as

$$v_p(a_1) \geq \frac{a}{2}, \quad v_p(a_2) \geq a, \quad f(t) \text{ has no roots in } \mathbb{Z}_p,$$

but it is easy to check that the irreducible Weil polynomials with (a_1, a_2) satisfying this last condition are precisely those listed in condition (SS1) above.

The case where $f(t)$ is reducible (SS2) is a consequence of Proposition 2.5 and it was first described in [Xing 94]. □

Corollary 2.10. *If $\mathbb{F}_q$ is the prime field $\mathbb{F}_p$ (that is $q = p$), then every Weil polynomial is the characteristic polynomial of an abelian surface defined over $\mathbb{F}_q$.*

Proof: Assume that $(a_1, a_2) \in \mathbb{Z}^2$ satisfies the inequalities (2–2). If $\Delta = a_1^2 - 4a_2 + 8q$ is a square in $\mathbb{Z}$, then the integers $\beta = (-a_1 \pm \sqrt{\Delta})/2$ satisfy: $|\beta| < 2\sqrt{p}$ and any integer satisfying this inequality is a p-Waterhouse number. If Δ is not a square in $\mathbb{Z}$ and $(a_1, a_2) \neq (0, -2q)$, then (a_1, a_2) falls in one of the cases (M), (O), (SS1). □

Corollary 2.11. *A Weil polynomial is the characteristic polynomial of a simple supersingular abelian surface defined over $\mathbb{F}_q$ if and only if it appears in the list (SS1) or (SS2).*

Proof: The supersingular condition is equivalent to $v_p(a_1) \geq a/2$, $v_p(a_2) \geq a$. In the list of simple abelian surfaces given in Theorem 2.9, only those of (SS1) and (SS2) satisfy this condition. □

This result completes the list given in [Xing 96], where some cases are missing.

(a_1, a_2)	L
(0,0), (a odd, $p \neq 2$) or (a even, $p \not\equiv 1 \pmod 8$), $p \not\equiv 1 \pmod 4$	$\mathbb{F}_{q^2}$
(0,0), (a odd, $p \neq 2$) or (a even, $p \not\equiv 1 \pmod 8$), $p \equiv 1 \pmod 4$	$\mathbb{F}_{q^4}$
$(0, q)$, a odd, $p \not\equiv 1 \pmod 3$	$\mathbb{F}_{q^2}$
$(0, q)$, a odd, $p \equiv 1 \pmod 3$	$\mathbb{F}_{q^6}$
$(0, -q)$, (a odd, $p \neq 3$) or (a even, $p \not\equiv 1 \pmod{12}$), $p \not\equiv 1 \pmod 3$	$\mathbb{F}_{q^2}$
$(0, -q)$, (a odd, $p \neq 3$) or (a even, $p \not\equiv 1 \pmod{12}$), $p \equiv 1 \pmod 3$	$\mathbb{F}_{q^3}$
$(\pm\sqrt{q}, q)$, a even, $p \not\equiv 1 \pmod 5$	$\mathbb{F}_{q^5}$
$(\pm\sqrt{5q}, 3q)$, a odd, $p = 5$	$\mathbb{F}_{q^5}$
$(\pm\sqrt{2q}, q)$, a odd, $p = 2$	$\mathbb{F}_{q^4}$
$(0, -2q)$, a odd	$\mathbb{F}_{q^2}$
$(0, 2q)$, a even, $p \equiv 1 \pmod 4$	$\mathbb{F}_{q^2}$
$(\pm 2\sqrt{q}, 3q)$, a even, $p \equiv 1 \pmod 3$	$\mathbb{F}_{q^3}$

TABLE 1. The minimum field L of decomposition of the supersingular surfaces.

2.2 Absolutely Simple Abelian Surfaces

We now characterize in terms of the pair (a_1, a_2) when an abelian surface A defined over $\mathbb{F}_q$ is absolutely simple. By abuse of language, we denote simply by $A = (a_1, a_2)$ the (isogeny class of an) abelian surface determined by a pair (a_1, a_2) satisfying the conditions of Theorem 2.9.

We have classified the simple abelian surfaces in three groups: (M) for mixed, (O) for ordinary and (SS1), (SS2) for supersingular. They can be distinguished by the Newton polygon of their characteristic polynomial, which has 3, 2, 1 sides, respectively. The number of sides of the Newton polygon is invariant under scalar extension; thus, attending to the particular shape of the polygon, we see that after scalar extension, a simple surface of type (M), (O), (SS) either remains simple of the same type or decomposes as the product of two elliptic curves, which are, respectively, ordinary×supersingular, ordinary×ordinary, and supersingular×supersingular. Actually, we shall prove that all simple surfaces of type (M) are absolutely simple.

Since the invariant Δ can be a square in $\mathbb{Z}$, or the characteristic polynomial can be reducible only for supersingular simple surfaces, we have

Lemma 2.12. *Let A be a nonsupersingular simple abelian surface defined over $\mathbb{F}_q$. The following conditions are equivalent:*

(i) A remains simple over $\mathbb{F}_{q^n}$.

(ii) The invariant $\Delta(\mathbb{F}_{q^n})$ is not a square in $\mathbb{Z}$.

(iii) The characteristic polynomial $f_{A_{|\mathbb{F}_{q^n}}}(t)$ is irreducible.

The proof of the following observation is straightforward.

Lemma 2.13. *Let $A = (a_1, a_2)$ be an abelian surface defined over $\mathbb{F}_q$ and let $A_{|\mathbb{F}_{q^2}} = (b_1, b_2)$, $A_{|\mathbb{F}_{q^3}} = (c_1, c_2)$. Then*

$$b_1 = 2a_2 - a_1^2, \quad b_2 = a_2^2 - 2qa_1^2 + 2q^2;$$

$$c_1 = a_1(a_1^2 - 3a_2 + 3q), \quad c_2 = a_2^3 + 6q^2a_1^2 - 3q^2a_2 - 3qa_1^2a_2.$$

Moreover,

$$\Delta(\mathbb{F}_{q^2}) = a_1^2\Delta, \quad \Delta(\mathbb{F}_{q^3}) = (q - a_1^2 + a_2)^2\Delta.$$

We can tell the minimum field L of decomposition of the supersingular surfaces just by checking Lemma 2.13 and Theorem 2.9. (See Table 1.)

In the nonsupersingular case, it is easy to analyze, using Lemmas 2.12 and 2.13, the decomposition in $\mathbb{F}_{q^n}$, for $n = 2, 3, 4, 6$:

Proposition 2.14. *Let $A = (a_1, a_2)$ be a simple abelian surface defined over $\mathbb{F}_q$, which is not supersingular. Then*

(i) A decomposes over $\mathbb{F}_{q^2}$ iff $a_1 = 0$.

(ii) A decomposes over $\mathbb{F}_{q^3}$ iff $q = a_1^2 - a_2$.

(iii) A is simple over $\mathbb{F}_{q^2}$ and decomposes over $\mathbb{F}_{q^4}$ iff $a_1^2 = 2a_2$.

(iv) A is simple over $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$ but decomposes over $\mathbb{F}_{q^6}$ iff $a_1^2 = 3(a_2 - q)$.

(v) If A is simple over $\mathbb{F}_{q^4}$ then it is simple over $\mathbb{F}_{q^8}$.

(vi) If A is simple over $\mathbb{F}_{q^4}$ and $\mathbb{F}_{q^6}$ then it is simple over $\mathbb{F}_{q^{12}}$.

Proof: Suppose that A decomposes over $\mathbb{F}_{q^n}$ and $n = 2$ or 3. Then $\Delta(\mathbb{F}_{q^n})$ is a square in $\mathbb{Z}$, but since $\Delta(\mathbb{F}_{q^2}) = a_1^2\Delta$ (respectively, $\Delta(\mathbb{F}_{q^3}) = (q - a_1^2 + a_2)^2\Delta$) and Δ is not a square in $\mathbb{Z}$, this implies $a_1 = 0$ (respectively, $q - a_1^2 + a_2 = 0$). Conversely, if $a_1 = 0$ (respectively, $q - a_1^2 + a_2 = 0$), then $\Delta(\mathbb{F}_{q^n}) = 0$ and A decomposes over $\mathbb{F}_{q^2}$ by Lemma 2.12. This proves (i) and (ii).

By (i), A decomposes over $\mathbb{F}_{q^4}$ and not before if and only if $a_1 \neq 0$ and $b_1 = 0$. This is equivalent to $b_1 = 0$ since the condition $a_1 = 0 = b_1$ is satisfied only by the supersingular surface $A = (0, 0)$. This proves (iii).

