Canad. J. Math. Vol. **59** (2), 2007 pp. 372–392

Zeta Functions of Supersingular Curves of Genus 2

Daniel Maisner and Enric Nart

Abstract. We determine which isogeny classes of supersingular abelian surfaces over a finite field k of characteristic 2 contain jacobians. We deal with this problem in a direct way by computing explicitly the zeta function of all supersingular curves of genus 2. Our procedure is constructive, so that we are able to exhibit curves with prescribed zeta function and find formulas for the number of curves, up to k-isomorphism, leading to the same zeta function.

Introduction

This paper was motivated by the problem of determining which isogeny classes of abelian surfaces over a finite field k contain jacobians. In [MN] we performed a numerical exploration of this problem which led to several conjectures. We present in this paper a complete answer for supersingular surfaces in characteristic 2 (Section 5). We deal with this problem in a direct way by computing explicitly the zeta function of all supersingular curves of genus two (Section 4). Our procedure is constructive, so that we are able to exhibit curves with prescribed zeta function and to count the number of curves, up to k-isomorphism, leading to the same zeta function.

We base our work on the ideas of van der Geer and van der Vlugt [VV1, VV2], who expressed the number of points of a supersingular curve of genus two in terms of certain invariants. In Section 2 we explicitly compute these invariants in terms of the coefficients of a defining equation and in Section 3 we compute the number of points of the curve over the quadratic extension in terms of objects defined over k.

1 Supersingular Curves of Genus 2 in Characteristic 2

In this section we review the results of van der Geer–van der Vlugt and we fix some notations. Let $k = \mathbb{F}_q$ be a finite field of even characteristic with $q = 2^m$. We recall some basic facts concerning the Artin–Schreier operator:

$$\mathrm{AS}\colon k \to k, \quad \mathrm{AS}(x) = x + x^2.$$

This is an $\mathbb{F}_2$-linear operator with kernel $\mathbb{F}_2$. The image $\mathrm{AS}(k)$ is an $\mathbb{F}_2$-subspace of k of codimension one; hence, $|\mathrm{AS}(k)| = q/2$ and $k/\mathrm{AS}(k) \simeq \mathbb{F}_2$.

We shall denote simply by Tr or Tr_k the absolute trace $\mathrm{Tr}_{k/\mathbb{F}_2}$. For any $x \in k$ we have $\mathrm{Tr}(x) = \mathrm{Tr}(x^2)$, because x^2 is a galois conjugate of x over the prime field $\mathbb{F}_2$. Therefore, $\mathrm{AS}(k) = \mathrm{Ker}(\mathrm{Tr})$.

Received by the editors September 17, 2004.
The authors acknowledge support from project BFM-2003-06092 of MCYT.
AMS subject classification: Primary: 11G20, 14G15; secondary: 11G10.

For any $a \in k$, the polynomial $x^2 + x + a \in k[x]$ is separable. Its roots are in k if and only if $a \in \mathrm{AS}(k)$.

Lemma 1.1 *A quadratic polynomial $f(x) = x^2 + ax + b \in k[x]$ is separable if and only if $a \neq 0$; in this case, $f(x)$ is irreducible if and only if $b/a^2 \notin \mathrm{AS}(k)$.*

Throughout the paper we shall denote by $\mu_n \subseteq \bar{k}$ the group of the n-th roots of 1 and we let $\epsilon \in \mu_3$ be a fixed root of the polynomial $x^2 + x + 1$. Also, we denote $k_n := \mathbb{F}_{q^n}$. Note that $k \subseteq \mathrm{AS}(k_2)$, since $\mathrm{Tr}_{k_2/k}(k) = 0$. Clearly,

$$\begin{aligned} 1 \in \mathrm{AS}(k) &\iff \quad \mathbb{F}_4 \subseteq k \iff m \text{ even},\\ \mu_3 \subseteq k &\iff (k^*)^3 \subsetneq k^* \iff m \text{ even},\\ \mu_3 \subseteq \mathrm{AS}(k) &\iff \quad \mathbb{F}_{16} \subseteq k \iff m \equiv 0 \pmod 4,\\ \mu_5 \subseteq k &\iff (k^*)^5 \subsetneq k^* \iff m \equiv 0 \pmod 4. \end{aligned}$$

Every projective smooth curve of genus 2, defined over k and supersingular, *i.e.,* with supersingular jacobian, admits an affine model of the type:

$$C\colon y^2 + y = ax^5 + bx^3 + cx + d, \quad a \in k^*,\ b, c \in k,\ d \in k/\,\mathrm{AS}(k), \tag{1}$$

which has only one point at infinity. We can think that the term d takes only two values, $d = 0$ or $d = d_0$, with $d_0 \in k - \mathrm{AS}(k)$ fixed. To apply the *hyperelliptic twist* to the curve C consists in adding d_0 to the defining equation. If we denote by C^τ the twisted curve, we have

$$|C(\mathbb{F}_q)| + |C^\tau(\mathbb{F}_q)| = 2q + 2. \tag{2}$$

The curves C and C^τ are isomorphic over the quadratic extension of k through the mapping $(x, y) \mapsto (x, y + u)$, where $u \in k_2$ satisfies $u + u^2 = d_0$.

Throughout the paper by abuse of terminology, we identify the curve C given by (1) with the 4-tuple (a, b, c, d) of parameters involved in the defining equation.

Remark 1.2 The mappings $(x, y) \mapsto (x, y + cx)$, $(x, y) \mapsto (x, y + cx + c^2x^2)$ set respective k-isomorphisms between the curve (1) and the curves

$$y^2 + y = ax^5 + bx^3 + c^2x^2 + d, \qquad y^2 + y = ax^5 + c^4x^4 + bx^3 + d,$$

which are the models used respectively in [VV1, CNP]. We ask the reader to pay attention to this change of models when we quote results from these two papers.

By (2), in order to study the number of points of these curves, we can assume $d = 0$. Consider the linear polynomial $R(x) = ax^4 + bx^2 + c^2x$. Since $\mathrm{Tr}(cx) = \mathrm{Tr}(c^2x^2)$, the function:

$$Q\colon k \to \mathbb{F}_2, \quad x \mapsto \mathrm{Tr}(ax^5 + bx^3 + cx) = \mathrm{Tr}(xR(x)),$$

is a quadratic form associated with the simplectic form:

$$k \times k \to \mathbb{F}_2, \quad (x, y) \mapsto \langle x, y \rangle_R = \operatorname{Tr}(xR(y) + yR(x)),$$

since clearly,

$$Q(x + y) = Q(x) + Q(y) + \langle x, y \rangle_R, \quad \forall x, y \in k. \tag{3}$$

The number of zeros of Q determines the number of points of C:

$$|C(\mathbb{F}_q)| = 1 + 2|Q^{-1}(0)|.$$

The radical of the simplectic form $\langle\,,\rangle_R$ coincides with the set of roots in k of the $\mathbb{F}_2$-linear and separable polynomial (independent of c):

$$E_{ab}(x) := a^4x^{16} + b^4x^8 + b^2x^2 + ax.$$

Let $\overline{W} = \operatorname{Ker}(E_{ab})$ denote the subspace of $\bar{k}$ formed by the 16 roots of this polynomial. We denote

$$W := \operatorname{rad}\langle\,,\rangle_R = \overline{W} \cap k, \quad w := \dim_{\mathbb{F}_2}(W), \quad 0 \le w \le 4.$$

From (3) we deduce:

$$Q(x + y) = Q(x) + Q(y), \quad \forall x \in k,\ y \in W.$$

In particular, Q defines a linear form, $Q\colon W \to \mathbb{F}_2$. The space $V := \operatorname{Ker}(Q_{|W})$ controls the behaviour of Q on the classes $x + W$; for all $x \in k$, $y \in W$:

$$Q(x + y) = Q(x) \iff y \in V.$$

This subspace V of W has codimension 0 or 1. If $V \subsetneq W$, in each class $x + W$ the quadratic form Q vanishes on half of the elements; therefore $|Q^{-1}(0)| = q/2$ and $|C(\mathbb{F}_q)| = 1 + q$.

If $V = W$, the quadratic form Q is constant on each class $x + W$. Hence, it factorizes through a quadratic form, which we still denote by Q,

$$Q\colon k/W \to \mathbb{F}_2,$$

associated to the non-degenerate simplectic form induced by $\langle\,,\rangle_R$ on k/W. In particular, the dimension of k/W is even, so that m, w have the same parity. Moreover, if $m - w = 2n$, the number of zeros of Q can take only two values: $2^{n-1}(2^n + 1)$ or $2^{n-1}(2^n - 1)$. Thus,

$$|C(\mathbb{F}_q)| = 1 + 2\left(2^w(2^{n-1}(2^n \pm 1))\right) = 1 + q \pm \sqrt{2^w q}.$$

Summarizing,

Theorem (van der Geer–van der Vlugt).

$$V \subsetneq W \Rightarrow |C(\mathbb{F}_q)| = 1 + q,$$
$$V = W \Rightarrow |C(\mathbb{F}_q)| = 1 + q \pm \sqrt{2^w q}.$$

There are, thus, three invariants that determine the number of points of C: the dimension w of the space W, the codimension 0 or 1 of the subspace $V \subseteq W$ and the sign "+" or "−" indicating the parity, even or odd, of the quadratic form Q, in the case $V = W$. Actually, the last two invariants can be unified using the following terminology:

$$\operatorname{sgn}(Q) := \begin{cases} 0 & \text{if } V \subsetneq W, \\ +/- & \text{the parity of } Q_{|(k/W)}, \text{ if } V = W. \end{cases}$$

We end this section of preliminaries by recalling the conditions that are necessary and sufficient for two models (1) to give k-isomorphic curves. In general (*cf.* [VV2, Lemma 2.3] or [CNP, Proposition 10]), the supersingular curves given respectively by (a, b, c, d), (a', b', c', d') are k-isomorphic if and only if there exist $\lambda \in k^*$, $\nu \in k$ such that

$$(4) \qquad (a', b', c', d') = \left(\lambda^5 a, \lambda^3 b, \lambda\left(c + \sqrt[4]{E_{ab}(\nu)}\right), a\nu^5 + b\nu^3 + c\nu + d\right),$$

the equality $d' = a\nu^5 + b\nu^3 + c\nu + d$ being understood in $k/\operatorname{AS}(k)$.

There are $4q - 2 + [8]_{4|m}$ k-isomorphism classes of supersingular curves [CNP, Theorem 2], where $+[8]_{4|m}$ means "add 8 if $4 \mid m$".

The two cases $b = 0$, $b \neq 0$, give disjoint families of isomorphism classes. The curves with $b = 0$ are all isomorphic to the curve $y^2 + y = x^5$ over $\bar{k}$ and they have 160 automorphisms. The curves with $b \neq 0$ are $\bar{k}$-isomorphic to curves of the type $y^2 + y = a(x^5 + x^3)$ and have 32 automorphisms.

Note that if $b \neq 0$, we can achieve $\lambda^5 a = \lambda^3 b$ by taking $\lambda = \sqrt{b/a}$. Hence, in this case we can always assume that $a = b$.

As a consequence of (4) we see that any curve with $|C(\mathbb{F}_q)| = q+1$ is isomorphic to its own hyperelliptic twist. In fact, since $V \subsetneq W$, there exists $\nu \in W$ with $Q(\nu) \neq 0$, that is, $a\nu^5 + b\nu^3 + c\nu \notin \operatorname{AS}(k)$. Hence, the curve $(a, b, c, 0)$ is isomorphic to the curve (a, b, c, d_0).

2 Computation of the Invariants W, V

In this section we compute explicitly the subspaces W, V in terms of the parameters a, b, c of the defining equation of the curve.

2.1 Computation of W

The polynomial E_{ab} factorizes in $k[x]$ [VV1, Theorem 3.4]:

$$\begin{aligned} E_{ab}(x) &= a^4x^{16} + b^4x^8 + b^2x^2 + ax \\ &= x(a^2x^5 + b^2x + a)(a^2x^{10} + b^2x^6 + ax^5 + 1) = xP(x)(1 + x^5P(x)), \end{aligned}$$

with $P(x) := P_{ab}(x) := a^2x^5 + b^2x + a$. Hence, we have $v^5P(v) = 1, 0$ respectively for $10, 6$ elements $v \in \overline{W}$.