By (i) and (ii), A decomposes over $\mathbb{F}_{q^6}$ and not before if and only if $c_1 = 0$, $a_1 \neq 0$, $q \neq a_1^2 - a_2$. The two first conditions are equivalent to $a_1^2 - 3a_2 + 3q = 0$ and this latter condition already implies that $q \neq a_1^2 - a_2$. In fact, $a_1^2 - 3a_2 + 3q = 0 = q - a_1^2 + a_2$ leads to $(a_1, a_2) = (\sqrt{3q}, 2q)$ which is either impossible or satisfied only by a supersingular surface. This proves (iv).

Suppose that A is simple over $\mathbb{F}_{q^4}$ and decomposes over $\mathbb{F}_{q^8}$. By (iii), applied to the surface $A_{|\mathbb{F}_{q^2}}$, we have $b_1^2 = 2b_2$, but this equation is impossible. In fact, it leads to

$$a_1^4 + 2a_2^2 - 4a_2a_1^2 + 4qa_1^2 - 4q^2 = 0.$$

This relation implies a_1, a_2 both even and $4q^2 \equiv 0 \pmod 8$, which is possible only for $p = 2$. But then, A would be supersingular. This proves (v).

Suppose that A is simple over $\mathbb{F}_{q^4}$ and $\mathbb{F}_{q^6}$, but it decomposes over $\mathbb{F}_{q^{12}}$. By (iv), applied to the surface $A_{|\mathbb{F}_{q^2}}$, we have $b_1^2 = 3(b_2 - q^2)$, which is impossible. In fact, it leads to

$$a_1^4 + (6q - 4a_2)a_1^2 + a_2^2 - 3q^2.$$

The discriminant of this quadratic equation in a_1^2 is $12(a_2 - 2q)^2$, which is a square in $\mathbb{Z}$ only if $a_2 = 2q$; but then $a_1^2 = q$ and (for a even) A would be supersingular. This proves (vi). □

Actually, Proposition 2.14 collects all possible cases in which a non-supersingular simple abelian surface is not absolutely simple.

Theorem 2.15. *Let $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2 \in \mathbb{Z}[t]$ be a Weil polynomial and let*

$$\Delta = a_1^2 - 4a_2 + 8q, \quad \delta = (a_2 + 2q)^2 - 4qa_1^2.$$

Then there exists an absolutely simple abelian surface A defined over $\mathbb{F}_q$ with $f(t) = f_A(t)$ if and only if Δ is not a square in $\mathbb{Z}$ and either

(a) $v_p(a_1) = 0$, $v_p(a_2) \geq a/2$, δ is not a square in $\mathbb{Z}_p$, or

(b) $v_p(a_2) = 0$, $a_1^2 \notin \{0, q + a_2, 2a_2, 3(a_2 - q)\}$.

Proof: We have already checked that all surfaces other than those listed above are not absolutely simple. We prove now that if $A = (a_1, a_2)$ is a nonsupersingular simple abelian surface which is not absolutely simple, then $a_1^2 \in \{0, q + a_2, 2a_2, 3(a_2 - q)\}$. For such a surface, the characteristic polynomial $f_A(t)$ is irreducible. Let π be one of its roots in $\bar{\mathbb{Q}}$ and let $K = \mathbb{Q}(\pi)$ be the quartic field generated by π. The quadratic algebraic integer $\beta = \pi + q/\pi$ belongs to K, hence, the discriminant Δ of its minimal polynomial over $\mathbb{Q}$ is a square in K, so that K contains $\mathbb{Q}(\sqrt{\Delta})$ as a quadratic subfield.

By Lemma 2.12, A decomposes over $\mathbb{F}_{q^n}$ if and only if the characteristic polynomial of $A_{|\mathbb{F}_{q^n}}$ reduces and this is equivalent to $\mathbb{Q}(\pi^n) \subsetneq K$. Take n minimum with this property and let L be a quadratic subfield of K containing π^n. If $\mathrm{Gal}(K/L) = \{1, \sigma\}$, we have

$$\pi^n \in L \Longleftrightarrow (\pi^n)^\sigma = \pi^n \Longleftrightarrow \pi^\sigma = \epsilon\pi,$$

where $\epsilon \in K$ is a primitive n-th root of 1, by the minimality of n. Thus, n belongs to the set $\{2, 3, 4, 5, 6, 8, 10, 12\}$. By Proposition 2.14, the cases $n = 8, 12$ are not possible and in the cases $n = 2, 3, 4, 6$, we have $a_1^2 \in \{0, q + a_2, 2a_2, 3(a_2 - q)\}$.

Finally, assume that $n = 5$ or 10. Then $K = \mathbb{Q}(\mu_5)$ is a cyclic extension of $\mathbb{Q}$ whose only quadratic subfield is $\mathbb{Q}(\sqrt{5})$. In this case, $\pi^n = \pm\sqrt{q^n}$, since π^n is a real Weil number. Thus, A would be supersingular. □

The ordinary case (b) has already been settled in [Howe and Zhu 02].

Corollary 2.16. *The minimum positive integer n for which a not absolutely simple abelian surface over $\mathbb{F}_q$ decomposes over $\mathbb{F}_{q^n}$ belongs to $\{1, 2, 3, 4, 5, 6\}$.*

Corollary 2.17. *If an abelian surface A defined over $\mathbb{F}_q$ decomposes over $\overline{\mathbb{F}}_q$ as the product of two elliptic curves, one supersingular, the other ordinary, then A decomposes already over $\mathbb{F}_q$.*

3. CURVES OF GENUS 2 OVER FINITE FIELDS

3.1 Generalities on Curves of Genus 2

Let k be a perfect field. Any smooth projective curve C defined over k of genus 2 is hyperelliptic; that is, it admits

a k-morphism, $x\colon C \longrightarrow \mathbb{P}^1$, of degree 2. In particular, the function field $k(C)$ is a separable quadratic extension of $k(\mathbb{P}^1)$. The k-automorphism, $\iota\colon C \longrightarrow C$, corresponding to the nontrivial element of $\mathrm{Gal}(k(C)/k(\mathbb{P}^1))$ is called the *hyperelliptic involution* of C. Any two k-morphisms of degree 2 from C to $\mathbb{P}^1$ differ by a k-automorphism of $\mathbb{P}^1$. Thus, the hyperelliptic involution does not depend on the particular choice of the morphism x. The fixed points of ι are the ramification points of any such morphism and they coincide also with the Weierstrass points of C. By the Hurwitz genus formula, the different of $k(C)/k(\mathbb{P}^1)$ is a divisor D of degree 6. If $\mathrm{char}(k) \neq 2$, D consists of six different points, but if $\mathrm{char}(k) = 2$, there are three different possibilities for the structure of this divisor [Igusa 60],[Lachaud 91]:

(a) $D = 5P_\infty$,

(b) $D = 3P_\infty + P_0$,

(c) $D = P_\infty + P_0 + P_1$.

Since the divisor D is defined over k, the points P_∞ and P_0 in cases (a) and (b) are defined over k too. However, in case (c), we have three possibilities:

(c1) P_∞, P_0, P_1 defined over k,

(c2) P_∞ defined over k and P_0, P_1 conjugated over a quadratic extension,

(c3) P_∞, P_0, P_1 conjugated over a cubic extension.

Clearly, the type of divisor and the structure of the support of D as a galois set are invariant by k-isomorphism; thus, the set $\mathcal{H}$ of k-isomorphy classes of smooth projective curves of genus 2 is the disjoint union of 5 subsets:

$$\mathcal{H} = \mathcal{H}_a \cup \mathcal{H}_b \cup \mathcal{H}_{c1} \cup \mathcal{H}_{c2} \cup \mathcal{H}_{c3}.$$

If $\mathrm{char}(k) \neq 2$, there are 11 possibilities for the structure of the support of D as a galois set, one for each partition of 6. We have a similar decomposition of $\mathcal{H}$ as the disjoint union of 11 subsets:

$$\begin{aligned}\mathcal{H} = \mathcal{H}_6 \cup \mathcal{H}_{5,1} \cup \mathcal{H}_{4,2} \cup \mathcal{H}_{4,1,1} \cup \mathcal{H}_{3,3} \cup \mathcal{H}_{3,2,1} \cup \mathcal{H}_{3,1,1,1} \\ \cup \mathcal{H}_{2,2,2} \cup \mathcal{H}_{2,2,1,1} \cup \mathcal{H}_{2,1,1,1,1} \cup \mathcal{H}_{1,1,1,1,1,1},\end{aligned}$$

where, for instance, $\mathcal{H}_{4,1,1}$ denotes the set of classes of curves in $\mathcal{H}$ having two Weierstrass points defined over k and four Weierstrass points defined over a quartic extension of k and forming a complete orbit under the action of $\mathrm{Gal}(\bar{k}/k)$.