Lemma 2.1

(i) *Any family of four roots of $P(x)$ is a basis of $\overline{W}$.*
(ii) *The ten elements $v \in \overline{W}$ such that $v^5P(v) = 1$ can be expressed in a unique way as the sum of two roots of $P(x)$.*

Proof Let $z_1, z_2, z_3, z_4, z_5 \in \bar{k}$ be the roots of $P(x)$ and let us check that z_1, z_2, z_3, z_4 are linearly independent. They are all non-zero and different, hence, the sum of any two of them cannot vanish. Since $z_1 + z_2 + z_3 + z_4 + z_5 = 0$, the sum of any three or four of them cannot vanish either.

The ten elements $z \in \overline{W}$, such that $vP(v) = 1$ are the sum of two or three of the elements of the basis. In any case, they are the sum of two roots of $P(x)$, uniquely determined. ∎

Lemma 2.2 *Let $v = z + z'$ be a root in k of $v^5P(v) = 1$, with z, z' roots of $P(x)$. Then*

$$(av^5)^{-1} \in \mathrm{AS}(k) \implies z, z' \in k,$$
$$(av^5)^{-1} \notin \mathrm{AS}(k) \implies z, z' \in k_2 - k \text{ and they are conjugate over } k.$$

Proof Let us impose that $v + z$ is a root of $P(x)$:

$$\begin{aligned} 0 &= a^2(v+z)^5 + b^2(v+z) + a = a^2v^5 + a^2v^4z + a^2vz^4 + a^2z^5 + b^2v + b^2z + a \\ &= a^2v^5 + a^2v^4z + a^2vz^4 + b^2v = v(a^2v^4 + a^2v^3z + a^2z^4 + b^2). \end{aligned}$$

We deduce that $a^2v^4 + a^2v^3z + a^2z^4 + b^2 = 0$. If we multiply by z and apply $a^2z^5 + b^2z = a$, we get $a^2v^3z^2 + a^2v^4z + a = 0$, or equivalently, $z^2 + vz + (av^3)^{-1} = 0$. Since $v \neq 0$, this equation in z is separable and the two roots are z, z'. By Lemma 1.1, the roots belong to k if and only if $(av^5)^{-1} \in \mathrm{AS}(k)$. ∎

We are ready to see that the factorization of $P(x)$ as a product of irreducible polynomials determines w. We shall write $P(x) = (n_1)(n_2)\cdots(n_t)$ to indicate that $P(x)$ factorizes in $k[x]$ as the product of t irreducible polynomials of degrees $n_1,\ n_2, \ldots, n_t$.

Proposition 2.3 *Let $P(x) = a^2x^5 + b^2x + a$, with $a \in k^*$, $b \in k$. Then,*

(i) $w = 0 \iff P(x)$ *is irreducible.*
(ii) $w = 1 \iff P(x) = (1)(4)$ *or* $P(x) = (2)(3)$.
(iii) $w = 2 \iff P(x) = (1)(1)(3)$ *or* $P(x) = (1)(2)(2)$.
(iv) $w = 3 \iff P(x) = (1)(1)(1)(2)$.
(v) $w = 4 \iff P(x) = (1)(1)(1)(1)(1)$.

Proof If $P(x) = (1)(1)(1)(1)(1)$, we have $W = \overline{W}$ by Lemma 2.1 and $w = 4$.

If $P(x) = (1)(1)(1)(2)$, we have $W \subsetneq \overline{W}$ and W contains the three roots of $P(x)$ in k, which are linearly independent by Lemma 2.1. Hence, $w = 3$.

Suppose that $P(x) = (1)(1)(3)$ and let z, z' be the roots of $P(x)$ in k. By Lemma 2.2, $z + z'$ is the only root of $1 + x^5P(x)$ that belongs to k. Hence, W is the subspace generated by z, z' and $w = 2$. Now suppose that $P(x) = (1)(2)(2)$. By Lemma 2.2, the two traces of the quadratic factors of $P(x)$ are the only roots of $1 + x^5P(x)$ that belong to k. Thus, W has four elements and $w = 2$.

Similarly, by Lemma 2.2 we have $w = 1$ if $P(x) = (1)(4)$ or $P(x) = (2)(3)$, and we have $w = 0$ if $P(x)$ is irreducible.

Since we have considered all possible factorizations of $P(x)$, the converse implications hold too. ■

We proceed now to find explicit criteria to determine the factorization type of $P(x)$ in terms of a, b. We start with an auxiliary result.

Lemma 2.4 *Let $e \in k^*$. The polynomial $f(x) = x^4 + x^3 + x^2 + x + e$ has the following decomposition in $k[x]$ as a product of irreducible factors:*

$$\begin{array}{lll}
e \notin (k^*)^3 & \Longrightarrow & f(x) = (1)(3), \\
e = \lambda^3,\ \lambda \in k - \mathrm{AS}(k),\ m \text{ odd} & \Longrightarrow & f(x) \text{ is irreducible}, \\
e = \lambda^3,\ \lambda \in \mathrm{AS}(k),\ m \text{ odd} & \Longrightarrow & f(x) = (1)(1)(2), \\
e = \lambda^3,\ \lambda\mu_3 \not\subseteq \mathrm{AS}(k),\ m \text{ even} & \Longrightarrow & f(x) = (2)(2), \\
e = \lambda^3,\ \lambda\mu_3 \subseteq \mathrm{AS}(k),\ m \text{ even} & \Longrightarrow & f(x) = (1)(1)(1)(1).
\end{array}$$

Proof We check first that $e = \lambda^3$, $\lambda \in \mathrm{AS}(k)$, are necessary and sufficient conditions in order that $f(x)$ decomposes in $k[x]$ as the product of two polynomials of degree 2, not necessarily irreducible. In fact, assume that we have such a decomposition:

$$x^4 + x^3 + x^2 + x + e = (x^2 + ux + s)(x^2 + (u + 1)x + t). \tag{5}$$

This amounts to

$$s + t = 1 + u + u^2, \quad u(s + t) + s = 1, \quad st = e.$$

From the first and second equations we deduce $s = (u + 1)^3$, $t = u^3$, so that $e = (u + u^2)^3$. Conversely, if $e = \lambda^3$ and $\lambda = u + u^2$, with $\lambda, u \in k$, we get the decomposition above by taking $s = (u + 1)^3$, $t = u^3$.