We choose a point $\infty \in \mathbb{P}^1(k)$, and we call it infinity. This choice determines an embedding $\mathbb{A}^1 \subseteq \mathbb{P}^1$ and identifications $k(\mathbb{P}^1) = k(x)$, $\mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2$. The function field $k(C)$, as a quadratic extension of $k(x)$, admits a generator $y \in k(C)$ satisfying:

$$\begin{aligned} y^2 &= f(x) \quad (\text{if } \mathrm{char}(k) \neq 2), \\ y^2 + y &= f(x) \quad (\text{if } \mathrm{char}(k) = 2), \end{aligned} \tag{3–1}$$

for some rational function $f(x) \in k(x)$. This equation for the function field of C is unique up to two actions: x can be replaced by any automorphism $\gamma(x) \in \mathrm{PGL}_2(k)$ and $f(x)$ can be replaced, respectively, by

$$\begin{aligned} &f(x)g(x)^2 && (\text{if } \mathrm{char}(k) \neq 2), \\ &f(x) + g(x) + g(x)^2 && (\text{if } \mathrm{char}(k) = 2), \end{aligned}$$

where $g(x) \in k(x)$ is an arbitrary rational function, $g(x) \neq 0$ in the odd characteristic case. Accordingly, one is able to exhibit a family of plane affine models containing all k-birational classes of curves of genus 2.

If $\mathrm{char}(k) \neq 2$, any projective smooth curve of genus 2 is k-isomorphic to the normalization of the projective closure of the plane affine curve C_0 defined by the equation $y^2 = f(x)$, where $f(x) = a_n x^n + \cdots + a_0 \in k[x]$ is a separable polynomial of degree 5 or 6. The curve C_0 is smooth and its closure $\tilde{C}$ in $\mathbb{P}^2$ has only one point at infinity, P_∞, which is a singular point. If $n = 5$, the point P_∞ has only one preimage in the normalization $C \to \tilde{C}$, which we still denote by P_∞; this point is a Weierstrass point and it is always defined over k. If $n = 6$, the point P_∞ has two preimages in C, which we denote by P_{∞_1}, P_{∞_2}; these points are permuted by ι and they are defined over k if and only if a_n is a square in k^*. Since the rest of the points of C are in bijection with the points in C_0, it is common to attach to these points of C the affine coordinates (x, y) of the corresponding points in C_0. In affine coordinates, the hyperelliptic involution is expressed by $\iota(x, y) = (x, -y)$.

If $\mathrm{char}(k) = 2$, any projective smooth curve of genus 2 is k-isomorphic to the normalization of the projective closure of the plane affine curve C_0 defined (after removal of denominators) by an equation:

(a) $y^2 + y = ax^5 + bx^3 + cx^2 + d, \qquad a \neq 0,$

(b) $y^2 + y = ax^3 + bx + \frac{c}{x} + d, \qquad ac \neq 0,$

(c1) $y^2 + y = ax + \frac{b}{x} + \frac{c}{x+1} + d, \qquad abc \neq 0,$

(c2) $y^2 + y = ax + \frac{bx+c}{Q(x)} + d, \qquad a \neq 0,\ (b, c) \neq (0, 0),$

(c3) $y^2 + y = \frac{ax^2+bx+c}{P(x)} + d, \qquad (a, b, c) \neq (0, 0, 0),$

where $Q(x)$, $P(x)$ are irreducible polynomials of respective degree 2,3. As before, one attaches to the points of C the affine coordinates of the corresponding affine model.

The set of "points at infinity" of C coincides with the set W of Weierstrass points, except for the model (c3), in which case

$$C(\bar{k}) \setminus C_0(\bar{k}) = W \cup \{P_{\infty_1}, P_{\infty_2}\},$$

with P_{∞_1}, P_{∞_2} permuted by ι; these two points are defined over k if and only if d belongs to the Artin-Schreier group: $AS(k) := \{\lambda + \lambda^2 \,|\, \lambda \in k\}$. In affine coordinates, the hyperelliptic involution is expressed by: $\iota(x, y) = (x, y + 1)$.

3.2 Quadratic Twist

The quadratic extensions of k are parameterized by $k^*/(k^*)^2$ if $\mathrm{char}(k) \neq 2$ (Kummer theory) and by $k/AS(k)$ if $\mathrm{char}(k) = 2$ (Artin-Schreier theory). If a smooth projective curve C of genus 2 is given by Equation (3–1), we define the twisted curve by an element $\lambda \in k^*/(k^*)^2$, respectively, $\lambda \in k/AS(k)$, as the curve C^λ determined by the equation

$$y^2 = \lambda f(x), \qquad \text{respectively,} \quad y^2 + y = f(x) + \lambda.$$

The curves C and C^λ are isomorphic over the quadratic extension of k determined by λ, but they are not necessarily k-isomorphic. This induces a well-defined action of $k^*/(k^*)^2$, respectively, $k/AS(k)$, on $\mathcal{H}$ and we denote by $\mathcal{H}^t$ the quotient set of classes of curves of genus 2 up to k-isomorphism and quadratic twist. The galois structure of the set of Weierstrass points is preserved by quadratic twist and we obtain an analogous decomposition for the set $\mathcal{H}^t$ as the disjoint union of 11, respectively, 5 subsets.

If $k = \mathbb{F}_q$ is a finite field, we have $k^*/(k^*)^2 \simeq \mathbb{Z}/2\mathbb{Z}$, respectively, $k/AS(k) \simeq \mathbb{Z}/2\mathbb{Z}$, according to the parity of q. Actually, if q is even, we have an exact sequence of additive groups

$$0 \longrightarrow \mathbb{F}_2 \longrightarrow \mathbb{F}_q \xrightarrow{AS} \mathbb{F}_q \xrightarrow{Tr} \mathbb{F}_2 \longrightarrow 0,$$

where $AS(\lambda) = \lambda + \lambda^2$. Thus, the subgroup $AS(\mathbb{F}_q)$ coincides with the set of elements of absolute trace zero.

Let $N_m(C) = \#C(\mathbb{F}_{q^m})$ be the number of rational points of C over the unique extension of degree m of k. If we denote by C' the nontrivial quadratic twist of C, we have

$$N_1(C) + N_1(C') = 2q + 2, \quad N_2(C) = N_2(C'),$$

or equivalently,

$$a_1 + a_1' = 0, \quad a_2 = a_2', \tag{3–2}$$

where a_1, a_2 and a_1', a_2' are the coefficients of the numerator of the zeta function, respectively, of C and C' (see, for example (1–2)).

3.3 Generating Curves of Genus 2 up to *k*-isomorphism and Quadratic Twist

If $\mathrm{char}(k) \neq 2$, the moduli functor of curves of genus 2 is the variety

$$\mathcal{M} = \begin{pmatrix} \mathbb{P}^1 \\ 6 \end{pmatrix} \backslash \mathrm{PGL}_2.$$

The set of k-points of this functor parameterizes smooth projective curves of genus 2 up to k-isomorphism and quadratic twist. More precisely, if we denote by

$$\mathbb{X} := \begin{pmatrix} \mathbb{P}^1(\bar{k}) \\ 6 \end{pmatrix}^{\mathrm{Gal}(\bar{k}/k)},$$

the set of families of six different points of $\mathbb{P}^1(\bar{k})$ which are invariant (as a family) under the galois action, we can consider the map

$$w : \mathcal{H}^t \longrightarrow \mathcal{M}(k) = \mathbb{X} \backslash \mathrm{PGL}_2(k), \tag{3–3}$$

which assigns to any curve C the set $\{x(P_1), \cdots, x(P_6)\}$ of images of the Weierstrass points $P_1, \cdots, P_6$ of C under any k-morphism, $x : C \longrightarrow \mathbb{P}^1$, of degree 2. This map w is well-defined and bijective. The inverse map sends $\{x_1, \cdots, x_6\}$ to the curve C defined by the equation

$$y^2 = \prod_{x_i \neq \infty} (x - x_i).$$

In exactly the same way as $\mathcal{H}$ and $\mathcal{H}^t$, the sets $\mathbb{X}$ and $\mathbb{X} \backslash \mathrm{PGL}_2(k)$ split as the union of 11 different subsets according to the galois structure of the sextuples of points. Clearly, the map w of (3–3) respects this decomposition. In fact, in an affine model, the Weierstrass points have coordinates $(x, 0)$ and the possible Weierstrass point at infinity P_∞ with image $x(P_\infty) = \infty$ is always defined over k.

In order to describe $\mathcal{H}^t$ when $\mathrm{char}(k) = 2$, we don't use the moduli space of curves of genus 2 (described in [Igusa 60]). Instead, we find for each of the cases (a), (b), (c1), (c2), and (c3) explicit conditions on the coefficients a, b, c, d of the equations, determining when two curves of the same type are k-isomorphic. Curves of type (a) are precisely those whose Jacobian is supersingular; this case has been thoroughly studied in [van der Geer and van der Vlugt 92]. For details concerning the other cases, see [Cardona et al. 02].

We have developed two independent MATHEMATICA subroutines that find unique representatives of the set $\mathcal{H}^t$ when $k = \mathbb{F}_q$ is the finite field with q elements. For q odd, the subroutine Gen2 finds representatives of the set $\mathbb{X}$ under the action of $\mathrm{PGL}_2(k)$. For the sake

Equation	N_1	N_2	a_1	a_2
type (a)				
$y^2+y=x^5$	3	5	0	0
$y^2+y=x^5+x^2$	5	9	2	4
$y^2+y=x^5+x^3$	5	5	2	2
$y^2+y=x^5+x^3+x^2$	3	9	0	2
type (b)				
$y^2+y=x^3+\frac{1}{x}$	4	4	1	0
$y^2+y=x^3+x+\frac{1}{x}$	2	8	-1	2
type (c1)				
$y^2+y=x+\frac{1}{x}+\frac{1}{x+1}$	3	3	0	-1
type (c2)				
$y^2+y=x+1/(x^2+x+1)$	3	7	0	1
$y^2+y=x+x/(x^2+x+1)$	5	7	2	3
type (c3)				
$y^2+y=1/(x^3+x+1)$	2	6	-1	1
$y^2+y=x/(x^3+x+1)$	4	10	1	3
$y^2+y=(x^2+x)/(x^3+x+1)$	6	6	3	5

TABLE 2. $q=2$.

of efficiency, we split the search of these representatives into 11 different cases, since for each different structure of the galois set, we use different procedures to lower the complexity of the search. For q even, the subroutine Gen2Ch2 works directly with the five types of generating equations, restricted always to the case $d=0$. We remark that since two triples of points of $\mathbb{P}^1$ with the same galois structure are in the same orbit under the action of $\mathrm{PGL}_2(\mathbb{F}_q)$, the quadratic and cubic irreducible polynomials $Q(x)$, $P(x)$ of cases (c2) and (c3) can be fixed a priori. These subroutines, as well as the package FF, can be downloaded at www.mat.uab.es/danielm.

Our programs also compute for each curve the numbers N_1, N_2 of points of the curve over the fields $\mathbb{F}_q, \mathbb{F}_{q^2}$ and the relevant coefficients a_1, a_2 of the numerator of the zeta function. For instance, we list in Table 2 the output for $q=2$ and in Table 3 the output for $q=3$.

Remark 3.1. For q odd, explicit formulas for $\sharp\mathcal{H}^t$ as a polynomial in q can be found in [López et al. 02]. By similar methods, we found formulas for the cardinality of each of the 11 subsets $\mathcal{H}^t_P$, where P is a partition of 6.

For q even, in [van der Geer and van der Vlugt 92] the authors find explicit formulas for $\sharp\mathcal{H}_a$ and, even more, for the number of curves in $\mathcal{H}_a$ with prescribed number N_1 of k-points. Formulas for $\sharp\mathcal{H}_b$ and $\sharp\mathcal{H}_{ci}$, $i=1,2,3$

Equation	N_1	N_2	a_1	a_2
21111				
$y^2=(1+x^2)x(1+x)(-1+x)$	4	6	0	-2
2211				
$y^2=(1+x^2)x(-1-x+x^2)$	6	10	2	2
$y^2=(1+x^2)(1+x)(-1+x+x^2)$	4	14	0	2
222				
$y^2=(1+x^2)(-1+x+x^2)(-1-x+x^2)$	8	14	4	10
42				
$y^2=(1+x^2)(-1-x^2+x^4)$	6	18	2	6
$y^2=(1+x^2)(1-x+x^2+x^4)$	6	14	2	4
$y^2=(1+x^2)(-1-x+x^4)$	4	14	0	2
$y^2=(1+x^2)(1-x+x^3+x^4)$	8	10	4	8
411				
$y^2=x(-1+x-x^2-x^3+x^4)$	4	10	0	0
$y^2=x(1+x+x^2+x^4)$	6	10	2	2
$y^2=x(1+x-x^3+x^4)$	4	6	0	-2
$y^2=x(-1-x^2+x^4)$	4	18	0	4
$y^2=x(-1+x+x^4)$	6	14	2	4
$y^2=x(1-x+x^2-x^3+x^4)$	6	18	2	6
33				
$y^2=(-1-x+x^3)(1-x+x^3)$	2	20	-2	7
$y^2=(-1-x+x^3)(1-x^2+x^3)$	4	12	0	1
$y^2=(-1-x+x^3)(-1+x^2+x^3)$	6	12	2	3
3111				
$y^2=x(x-1)(1+x-x^2+x^3)$	3	5	-1	-2
$y^2=x(x-1)(-1+x^2+x^3)$	5	13	1	2
321				
$y^2=(1+x^2)(1+x-x^2+x^3)$	5	13	1	2
$y^2=(1+x^2)(-1+x^2+x^3)$	3	9	-1	0
$y^2=(1+x^2)(-1-x-x^2+x^3)$	1	13	-3	6
$y^2=(1+x^2)(1-x+x^3)$	3	17	-1	4
6				
$y^2=1+x^2-x^4+x^6$	4	20	0	5
$y^2=1-x^2+x^6$	8	12	4	9
$y^2=-1+x+x^3+x^4+x^5+x^6$	6	16	2	5
$y^2=-1+x^5+x^6$	4	16	0	3
$y^2=-1-x^3-x^4+x^5+x^6$	2	12	-2	3
$y^2=-1+x+x^5+x^6$	4	8	0	-1
$y^2=1-x+x^2-x^3+x^5+x^6$	6	8	2	1
51				
$y^2=-1+x-x^2-x^4+x^5$	3	15	-1	3
$y^2=1-x+x^5$	7	15	3	7
$y^2=-1+x+x^3+x^5$	1	11	-3	5
$y^2=-1-x^3-x^4+x^5$	5	15	1	3
$y^2=1+x-x^2-x^3+x^5$	5	19	1	5
$y^2=-1-x-x^2+x^3-x^4+x^5$	3	7	-1	-1
$y^2=-1-x+x^2+x^3+x^5$	3	11	-1	1
$y^2=-1-x-x^4+x^5$	5	11	1	1

TABLE 3. $q=3$.

$q=2$	$y^2+y=1+(x^2+x)/(x^3+x+1)$
$q=3$	$y^2=-(x^2+1)(x^2+x-1)(x^2-x-1)$ $y^2=-(x^2+1)(x^4+x^3-x+1)$ $y^2=-x^6+x^2-1$
$q=4$	$y^2+y=s+x/(x^3+x+1),\ \ s^2=s+1$
$q=5$	$y^2=(2x^3+4x-2)(x^3-2x^2-1)$ $y^2=2x^6-2x^5+2x^4+x^3-x^2-2x+2$ $y^2=(2x^2+1)(x^4-2x^3+x^2-2x-2)$
$q=7$	$y^2=(-x^2+3)(x^2+1)(x^2+2)$ $y^2=-x^6+2x^4-3x^2-2$
$q=8$	$y^2+y=u+((u+u^2)+ux+ux^2)/(x^3+ux+u),\ \ u^3=u^2+1$
$q=9$	$y^2=s(x^3-x+1)(x^3-x-1),\ s^2=-1$
$q=11$	$y^2=(-x^2+2)(x^4-5x^3+x^2+x+4)$

TABLE 4.

can be found in [Cardona et al. 02]. Our numerical computations agree with all these results.

As a by-product of our search, we obtain the complete list of curves of genus 2 without rational points. By Weil's bound, any curve of genus 2 over $\mathbb{F}_q$ has rational points if $q>13$. By searching all curves for $q\leq 13$, we obtain

Theorem 3.2. *Any smooth projective curve C of genus 2 defined over a finite field $\mathbb{F}_q$, such that $C(\mathbb{F}_q)=\emptyset$, is $\mathbb{F}_q$-isomorphic to one of the curves listed in Table 4.*

The fact that $C(\mathbb{F}_{13})\neq\emptyset$ for all curves defined over $\mathbb{F}_{13}$ has already been observed by Stark [Stark 72].

4. ABELIAN SURFACES AS JACOBIANS

We are far from having a complete answer to the question of which isogeny classes of abelian surfaces contain a Jacobian. There is abundant literature about existence and nonexistence results for decomposable surfaces, with significant contributions by Serre, Hayashida-Nishi, Rück, Frey-Kani, Kani, Ibukiyama-Katsura, and Oort among others, although in some cases, the adaptation of the arguments to the finite field case is still to be done.