By Lemma 1.1, the quadratic factor $x^2 + ux + (u + 1)^3$ is irreducible if and only if $(u + 1)^3/u^2$ does not belong to $\mathrm{AS}(k)$. Since $(u + 1)^3/u^2 = u + 1 + u^{-1} + u^{-2}$, this condition is equivalent to $u+1 \notin \mathrm{AS}(k)$. Similarly, the quadratic factor $x^2+(u+1)x+u^3$ is irreducible if and only if $u \notin \mathrm{AS}(k)$.

Now we start the proof of the lemma. Assume that $e \notin (k^*)^3$. Then $x^3 + e$ is irreducible in $k_2[x]$. Therefore, $f(x) = (1)(3)$, since this is the only factorization for which $f(x)$ is not the product of two polynomials of degree 2 over k_2.

If m is odd, then $e = \lambda^3$ for a unique $\lambda \in k$. If $\lambda \notin \mathrm{AS}(k)$, then $f(x)$ does not factorize as the product of two polynomials of degree 2 in $k[x]$, but it admits such a factorization over $k_2[x]$; hence, $f(x)$ is irreducible. On the other hand, if $\lambda = u + u^2$, with $u \in k$, we have a factorization (5). Now, since m is odd, we have $1 \notin \mathrm{AS}(k)$ and necessarily $f(x)$=(1)(1)(2), since exactly one of the two conditions, $u + 1 \notin \mathrm{AS}(k)$, $u \notin \mathrm{AS}(k)$, is satisfied.

Suppose now that $e \in (k^*)^3$ and m is even. If $\lambda^3 = e$, with $\lambda \in k$, the elements $\lambda\epsilon$ and $\lambda\epsilon^2$ are cubic roots of e, too. Since their sum is zero, either all three belong to $\mathrm{AS}(k)$, or only one of them. This corresponds to $f(x)$ having three different decompositions (5) or only one, that is, to $f(x) = (1)(1)(1)(1)$ or $f(x) = (2)(2)$. ■

In order to study the decomposition of $P_{ab}(x)$, we can assume that $b = 0$ or $b = a$, as remarked at the end of Section 1.

Proposition 2.5 *Let $a \in k^*$ and $P_{a0}(x) = a^2(x^5 + a^{-1})$. Then*

$$P_{a0}(x) = \begin{cases} (1)(4) & \text{if } m \text{ is odd,} \\ (1)(2)(2) & \text{if } m \equiv 2 \pmod 4, \\ (1)(1)(1)(1)(1) & \text{if } m \equiv 0 \pmod 4,\ a \in (k^*)^5, \\ \textit{irreducible} & \text{if } m \equiv 0 \pmod 4,\ a \notin (k^*)^5. \end{cases}$$

Proof Suppose first $a \notin (k^*)^5$, or equivalently, that $P_{a0}(x)$ has no roots in k. We have necessarily $m \equiv 0 \pmod 4$ and $\mu_5 \subseteq k$. Thus, if we adjoin to k any root of $P_{a0}(x)$, this polynomial will split completely in the larger field. Thus, $P_{a0}(x)$ cannot be (2)(3) and it must be irreducible.

Suppose now $a \in (k^*)^5$ and let $z \in k$ satisfy $z^5 = a^{-1}$. We have

$$x^5 + a^{-1} = (x + z)(x^4 + zx^3 + z^2x^2 + z^3x + z^4),$$

and the quartic factor has the same factorization type as the polynomial $x^4 + x^3 + x^2 + x + 1$ that was studied in Lemma 2.4. ■

Proposition 2.6 *Let $a \in k^*$ and $P_{aa}(x) = a^2(x^5 + x + a^{-1})$. Suppose that $P_{aa}(x)$ has no roots in k. Then*

$$P_{aa}(x) = \begin{cases} (2)(3) & \text{if } m \text{ odd,} \\ \textit{irreducible} & \text{if } m \text{ even.} \end{cases}$$

Suppose that $P_{aa}(x)$ has a root $z \in k$. Then for $e = 1 + z^{-4}$, we have

$$P_{aa}(x) = \begin{cases} (1)(1)(3) & \text{if } e \notin (k^*)^3, \\ (1)(4) & \text{if } e = \lambda^3, \lambda \in k - \mathrm{AS}(k), m \text{ odd,} \\ (1)(1)(1)(2) & \text{if } e = \lambda^3, \lambda \in \mathrm{AS}(k), m \text{ odd,} \\ (1)(2)(2) & \text{if } e = \lambda^3, \lambda\mu_3 \not\subseteq \mathrm{AS}(k), m \text{ even,} \\ (1)(1)(1)(1)(1) & \text{if } e = \lambda^3, \lambda\mu_3 \subseteq \mathrm{AS}(k), m \text{ even.} \end{cases}$$

https://doi.org/10.4153/CJM-2007-016-6 Published online by Cambridge University Press

Proof If the polynomial has no roots in k, the assertion is a consequence of Proposition 2.3 and the fact that m and w have the same parity.

If the polynomial has some root $z \in k$, then

$$x^5 + x + a^{-1} = (x + z)(x^4 + zx^3 + z^2x^2 + z^3x + z^4 + 1),$$

and the quartic factor has the same decomposition type as the polynomial $x^4 + x^3 + x^2 + x + (1 + z^{-4})$ that was obtained in Lemma 2.4 ■

This result allows us to count the number of times that each decomposition of $P_{aa}(x)$ appears, when a varies. In Section 4, this computation is crucial to finding explicit formulas for the number of curves with prescribed zeta function.

Corollary 2.7 *The following two tables give the number of values of $a \in k^*$ leading to each of the possible factorizations of $P_{aa}(x)$ in the cases m odd and m even, respectively.*

(2)(3)	(1)(1)(1)(2)	(1)(4)
$(q+1)/3$	$(q-2)/6$	$(q/2)-1$

(1)(1)(3)	(1)(2)(2)	(1)(1)(1)(1)(1)	irreducible
$(q-1)/3$	$(q/4)-[1]_{4\nmid m}$	$((q-4)/60)-\left[\frac{1}{5}\right]_{4\mid m}$	$\frac{2}{5}(q+1-[2]_{4\mid m})$

Proof Suppose that m is odd. By Proposition 2.6, the values of $a \in k^*$ leading to $P_{aa}(x) = (1)(4)$ are parameterized by elements $\lambda \in k - \mathrm{AS}(k)$, $\lambda \neq 1$, via

$$1 + z^{-4} = \lambda^3, \quad a = (z^5 + z)^{-1}. \tag{6}$$

These two relations set λ in a one-to-one correspondence with z (since $(k^*)^3 = k^*$) and z in a one-to-one correspondence with a (since $z^5 + z = a^{-1}$ has only one root). We get $(q/2) - 1$ values of a.

Similarly, the values of $a \in k^*$ leading to $P_{aa}(x) = (1)(1)(1)(2)$ are parameterized by choosing $\lambda \in \mathrm{AS}(k)$, $\lambda \neq 0$ and taking z, a as before. The relation between λ and z is still one-to-one, but now there are three different values of z linked to the same a. We get $1/3$ of the values computed above.

All other values of $a \in k^*$ lead to $P_{aa}(x) = (2)(3)$.

Now suppose m even. There are $2(q-1)/3$ values of $z \in k$ satisfying $1 + z^{-4} \notin (k^*)^3$, and each pair of these values give the same $a = (z^5 + z)^{-1}$. We have thus $(q-1)/3$ values of a with $P_{aa}(x) = (1)(1)(3)$.

https://doi.org/10.4153/CJM-2007-016-6 Published online by Cambridge University Press

In order to ensure the factorization $P_{aa}(x) = (1)(2)(2)$, we take $\lambda \notin \mathrm{AS}(k) \cup \mathbb{F}_4$ and consider z, a determined by (6). The fact that $\lambda \notin \mathbb{F}_4$ guarantees that $z \neq 0, 1$ and $a \neq 0$. The number of different values of λ with these properties is

$$(7) \qquad \frac{q}{2} - 2, \text{ if } 4 \nmid m, \quad \frac{q}{2}, \text{ if } 4 \mid m.$$

Since $\lambda + \lambda\epsilon + \lambda\epsilon^2 = 0$, in the pair $\lambda\epsilon$, $\lambda\epsilon^2$ exactly one element belongs to $\mathrm{AS}(k)$. The element not belonging to $\mathrm{AS}(k)$ and λ both give the same value of a. Hence, the number of values of a is half of the quantities given in (7).

For $P_{aa}(x)$ to split completely, we have to take $\lambda \in k$ such that $\lambda, \lambda\epsilon \in \mathrm{AS}(k)$; this will ensure that $\lambda\mu_3 \subseteq \mathrm{AS}(k)$. By the non-degeneracy of the pairing $\mathrm{Tr}(xy)$, there are $q/4$ values of $\lambda \in k$ with this property: $\lambda \in \langle 1, \epsilon \rangle^{\perp} = \mathbb{F}_4^{\perp}$. Also, we need $\lambda \notin \mathbb{F}_4$ in order that $z \neq 0, 1$. Since $\mathbb{F}_4^{\perp} \cap \mathbb{F}_4 = \{0\}$ if $4 \nmid m$ and $\mathbb{F}_4^{\perp} \supseteq \mathbb{F}_4$ if $4 \mid m$, the number of values of λ is,

$$(8) \qquad \frac{q}{4} - 1 \text{ if } 4 \nmid m, \quad \frac{q}{4} - 4, \text{ if } 4 \mid m.$$

Every three values of λ give the same z and every five values of z give the same a. Hence, the number of different values of a is obtained by dividing by 15 the numbers given in (8).

All other values of $a \in k^*$ lead to $P_{aa}(x)$ irreducible. ■

2.2 Computation of V

We can use Lemmas 2.1 and 2.2 to reinterpret the linear form $Q_{|W}$ in a way that provides an explicit computation of $\mathrm{codim}(V, W)$. Let us start with some remarks on linear forms over k. For any $c \in k$, let us denote by L_c the linear form,

$$L_c \colon k \to \mathbb{F}_2, \quad x \mapsto \mathrm{Tr}_k(cx).$$

The non-degeneracy of the pairing $\mathrm{Tr}(xy)$ allows us to consider a linear isomorphism:

$$L \colon k \to \mathrm{Hom}(k, \mathbb{F}_2), \quad c \mapsto L_c$$

In particular, for any subspace $W \subseteq k$ of dimension w, the linear mapping,

$$L \colon k \to \mathrm{Hom}(W, \mathbb{F}_2), \quad c \mapsto L_{c\,|W},$$

is onto and each linear form over W has $q/2^w$ preimages.

Proposition 2.8 *Let (a, b, c, d) be parameters defining a supersingular curve* (1)*. Let $\ell, \ell_c \colon W \to \mathbb{F}_2$ be the linear forms determined by:*

$$\begin{aligned} \ell(z) &= \mathrm{Tr}(1), && \text{if } P(z) = 0, \\ \ell(v) &= 0, && \text{if } v = z + z', \text{ with } z, z' \text{ roots of } P(x) \text{ in } k, \\ \ell(v) &= 1, && \text{if } v = z + z', \text{ with } z, z' \text{ roots of } P(x) \text{ in } k_2 - k, \end{aligned}$$

and $\ell_c = L_{c+b^2a^{-1}}$ restricted to W. Then $Q_{|W} = \ell_c + \ell$. In particular, $V = W$ if and only if $\ell_c = \ell$.