For simple surfaces, the situation is much clearer, principally because of a well-known result of Weil. Actually, we need a generalization of the classical result of [Weil 57], which can be easily deduced from the arguments of Section 5.10 of [Adleman and Huang 92]:

Theorem 4.1. (Weil, Adleman-Huang.) *Let A be a principally polarized abelian surface defined over a finite field k. If A is simple over the quadratic extension of k, then A is k-isomorphic to the Jacobian of a projective smooth curve of genus 2.*

Using this result, if A is simple over the quadratic extension of k, then the isogeny class of A contains a Jacobian if and only if it contains a principally polarized surface. This latter question has been completely solved in the ordinary case in [Howe 95]. Moreover, in Theorem 4.3 below, we use a criterion of Howe to prove that any simple surface of the family (M) of Theorem 2.9 is isogenous to a principally polarized surface. Thus, it remains to solve the question only for a scattered family of supersingular simple surfaces and for the simple sur-

faces with $a_1 = 0$, which, by Proposition 2.14, are the only nonsupersingular surfaces that decompose over the quadratic extension of k.

In any case, it is quite simple to carry out a computational exploration of the problem. We have written two programs Jac2,Jac2Ch2, which for a given (odd, respectively, even) prime power q display all isogeny classes of abelian surfaces A over $\mathbb{F}_q$, determine the decomposition type of A and count the number of projective smooth curves of genus 2 for which the Jacobian is isogenous to A.

As a first step, the program considers the pairs of integers (a_1, a_2) parameterizing all Weil polynomials (Lemma 2.1) and for each of them, it checks the conditions of Theorems 2.9 and 2.15 labeling each polynomial with one of the following symbols:

- **x** there exists no abelian surface corresponding to this pair (a_1, a_2)
- **a** absolutely simple
- **o** ordinary, simple, not absolutely simple
- **s** simple, supersingular
- **d** decomposes as $E_1 \times E_2$, with E_1, E_2 not $\mathbb{F}_q$-isogenous
- **e** decomposes as $E \times E$

This information is kept in the form of a matrix indexed by the values of (a_1, a_2), with the above symbols as entries. Once this matrix is obtained (with an insignificant expenditure of time), it is written as a first output of the program. Afterwards, the programs Gen2,Gen2Ch2 search for all curves of genus 2 over $\mathbb{F}_q$ and for each curve, they compute the pair (a_1, a_2) of relevant coefficients of the characteristic polynomial of its Jacobian and then add one to the entry $(|a_1|, a_2)$ of the matrix. Then, the programs produce as a second output the same matrix with the changes produced by counting the Jacobians. These subroutines can be downloaded at www.mat.uab.es/danielm.

For instance, for $q = 2, 3$, the two outputs of Jac2Ch2,Jac2 are given in Tables 5 and 6.

In the display of the matrix, the rows are indexed by increasing values of a_1, starting with $a_1 = 0$, whereas the columns are indexed by the values of a_2 within the bounds

$$2|a_1|\sqrt{q} - 2q \le a_2 \le \frac{a_1^2}{4} + 2q,$$

given by Lemma 2.1. To accommodate the reader we write the minimum value of a_2 corresponding to the first entry in the row at the beginning of each row.

a_1	min.a_2		
0	-4	sosodosde	**s o s** 1 1 1 **d e**
1	-1	oaadad	**o** 1 1 1 **d**
2	2	sade	1 1 **e**
3	5	od	1 **d**
4	8	e	**e**

TABLE 5. $q = 2$.

a_1	min.a_2		
0	-6	soodoosodsode	**s o o d** 2 1 1 1 2 1 1 1 **e**
1	-2	oadaaadad	1 1 1 2 2 2 1 1 **d**
2	1	oodaade	1 2 2 2 1 2 1
3	5	adad	1 1 1 **d**
4	8	ode	1 1 1
5	12	d	**d**
6	15	e	**e**

TABLE 6. $q = 3$.

Finally, the matrix has entries only with $a_1 \ge 0$ and the program takes into account only one curve for each pair C, C' of twisted curves. This is harmless after the following observation, which is an immediate consequence of Theorem 2.9, Theorem 2.15 and (3–2) of Section 3.2:

Lemma 4.2.

(i) For any $a_1, a_2 \in \mathbb{Z}$, the couples (a_1, a_2) and $(-a_1, a_2)$ have the same symbol **x,a,o,s,d,e** *attached as above.*

(ii) If C is a curve of genus 2 whose Jacobian corresponds to the couple (a_1, a_2), then the nontrivially twisted curve C' has Jacobian corresponding to the couple $(-a_1, a_2)$.

In particular, the figures occurring in the rows with $a_1 > 0$ give the exact number of k-isomorphy classes of curves whose Jacobian belongs to this isogeny class. Only in the row $a_1 = 0$ do the figures give the number of curves up to k-isomorphism and quadratic twist.

One can observe some regular behavior in the numerical results obtained by running the programs Jac2,Jac2Ch2 for all $q \le 49$.

4.1 Observations

For $q \le 49$, one can check that in the second output matrix:

1. There is no **a**.
2. In the last position of the odd rows, we find either an **x** or a **d**.

3. In the second position of the top row, we always find **o**. If $\mathrm{char}(k) \neq 2$, in the third position of the top row we find **o**, too.

4. Assume $q \geq 5$ and $p \neq 3$. Then, all other surfaces in the top row, apart from the two (one if $\mathrm{char}(k) = 2$) mentioned above, are Jacobians, with the only exception of $A = (0, -q)$ when q is not a square and $p \equiv 1 \pmod 3$ or $p = 2$, or when q is a square and $p \equiv 7 \pmod{12}$.

The first two observations can be generalized as follows:

Theorem 4.3. *Every absolutely simple abelian surface A defined over a finite field $\mathbb{F}_q$ is $\mathbb{F}_q$-isogenous to the Jacobian of a projective smooth curve of genus 2.*

Theorem 4.4. *Let a_1 be an odd integer, $|a_1| < 2[2\sqrt{q}]$. Let $a_2 = 2q + (a_1^2 - 1)/4$ be the largest integer such that (a_1, a_2) determine a Weil polynomial and assume that $(a_1 \pm 1)/2$ are q-Waterhouse numbers. Then, the abelian surface $A = (a_1, a_2)$ decomposes over $\mathbb{F}_q$ and it is not $\mathbb{F}_q$-isogenous to the Jacobian of a smooth projective curve of genus 2.*

Theorem 4.4 is an immediate consequence of a result of Serre ([Lauter 00], Lemma 1). For such a surface, we have $\Delta = 1$, so that A decomposes. Moreover, $\beta_1, \beta_2 = (a_1 \pm 1)/2$ are integers such that $\beta_1 - \beta_2 = \pm 1$; hence, the polynomial $(t - \beta_1)(t - \beta_2)$ factorizes in $\mathbb{Z}[t]$ as the product of two polynomials whose resultant is ± 1. By the result of Serre, $\pi_1, \bar{\pi}_1, \pi_2, \bar{\pi}_2$ cannot be the eigenvalues of Frobenius of a smooth projective curve of genus 2 defined over $\mathbb{F}_q$.

Theorem 4.4 can be reinterpreted in terms of number of points as follows: If we restrict our attention to curves C with a fixed value of $N_1 = \sharp C(\mathbb{F}_q)$, then the number N_2 of points of C over the quadratic extension is bounded by $a_2 \leq 2q + (a_1^2/4)$, which by (1–2) translates into

$$N_2 \leq 3q + (q+1)N_1 + \frac{q^2 + 1 - N_1^2}{2}.$$

Since $N_1 \equiv q \pmod 2$, the maximum possible value of N_2 would be

$$N_2 = 3q + (q+1)N_1 + \frac{q^2 - N_1^2}{2},$$

and Theorem 4.4 asserts that this value is never attained.

Theorem 4.3 is a consequence of Theorem 4.1, the work of [Howe 95], [Howe 96] and our characterization of the absolutely simple surfaces (Theorem 2.15).

Proof of Theorem 4.3: By Theorem 4.1, it is sufficient to show that any absolutely simple abelian surface A defined over $\mathbb{F}_q$ is $\mathbb{F}_q$-isogenous to a principally polarized one. If A is ordinary, this has been proved by Howe [Howe 95]. In fact, he proves that the parameters (a_1, a_2) of an ordinary abelian surface over $\mathbb{F}_q$ which is not isogenous to any principally polarized surface satisfy $q = a_1^2 - a_2$ and this implies that A decomposes over $\mathbb{F}_{q^3}$ by Proposition 2.13. For A nonordinary, Howe has found sufficient conditions for an abelian surface to be principally polarized, which are applicable in our case ([Howe 96], Prop. 7.2).