Proof Suppose that $P(z) = 0$, with $z \in k$. We have $a^2z^5 + b^2z + a = 0$. If we multiply by z^5, we get $az^5 + a^2z^{10} = b^2z^6$, so that $b^2z^6 \in \mathrm{AS}(k)$ and, in consequence, $bz^3 \in \mathrm{AS}(k)$. We can now compute

$$Q(z) = \mathrm{Tr}(az^5 + bz^3 + cz) = \mathrm{Tr}(b^2a^{-1}z + 1 + cz) = \ell_c(z) + \mathrm{Tr}(1).$$

If $v^5P(v) = 1$, we have $a^2v^{10} + b^2v^6 + av^5 + 1 = 0$, so that $b^2v^6 \equiv 1 \pmod{\mathrm{AS}(k)}$ and, in consequence, $bv^3 \equiv 1 \pmod{\mathrm{AS}(k)}$. On the other hand,

$$av^5 = b^2a^{-1}v + 1 + (av^5)^{-1},$$

so that,

$$av^5 + bv^3 \equiv b^2a^{-1}v + (av^5)^{-1} \pmod{\mathrm{AS}(k)}.$$

By Lemma 2.2, $\mathrm{Tr}((av^5)^{-1}) = 0, 1$ according to z, z' belonging to k or to $k_2 - k$. This ends the proof. ∎

Note that ℓ depends on a, b and ℓ_c depends on a, b, c. Thus, for a, b fixed, the invariant $\mathrm{codim}(V, W)$ is determined by the linear form ℓ_c, or equivalently, by the linear form $L_{c|W}$. Let us check now that this linear form determines in most of the cases the k-isomorphism class of the curve too, up to hyperelliptic twist.

Lemma 2.9 *Let $C = (a, b, c, 0)$ and suppose that $b \neq 0$ or $4 \nmid m$. Then for any $c' \in k$, the following conditions are equivalent:*

(i) *$C' = (a, b, c', 0)$ is k-isomorphic to C, if $V \subsetneq W$,*
$C' = (a, b, c', 0)$ is k-isomorphic either to C or to C^τ, if $V = W$.
(ii) $c' \in c + \sqrt[4]{E_{ab}(k)}$,
(iii) $L_{c|W} = L_{c'|W}$,
(iv) $\ell_c = \ell_{c'}$.

Proof Conditions (i) and (ii) are equivalent by (4), since our hypothesis on b and/or m imply that $\lambda = 1$ in (4).

In order to check that (ii) and (iii) are equivalent, let us show that $E_{ab}(k) = (W^4)^\perp$, where the orthogonal is taken with respect to the isomorphism of k with its dual obtained from the perfect pairing $\mathrm{Tr}(xy)$. In fact, for an arbitrary $\nu \in k$ we have

$$0 = \langle z, \nu \rangle_R = \mathrm{Tr}(z(a\nu^4 + b\nu^2) + \nu(az^4 + bz^2)), \quad \forall z \in W. \tag{9}$$

Clearly,

$$z(a\nu^4 + b\nu^2) \equiv z^4(a^4\nu^{16} + b^4\nu^8) \pmod{\mathrm{AS}(k)}, \quad \nu bz^2 \equiv \nu^2b^2z^4 \pmod{\mathrm{AS}(k)},$$

so that (9) is equivalent to

$$\mathrm{Tr}(z^4E_{ab}(\nu)) = 0, \forall z \in W. \tag{10}$$

Hence, $E_{ab}(k) \subseteq (W^4)^\perp$ and, having the same dimension, they coincide. Therefore, condition (ii) is equivalent to $c' \in c + W^\perp$, which is equivalent to (iii) by the definition of L_c.

Finally, it is obvious that (iii) and (iv) are equivalent. ∎

https://doi.org/10.4153/CJM-2007-016-6 Published online by Cambridge University Press

3 Computation of the zeta Function

Let C be a smooth projective curve of genus 2, defined over k. The zeta function of C is a formal series in one indeterminate, which can be expressed as a rational function:

$$\mathrm{Z}(C/\mathbb{F}_q, t) = \exp\Bigl(\sum_{n\geq 1} N_n \frac{t^n}{n}\Bigr) = \frac{1 + a_1 t + a_2 t^2 + q a_1 t^3 + q^2 t^4}{(1-t)(1-qt)}, \tag{11}$$

where $N_n := |C(\mathbb{F}_{q^n})|$ and $a_1, a_2 \in \mathbb{Z}$. From this identity one deduces immediately that

$$N_1 = q + 1 + a_1, \quad N_2 = q^2 + 1 + 2a_2 - a_1^2.$$

Thus, the zeta function is determined by the pair (N_1, N_2).

Let J_C be the jacobian variety of C. The polynomial $t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2$ is the characteristic polynomial of the Frobenius endomorphism of the abelian surface J_C. This polynomial determines the k-isogeny class of J_C. Thus, two curves have the same zeta function if and only if their jacobian varieties are k-isogenous.

Let C be a supersingular curve defined by (1), with parameters $(a, b, c, 0)$. Denote by w, V, W, Q, ℓ, ℓ_c the objects associated to $C_{|k}$ in Sections 1 and 2 and by $\tilde{w}, \tilde{V}, \tilde{W}, \tilde{Q}, \tilde{\ell}, \tilde{\ell}_c$ the corresponding objects associated to the curve $C_{|k_2}$.

In this section we compute $N_2 = |C(\mathbb{F}_{q^2})|$ in terms of a, b, c. The idea is to apply the results of the last section and take advantage of the fact that the curve is defined over k to avoid any computation in k_2. More precisely, we shall see that the linear form ℓ_c on W contains already sufficient information to determine N_2.