Let A be a nonordinary absolutely simple abelian surface. By Theorem 2.15, A is of type (M). The quartic field K generated by any root π of $f_A(t)$ is a CM field with $K^+ = \mathbb{Q}(\sqrt{\Delta})$ as the real quadratic subfield. The criterion of Howe asserts in this case that if there is a prime ideal that ramifies in K/K^+, or there is an inert prime ideal in K/K^+ dividing $\pi - \bar{\pi}$, then A is $\mathbb{F}_q$-isogenous to a principally polarized abelian surface. Let us check that this condition is always satisfied.

We denote by $\mathcal{O}, \mathcal{O}^+$ the respective rings of integers of K, K^+. Since $p \nmid \Delta$ and Δ is a quadratic residue modulo p (with $\Delta \equiv 1 \pmod 8$ if $p = 2$), the prime p decomposes in K^+:

$$p\mathcal{O}^+ = \wp\wp'. \tag{4–1}$$

On the other hand, $f_A(t)$ decomposes in $\mathbb{Q}_p[t]$ as

$$f_A(t) = (t^2 + \beta t + q)(t - \alpha_1)(t - \alpha_2),$$

with $t^2 + \beta t + q$ irreducible ([Rück 90], Lemma 3.2). Hence, p decomposes in $\mathcal{O}$ as

$$p\mathcal{O} = \mathcal{P}_1\mathcal{P}_2\mathcal{P}^2, \text{ or } p\mathcal{O} = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_{(2)}. \tag{4–2}$$

From $f_A(t) \equiv t^3(t + a_1) \pmod p$, we get by an old result of Kummer that p and $\pi + a_1$ are generators of one of the prime ideals $\mathcal{P}_1, \mathcal{P}_2$; let's say: $\mathcal{P}_1 = (p, \pi + a_1)$. The two decompositions (4–1), (4–2) imply that one of the prime ideals of $\mathcal{O}^+$ above p decomposes in $\mathcal{O}$ as the product $\mathcal{P}_1\mathcal{P}_2$ and the other is either ramified or inert (it is easy to determine when it is inert or ramified in terms of δ). Since $\mathrm{Gal}(K/K^+) = \{1, \sigma\}$, where σ is complex conjugation, we know explicit generators for $\mathcal{P}_2 = \mathcal{P}_1^\sigma$ too: $\mathcal{P}_2 = (p, \bar{\pi} + a_1)$. In particular, neither $\mathcal{P}_1$ nor $\mathcal{P}_2$ can divide $\pi - \bar{\pi}$; for instance,

$$\mathcal{P}_1 \mid \pi - \bar{\pi} = (\pi + a_1) - (\bar{\pi} + a_1) \Longrightarrow \mathcal{P}_1 \mid (\bar{\pi} + a_1)$$
$$\Longrightarrow \mathcal{P}_1 \supseteq \mathcal{P}_2,$$

a_1	min. a_2		
0	-8	doxosoxdsoxodoxde	**d o x** 2 1 2 **x** 2 2 4 **x** 4 2 2 **x** 1 1
1	-4	doaaaadaaadad	**d** 1 2 2 2 2 2 4 1 3 2 2 **d**
2	0	daxasdxade	**d** 3 **x** 4 2 4 **x** 4 **d** 1
3	4	doaodad	**d** 2 2 4 1 2 **d**
4	8	daxde	1 2 **x** 2 1
5	12	dad	**d** 1 **d**
6	16	de	**d e**
7	20	d	**d**
8	24	e	**e**

TABLE 7. $q = 4$.

a_1	min. a_2		
0	-10	sooodsoooosdooosdoode	1 **o o** 1 2 1 1 1 4 2 2 3 5 1 3 3 3 2 2 1 2
1	-5	aoadaaaaadaaadad	1 1 1 2 3 4 3 2 5 3 2 2 3 3 2 **d**
2	-1	oaadaaaadaade	**o** 2 2 5 3 4 2 6 6 2 1 4 1
3	4	oadaoadad	3 2 1 4 4 1 2 2 **d**
4	8	oadoade	1 2 3 2 3 3 1
5	13	adsd	1 1 2 **d**
6	17	ode	1 1 1
7	22	d	**d**
8	26	e	**e**

TABLE 8. $q = 5$.

which is impossible. But, $p \mid \delta$ and $\mathrm{N}_{K/\mathbb{Q}}(\pi - \bar{\pi}) = \delta$ (see Lemma 4.5 below); hence the other prime in $\mathcal{O}$ above p must divide $\pi - \bar{\pi}$ and the criterion of Howe is satisfied. □

Lemma 4.5. *Let A be an abelian surface defined over $\mathbb{F}_q$ such that $f_A(t) \in \mathbb{Z}[t]$ is irreducible. Let $K = \mathbb{Q}(\pi)$ be the quartic field generated by a root π of $f_A(t)$ in $\bar{\mathbb{Q}}$. Then,*

$$N_{K/\mathbb{Q}}(\pi - \bar{\pi}) = \delta := (a_2 + 2q)^2 - 4qa_1^2.$$

Proof: If $\pi_1, \bar{\pi}_1, \pi_2, \bar{\pi}_2$ are the four roots of $f_A(t)$ in $\bar{\mathbb{Q}}$, we have:

$$f_A(t) = (t^2 + \beta_1 t + q)(t^2 + \beta_2 t + q),$$

where $\beta_i = \pi_i + \bar{\pi}_i$ are real numbers. The invariant δ is the product, $\delta = d_1 d_2$, of the two discriminants of these quadratic factors. Hence, $\pi_i - \bar{\pi}_i = \pm\sqrt{d_i}$ and

$$\begin{aligned} \mathrm{N}_{K/\mathbb{Q}}(\pi - \bar{\pi}) &= (\pi_1 - \bar{\pi}_1)(\bar{\pi}_1 - \pi_1)(\pi_2 - \bar{\pi}_2)(\bar{\pi}_2 - \pi_2) \\ &= (-d_1)(-d_2) = \delta. \end{aligned}$$ □

We have not been able to check if the third and fourth observations above are true in general or not. By Theorem 2.9, the abelian surfaces $A_1 = (0, -2q + 1)$ and (for q odd) $A_2 = (0, -2q + 2)$ are simple and ordinary. By ([Howe 95], §13) they are $\mathbb{F}_q$-isogenous to the generalized Jacobian of a *good curve* in the sense of Oort-Ueno, but as our tables show, they seem to be not $\mathbb{F}_q$-isogenous to the Jacobian of a smooth curve.

Actually, we have run a modified version of our programs centering the attention only in curves with $N_1 = q + 1$ (that is, $a_1 = 0$) and we have checked that observations 3 and 4 remain true for $q \leq 64$. The assertion of Obervation 3 has been proved recently by Howe. His proof that A_1 is not isogenous to a Jacobian is included in Section 6. For the surface A_2, see [Howe 02].

5. COMPUTATIONAL RESULTS

In Tables 7–14, we collect the output of the programs Jac2, Jac2Ch2 for $4 \leq q \leq 16$. For each q, the output consists of two matrices, indexed by pairs of integers (a_1, a_2), corresponding to Weil polynomials. The content of the matrices is explained at the beginning of Section 4. For $q \geq 11$ only the second matrix is displayed.

a_1	min. a_2	
0	-14	soodooosoooodosoooodosoodoode
1	-8	aadaaaaaaaadaaaaadaaadad
2	-3	oadaaoaaadaaaadaade
3	2	oadaaaaadaaadad
4	8	odaaaadaade
5	13	adaaadad
6	18	odaade
7	24	dad
8	29	de
9	34	d
10	39	e

TABLE 9. $q = 7$.

a_1	min. a_2	
0	-16	soxoxoxdsoxoxoxodoxoxoxdsoxoxoxde
1	-10	xaaoxadaxaaaxadaxaaaxaaaxad
2	-4	xaxaxdxaxaxaxaxaxdxaxe
3	1	oxaaaxaaaxodaxadax
4	7	asaxdxaxadaxdx
5	13	axadoxadax
6	18	xaxdxaxe
7	24	aaxad
8	30	xde
9	35	od
10	41	e

TABLE 10. $q = 8$.

a_1	min. a_2	
0	-18	dooxooxoosodxooxoosodxooxoodooxodxode
1	-12	daaaoaaaaadaaaaaaadaaaaadaaxdad
2	-6	doaxaaaaodaaaaaadaaaadaade
3	0	daaxaaxadsaaxadxaadad
4	6	dooaaaxdaaaadaade
5	12	daaaoadaaadad
6	18	daaxadxade
7	24	daaadad
8	30	daode
9	36	dad
10	44	de
11	48	d
12	54	e