To begin with we recall some observations on linear forms over k_2/k. For any $c \in k$, we denote by $\tilde{L}_c$ the linear mapping:

$$\tilde{L}_c \colon k_2 \to \mathbb{F}_2, \quad x \mapsto \tilde{L}_c(x) = \mathrm{Tr}_{k_2}(cx).$$

As before, we can consider the isomorphism,

$$\tilde{L} \colon k \to \mathrm{Hom}(k_2/k, \mathbb{F}_2), \quad c \mapsto \tilde{L}_c.$$

Lemma 3.1 *Think of* $\mathrm{Tr}_{k_2/k}$ *as a linear isomorphism between* k_2/k *and* k *and denote by* $(\mathrm{Tr}_{k_2/k})^*$ *its dual isomorphism. We have a commutative diagram of linear isomorphisms:*

$$\begin{tikzcd} \mathrm{Hom}(k, \mathbb{F}_2) \arrow[rr, "(\mathrm{Tr}_{k_2/k})^*"] & & \mathrm{Hom}(k_2/k, \mathbb{F}_2) \\ & k \arrow[ul, "L"] \arrow[ur, "\tilde{L}"'] & \end{tikzcd}$$

Proof By the transitivity of the trace, for any $x \in k_2$ we have

$$\tilde{L}_c(x) = \mathrm{Tr}_{k_2}(cx) = \mathrm{Tr}_k(\mathrm{Tr}_{k_2/k}(cx)) = \mathrm{Tr}_k(c\,\mathrm{Tr}_{k_2/k}(x)) = L_c(\mathrm{Tr}_{k_2/k}(x)). \qquad \blacksquare$$

The invariant $\tilde{w}$ is completely determined by the factorization of $P(x)$ in $k[x]$, which was obtained in Propositions 2.5 and 2.6. The invariant $\mathrm{codim}(\tilde{V}, \tilde{W})$ can be determined as follows.

https://doi.org/10.4153/CJM-2007-016-6 Published online by Cambridge University Press

Proposition 3.2 *We have $\tilde{V} = \tilde{W}$ if and only if the following two conditions are satisfied:*

(i) $\ell_c(v) = 0$, *for* $v = z + z' \in W$, *with* z, z' *roots of* $P(x)$ *in* $k_2 - k$;
(ii) $\ell_c(z) = 1$, *if* $P(x) = (1)(4)$ *over* $k[x]$ *and* z *is its root in* k.

Proof Assume first that $\tilde{V} = \tilde{W}$. By Proposition 2.8, we have $\tilde{\ell}_c = \tilde{\ell}$. If $v = z + z' \in k$, with z, z' roots of $P(x)$ in $k_2 - k$, we have $\tilde{\ell}(z) = 0$ by definition. Hence, by Lemma 3.1, $\ell_c(v) = \tilde{\ell}_c(z) = \tilde{\ell}(z) = 0$. If $P(x) = (1)(4)$, then it factorizes over k_2 as $P(x) = (x + z)(x^2 + ux + t)(x^2 + u'x + t')$, with $u, u' \in k_2 - k$ galois conjugate and $z + u + u' = 0$. By definition, $\tilde{\ell}(u) = 1$; hence, by Lemma 3.1, $\ell_c(z) = \tilde{\ell}_c(u) = \tilde{\ell}(u) = 1$.

Assume now that conditions (i) and (ii) are satisfied and let us check that $\tilde{\ell}_c = \tilde{\ell}$. For any root z of $P(x)$ in k_2, we have $\tilde{\ell}(z) = 0$. If $z \in k$, we have directly $\tilde{\ell}_c(z) = 0$, whereas for $z \in k_2 - k$ with galois conjugate z' we have $\tilde{\ell}_c(z) = \ell_c(z + z') = 0$ by condition (i). In particular, if $v = z + z'$, with z, z' roots of $P(x)$ in k_2, we have $\tilde{\ell}(v) = 0$ and $\tilde{\ell}_c(v) = 0$, too. Finally, $\tilde{\ell}(v) = 1$ if $v = \omega + \omega'$, with ω, ω' roots of $P(x)$ in $k_4 - k_2$. In this case necessarily $P(x) = (1)(4)$ over $k[x]$, $z := \mathrm{Tr}_{k_2/k}(v)$ is the only root of $P(x)$ in k and $\tilde{\ell}_c(v) = \ell_c(z) = 1$ by condition (ii). ■

We now address the computation of the sign of $\tilde{Q}$ when $\tilde{V} = \tilde{W}$. The crucial observation is that over k_2 we have

$$\langle k + \tilde{W}, k + \tilde{W} \rangle_R = 0, \quad \tilde{Q}(k + \tilde{W}) = 0,$$

since $k \subseteq \mathrm{AS}(k_2)$ and $\tilde{Q}(\tilde{W}) = 0$ by assumption. This will allow us to control the behavior of $\tilde{Q}$ on the classes of elements of k_2 modulo $k + \tilde{W}$.

The simplectic form $\langle\ ,\ \rangle_R$ is non-degenerate over $k_2/\tilde{W}$; hence,

$$\begin{aligned}\dim((k + \tilde{W})/\tilde{W})^{\perp} &= \dim k_2/\tilde{W} - \dim(k + \tilde{W})/\tilde{W}\\ &= (2m - \tilde{w}) - (m - w) = m + w - \tilde{w}.\end{aligned}$$

Let $k + \tilde{W} \subseteq U \subseteq k_2$ be the subspace such that $U/\tilde{W} = ((k + \tilde{W})/\tilde{W})^{\perp}$. We know that $\dim U = m + w$. Clearly, $\langle\ ,\ \rangle_R$ induces a non-degenerate simplectic form:

$$U/(k + \tilde{W}) \times U/(k + \tilde{W}) \to \mathbb{F}_2, \quad (x, y) \mapsto \langle x, y \rangle_R, \tag{12}$$

on the space $U/(k + \tilde{W})$, of dimension $2w - \tilde{w}$. Let $n := w - (\tilde{w}/2)$.

For arbitrary $x \in k_2$, $y \in k + \tilde{W}$ we have

$$\tilde{Q}(x + y) = \tilde{Q}(x) + \tilde{Q}(y) + \langle x, y \rangle_R = \tilde{Q}(x) + \langle x, y \rangle_R. \tag{13}$$

For fixed x, the linear mapping,

$$k + \tilde{W} \to \mathbb{F}_2, \quad y \mapsto \langle x, y \rangle_R$$

vanishes only for $x \in U$. Thus, for $x \in U$, $\tilde{Q}$ is constant in the class $x + (k + \tilde{W})$ and it determines a quadratic form $\tilde{Q}\colon U/(k + \tilde{W}) \to \mathbb{F}_2$ associated to the simplectic form (12). The number of zeros of $\tilde{Q}$ will be $2^{n-1}(2^n \pm 1)$ and altogether there are

$$2^{n-1}(2^n \pm 1)2^{m+\tilde{w}-w} = 2^{m+w-1} \pm 2^{m+(\tilde{w}/2)-1}$$

zeros of $\tilde{Q}$ in U.