TABLE 11. $q = 9$.

a_1	min. a_2	
0	-22	1 o o 1 3 2 1 2 6 4 1 2 13 1 6 4 9 8 3 5 13 4 5 6 14 6 14 7 11 6 6 3 16 5 5 13 12 2 7 8 7 4 5 1 5
1	-15	1 4 2 4 4 3 7 5 5 10 9 4 9 12 8 4 6 16 8 10 6 8 13 4 12 14 12 6 13 8 5 10 4 10 5 4 5 **d**
2	-8	4 o 6 6 8 6 14 6 8 8 16 12 12 6 20 24 8 6 18 6 14 6 20 9 8 6 12 12 6 4 12 2
3	-2	2 2 2 8 12 2 8 8 4 14 4 4 20 8 6 15 10 4 12 12 6 10 4 3 8 4 **d**
4	5	4 9 4 9 4 14 4 14 14 12 4 9 11 13 8 6 12 15 4 6 6 5
5	12	2 5 7 7 4 9 10 8 4 4 8 4 4 5 4 5 **d**
6	18	2 6 4 2 16 9 4 11 12 6 10 2 4 5
7	25	3 4 4 3 2 4 5 4 2 **d**
8	32	3 4 6 2 4 6 3
9	38	2 1 2 3 **d**
10	45	1 2 1
11	51	1 **d**
12	58	1

TABLE 12. $q = 11$.

a_1	min.	a_2
0	-26	2 **o** **o** 1 5 1 2 3 4 4 2 6 9 **s** 3 4 17 4 9 4 16 8 4 6 14 8 12 13 9 6 6 12 20 4 12 8 30 2 7 10 16 12 7 5 11 9 7 5 13 4 5 5 4
1	-18	2 3 3 4 4 5 10 7 4 8 10 8 8 6 12 16 8 8 12 13 8 12 20 12 14 10 16 16 8 8 12 12 10 16 12 6 8 11 10 8 6 9 10 3 **d**
2	-11	2 6 4 8 6 16 7 4 8 24 6 18 6 23 12 12 12 12 20 8 8 28 16 28 6 12 18 6 10 32 18 12 4 18 12 8 3 8 6
3	-4	1 6 5 5 12 4 8 9 18 6 6 18 12 16 8 6 24 16 6 11 14 15 10 8 6 9 10 8 12 10 4 5 **d**
4	3	4 4 5 12 6 11 16 12 6 17 8 23 4 18 18 24 6 10 20 14 6 14 8 15 6 7 6 12
5	11	2 10 6 4 12 8 5 8 12 12 8 4 4 12 15 8 4 12 4 6 3 **d**
6	18	8 8 4 6 18 12 10 10 18 9 8 4 12 16 6 5 10 2
7	25	1 2 8 6 9 4 3 6 8 4 4 7 4 **d**
8	32	3 6 7 2 5 10 10 4 6 4 5
9	39	1 4 2 4 4 3 3 **d**
10	47	2 4 2 5 2
11	54	1 1 **d**
12	61	2 1
13	68	**d**
14	75	**e**

TABLE 13. $q = 13$.

a_1	min.	a_2
0	-32	1 **o** **x** 4 **x** 4 **x** 8 **x** 16 **x** 8 **x** 8 **x** 17 5 16 **x** 24 **x** 16 **x** 24 **x** 24 **x** 44 **x** 24 **x** 24 8 16 **x** 32 **x** 16 **x** 38 **x** 32 **x** 16 **x** 36 **x** 40 10 32 **x** 32 **x** 12 **x** 38 **x** 16 **x** 24 **x** 12 **x** 10 6
1	-24	**d** 4 **x** 8 4 8 **x** 8 4 10 **x** 16 8 12 **x** 16 4 16 **x** 16 12 16 **x** 24 8 25 **x** 36 8 20 **x** 32 4 28 **x** 16 16 32 **x** 16 8 16 **x** 20 8 32 **x** 24 2 18 **x** 24 8 8 **x** 8 **d**
2	-16	**x** 14 **x** 16 **x** 24 **x** 16 **x** 36 **x** 24 **x** 64 **x** 16 **x** 63 **x** 32 **x** 48 **x** 48 **x** 60 **x** 32 **x** 40 **x** 64 **x** 64 **x** 32 **x** 48 **x** 16 **x** 24 **x** 40 **x** 40 **x** 16 **x** 12
3	-8	**d** **o** **x** 8 6 20 **x** 8 8 20 **x** 24 8 20 **x** 40 **x** 16 **x** 16 16 16 **x** 24 12 28 **x** 40 8 24 **x** 24 4 34 **x** 24 10 8 **x** 16 4 8 **x**
4	0	**d** 8 **x** 32 **x** 16 **x** 32 **x** 36 **x** 48 **x** 32 **x** 32 10 36 **x** 72 **x** 32 **x** 32 **x** 28 **x** 68 **x** 16 **x** 32 d 16 **x** 20 **x**
5	8	**d** 16 **x** 4 8 8 **x** 24 4 24 **x** 16 8 16 **x** 16 4 16 **x** 32 10 16 **x** 8 4 20 **x** 16 4 12 **x**
6	16	**x** 12 **x** 24 **x** 40 **x** 24 **x** 40 **x** 32 **x** 24 **x** 32 **x** 48 **x** 16 **x** 40 **x** 16 **x** 8
7	24	1 4 **x** 16 4 12 **x** 16 4 29 **x** 8 8 24 **x** 8 1 8 **x** 4 **d**
8	32	4 8 **x** 16 **x** 16 **x** 34 **x** 24 **x** 16 **x** 16 **x** 16 5
9	40	**d** 6 **x** 12 4 12 **x** 8 4 15 **x** 8 **d**
10	48	**x** 12 **x** 8 **x** 16 **x** 8 **x** 6
11	56	**d** 4 **x** 4 2 4 **x**
12	64	**d** 4 **x** 8 **x**
13	72	**d** 2 **x**
14	80	**x** 1
15	88	**d**
16	96	1

TABLE 14. $q = 16$.

6. APPENDIX BY EVERETT W. HOWE

For every prime power q, let f_q denote the polynomial $x^4 + (1-2q)x^2 + q^2$. In Section 4 of this article, Maisner and Nart observe that for all prime powers $q \leq 64$, no genus-2 curve over $\mathbf{F}_q$ has characteristic polynomial f_q. (By the *characteristic polynomial* of a curve, we mean the characteristic polynomial of the Frobenius endomorphism of the Jacobian of the curve.) The purpose of this appendix is to prove that Maisner and Nart's observation holds for all prime powers q.

Theorem. *There is no curve of genus* 2 *over any finite field* $\mathbf{F}_q$ *whose characteristic polynomial is equal to* f_q.

Proof: Suppose, to obtain a contradiction, that C is a genus-2 curve over a finite field $\mathbf{F}_q$ whose characteristic polynomial is equal to f_q. Note that then $\#C(\mathbf{F}_q) = q+1$ and $\#C(\mathbf{F}_{q^2}) = (q-1)(q-3)$.

Let J be the Jacobian of C, let λ be the canonical principal polarization of J, let F be the Frobenius endomorphism of J, and let $V = q/F$ be the Verschiebung endomorphism of J. Since f_q is irreducible and its middle coefficient is coprime to q, we see that J is a simple ordinary abelian surface, and it follows that the ring $(\operatorname{End} J) \otimes \mathbf{Q}$ is equal to the field $\mathbf{Q}(F)$. In fact, this field is a totally imaginary quadratic extension of a totally real quadratic field, and general theory (see [Mumford 74, p. 201]) shows that the Rosati involution $x \mapsto x^\dagger$ on $\mathbf{Q}(F)$ is complex conjugation.

Let i be the endomorphism $F - V$ of J. It is easy to check that $i^2 = -1$, and it follows that $i^\dagger i = 1$. Thus i is an automorphism of J that respects the polarization λ, so i can be viewed as an automorphism of the

polarized abelian variety (J, λ). Since C is hyperelliptic, Torelli's theorem (see [Milne 86, p. 202]) shows that the natural map from the automorphism group of C to the automorphism group of (J, λ) is an isomorphism that takes the hyperelliptic involution to -1. Thus, the automorphism i of (J, λ) gives us an automorphism α of C, defined over $\mathbf{F}_q$, whose square is the hyperelliptic involution.

Let W denote the set of Weierstrass points of C, viewed as a set with an action of the absolute Galois group of $\mathbf{F}_q$. If P is a geometric point of C whose orbit under the action of α contains fewer than four points, then P must be fixed by $\alpha^2 = -1$, so P must lie in W. Thus, for every finite extension field k of $\mathbf{F}_q$ we have $\#C(k) \equiv \#W(k) \bmod 4$.

Suppose that q is odd. Then W consists of six points, and we will show that exactly two of these points are fixed by α.

Consider the map $C \to \mathbf{P}^1$ obtained from the hyperelliptic involution, and let W' denote the set of six points of $\mathbf{P}^1$ lying under the Weierstrass points of C. The automorphism α induces an involution β of $\mathbf{P}^1$ that takes the set W' to itself. Geometrically, this involution is conjugate to the involution $x \mapsto -x$, so if none of the points in W' were fixed by β the curve C would be isomorphic (over the algebraic closure of $\mathbf{F}_q$) to a curve of the form $y^2 = f(x^2)$, where f is a cubic polynomial. But then α would have to be of the form $(x, y) \mapsto (-x, \pm y)$, and such an automorphism has order two. Thus, β must fix at least one of the six points of W'. But the points not fixed by β come in plus/minus pairs, so there must be at least two points of W' fixed by β. Since $x \mapsto -x$ has exactly two fixed points in $\mathbf{P}^1$, there must be exactly two points of W' fixed by β. It follows that exactly two points of W are fixed by α, as claimed.

Since α is defined over $\mathbf{F}_q$, the two points of W fixed by α must be defined over $\mathbf{F}_{q^2}$. Thus, $\#W(\mathbf{F}_{q^2}) \geq 2$. But we also have

$$\#W(\mathbf{F}_{q^2}) \equiv \#C(\mathbf{F}_{q^2}) = (q-1)(q-3) \equiv 0 \bmod 4,$$

so we must have $\#W(\mathbf{F}_{q^2}) = 4$. But this is impossible, as one can see by asking where the other two points of W are defined. Thus, if q is odd, no curve can have characteristic polynomial f_q.

Suppose that q is a power of 2. Then q must be a multiple of 4, because if q were 2 the curve C would have -1 points over $\mathbf{F}_4$. We see that $\#W(\mathbf{F}_q) \equiv 1 \bmod 4$ and $\#W(\mathbf{F}_{q^2}) \equiv 3 \bmod 4$. But a genus-2 curve in characteristic 2 has at most three Weierstrass points, so C must have exactly three Weierstrass points, and exactly one of them is defined over $\mathbf{F}_q$.

Once again we let W' denote the points of $\mathbf{P}^1$ lying under the Weierstrass points of C and we let β be the involution of $\mathbf{P}^1$ obtained from α. Clearly β must fix the unique point of $W'(\mathbf{F}_q)$. But β cannot fix the other two points of W', because in that case β would be the identity on $\mathbf{P}^1$, and α could not have order four. Thus, β must swap the other two points of W'. It follows that over the algebraic closure of $\mathbf{F}_q$ we can write C as $y^2 + y = ax + b/x + b/(x+1)$, where we have chosen the coordinates so that β is given by $x \mapsto x + 1$. But then α must send (x, y) to $(x + 1, y + c)$ where $c^2 + c = a$, and this automorphism has order two. Once again we obtain a contradiction, and the theorem is proved. □

Maisner and Nart also note that for every odd prime power $q < 64$, no genus-2 curve over $\mathbf{F}_q$ has characteristic polynomial $g_q = x^4 + (2 - 2q)x^2 + q^2$. The obvious conjecture is that the same statement is true for all odd prime powers q. Unfortunately, the argument we used above cannot be easily modified to prove this conjecture; the critical fact we used was that the ring $\mathbf{Z}[F, V]$ contains a root of unity other than ± 1, and this is no longer true when we replace f_q with g_q in our argument. In a forthcoming paper [Howe 02], we will prove this conjecture using an argument that depends on the Brauer relations in a biquadratic number field.

ACKNOWLEDGMENTS

We thank the referee for several suggestions which have led us to give a more complete form to the paper. We are also grateful to Everett W. Howe for his extreme kindness in accepting that his proof of one of the questions raised by our computations appears as an appendix to the paper. The first author was supported by CONACYT; the second author was supported by DGI, BHA2000-0180.

REFERENCES

[Adleman and Huang 92] L. M. Adleman, M.-D. A. Huang. *Primality testing and abelian varieties over finite fields*, Lecture Notes in Mathematics 1512, Springer-Verlag, Berlin-Heidelberg, 1992.

[Cardona et al. 02] G. Cardona, E. Nart, and J. Pujolàs. *Curves of genus two over fields of even characteristic.* to appear, http://www.arxiv.org/math.NT/0210105.

[Guàrdia 98] J. Guàrdia. *Geometria Aritmètica en una família de corbes de gènere tres.* Tesi, Universitat de Barcelona, 1998.

[Howe 95] E. W. Howe. "Principally polarized abelian varieties over finite fields." *Transactions of the American Mathematical Society* **347** (1995), 2361–2401.

[Howe 96] E. W. Howe. "Kernels of polarizations of abelian varieties over finite fields." *Journal of Algebraic Geometry* **5** (1996), 583–608.

[Howe 02] E. W. Howe. "On the nonexistence of certain curves of genus two." *Compositio Mathematica*, to appear. arxiv:math.NT/0201311.

[Howe and Zhu 02] E. W. Howe and H. J. Zhu. "On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field." *Journal of Number Theory* **92** (2002), 139–163.

[Igusa 60] J.-I. Igusa. "Arithmetic variety of moduli for genus two." *Annals of Mathematics* **72** (1960), 612–649.

[Lachaud 91] G. Lachaud. "Artin-Schreier curves, exponential sums and the Carlitz-Uchiyama bound for geometric codes." *Journal of Number Theory* **39** (1991), 18–40.

[Lauter 00] K. Lauter. "Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points." *Proceedings of the American Mathematical Society* **128**:2 (2000), 369–374.

[López et al. 02] A. López, D. Maisner, E. Nart, and X. Xarles. "Orbits of galois invariant n-sets of $\mathbb{P}^1$ under the action of PGL_2." *Finite Fields and Their Applications* **8** (2002), 193–206.

[Milne 86] J. S. Milne. "Jacobian varieties." in *Arithmetic Geometry*, (G. Cornell and J. H. Silverman, eds.), pp. 167–212, Springer-Verlag, New York, 1986.

[Mumford 74] David Mumford. *Abelian Varieties*, 2nd ed., Oxford University Press, Oxford, 1974.

[Rück 90] H.-G. Rück. "Abelian surfaces and Jacobian varieties over finite fields." *Compositio Mathematica* **76** (1990), 351–366.

[Stark 72] H. Stark. "On the Riemann hypothesis in hyperelliptic function fields." in *Analytic Number Theory*, Proceedings of Symposia in Pure Mathematics, Vol. XXIV, pp. 285–302, American Mathematical Society, Providence, RI, 1973.

[Tate 69] J. Tate. "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après Honda)." in *Séminaire Bourbaki 1968/69, Exposé 352*, pp. 95–110, Lecture Notes in Mathematics 179, Springer-Verlag, Berlin 1971.

[van der Geer and van der Vlugt 92] G. van der Geer and M. van der Vlugt. "Supersingular curves of genus 2 over finite fields of characteristic 2." *Mathematische Nachrichten* **159** (1992), 73–81.

[Waterhouse 69] W. C. Waterhouse. "Abelian varieties over finite fields." *Annales Scientifiques de l'École Normale Supérieure (4)* **2** (1969), 521–560.

[Waterhouse and Milne 69] W. Waterhouse and J. Milne. "Abelian varieties over finite fields." in *1969 Number Theory Institute*, Proceedings of Symposia in Pure Mathematics, Vol. XX, pp. 53–64, American Mathematical Society, Providence, RI, 1971.

[Weil 57] A. Weil. "Zum Beweis des Torellischen Satzes." *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse IIa* (1957), 33–53.

[Xing 94] C. P. Xing. "The structure of the rational point groups of simple abelian varieties of dimension two over finite fields." *Archiv der Mathematik* **63** (1994), 427–430.

[Xing 96] C. P. Xing. "On supersingular abelian varieties of dimension two over finite fields." *Finite Fields and Their Applications* **2** (1996), 407–421.

Daniel Maisner, Departament de Matemàtiques Universitat Autònoma de Barcelona, Edifici C, 08193 Bellaterra, Barcelona, Spain (danielm@mat.uab.es)

Enric Nart, Departament de Matemàtiques Universitat Autònoma de Barcelona, Edifici C, 08193 Bellaterra, Barcelona, Spain (nart@mat.uab.es)

Everett W. Howe, Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1967 (however@alumni.caltech.edu)

Received January 18, 2001; accepted in revised form November 21, 2001.