Moreover, for $x \notin U$, $\langle x, -\rangle_R$ does not vanish on $k + \tilde{W}$ and, by (13), $\tilde{Q}$ takes the values 0, 1 the same number of times, $2^{m+\tilde{w}-w-1}$, in the class $x + (k + \tilde{W})$. There are $2^{\dim k_2/(k+\tilde{W})} - 2^{\dim U/(k+\tilde{W})} = 2^{m+w-\tilde{w}} - 2^{2w-\tilde{w}}$ such classes and we count

$$(2^{m+w-\tilde{w}} - 2^{2w-\tilde{w}})2^{m+\tilde{w}-w-1} = 2^{2m-1} - 2^{m+w-1}$$

zeros of $\tilde{Q}$ in $k_2 - U$.

Therefore, the number of points of C over k_2 is

$$|C(\mathbb{F}_{q^2})| = 1 + 2\big(2^{2m-1} \pm 2^{m+(\tilde{w}/2)-1}\big) = 1 + q^2 \pm \sqrt{2^{\tilde{w}}q^2}.$$

We have thus proved the following.

Proposition 3.3 *If $\tilde{V} = \tilde{W}$, the sign of $\tilde{Q}$ as a quadratic form over $k_2/\tilde{W}$ coincides with the sign of $\tilde{Q}$ as a quadratic form over $U/(k + \tilde{W})$.*

In order to determine this latter sign, we find an explicit description of U and we express the action of $\tilde{Q}$ on U in terms of the action of Q on W.

Proposition 3.4 *We have $U = \operatorname{Tr}_{k_2/k}^{-1}(W)$. Moreover, for any $u \in U$, with relative trace $z = \operatorname{Tr}_{k_2/k}(u) \in W$, we have*

$$\tilde{Q}(u) = Q(z) \iff P(z) = 0 \text{ or } z = 0.$$

Proof For any $u \in k_2$ with $\operatorname{Tr}_{k_2/k}(u) = z$, we have $u \in U$ if and only if:

$$(14) \qquad 0 = \langle u, \lambda\rangle_R = \operatorname{Tr}_{k_2}(\lambda(au^4 + bu^2) + u(a\lambda^4 + b\lambda^2)), \quad \forall\lambda \in k.$$

By the same argument used to show that (9) was equivalent to (10), we see that (14) is equivalent to

$$\operatorname{Tr}_{k_2}(\lambda^4 E_{ab}(u)) = 0,\ \forall\lambda \in k \iff \operatorname{Tr}_k(\lambda^4 E_{ab}(z)) = 0,\ \forall\lambda \in k \iff$$
$$\iff \operatorname{Tr}_k(\lambda E_{ab}(z)) = 0,\ \forall\lambda \in k \iff E_{ab}(z) = 0,$$

the last equivalence by the non-degeneracy of the pairing $\operatorname{Tr}(xy)$. This proves the first assertion.

Now, let $u \in U$. The galois conjugate of u is $u^\sigma = u + z$. Hence,

$$\begin{aligned}\mathrm{Tr}_{k_2/k}(au^5 + bu^3 + cu) &= au^5 + bu^3 + cu + a(u+z)^5 + b(u+z^3) + c(u+z)\\ &= au^4z + auz^4 + az^5 + bu^2z + buz^2 + bz^3 + cz\\ &= az^5 + bz^3 + cz + uR(z) + zR(u),\end{aligned}$$

so that,

$$\begin{aligned}\tilde{Q}(u) = \mathrm{Tr}_{k_2}(au^5 + bu^3 + cu) &= \mathrm{Tr}_k(az^5 + bz^3 + cz + uR(z) + zR(u))\\ &= Q(z) + \mathrm{Tr}_k(uR(z) + zR(u)).\end{aligned}$$

We have to check when $uR(z) + zR(u) \in \mathrm{AS}(k)$. Let us express $u = zv$, with $v \in k_2$ an element of relative trace 1: $v^2 + v = r$, $r \in k - \mathrm{AS}(k)$. Note that $v^4 = v^2 + r^2 = v + r + r^2$. We have

$$\begin{aligned}uR(z) + zR(u) &= zv(az^4 + bz^2) + z(az^4v^4 + bz^2v^2)\\ &= v(az^5 + bz^3) + v^4az^5 + v^2bz^3 = (r + r^2)az^5 + rbz^3\\ &\equiv (r + r^2)az^5 + r^2b^2z^6 = raz^5 + r^2(a^2z^{10} + z^5P(z))\\ &\equiv r^2z^5P(z) \pmod{\mathrm{AS}(k)}.\end{aligned}$$

Hence, if $z^5P(z) = 0$, we have $uR(z) + zR(u) \in \mathrm{AS}(k)$ and if $z^5P(z) = 1$, we have $uR(z) + zR(u) \equiv r^2 \not\equiv 0 \pmod{\mathrm{AS}(k)}$, since $r \notin \mathrm{AS}(k)$. ∎

Theorem 3.5 *The possible signs of $\tilde{Q}$ are given in the following table:*

w	$\tilde{w}$	$P(x)$	$\dim U/(k+\tilde{W})$	$\mathrm{sgn}(\tilde{Q})$
0	0	*irreducible*	0	$+$
1	2	(1)(4) *or* (2)(3)	0	$0/+$
2	2	(1)(1)(3)	2	$+/-$
2	4	(1)(2)(2)	0	$0/+$
3	4	(1)(1)(1)(2)	2	$0/+/-$
4	4	(1)(1)(1)(1)(1)	4	$+/-$

Moreover, let $Z \subseteq W$ be the subset of all roots of $P(x)$ in k. For $P(x) = (1)(1)(3)$ or $(1)(1)(1)(2)$, we have

$$\mathrm{sgn}(\tilde{Q}) = \text{“}-\text{”} \iff \ell_c(z) \neq \mathrm{Tr}(1),\ \forall z \in Z,$$

whereas for $P(x) = (1)(1)(1)(1)(1)$, we have

$$\mathrm{sgn}(\tilde{Q}) = \text{“}+\text{”} \iff \ell_c(z) = 0,\ \text{for exactly 3 of the 5 roots } z \in Z.$$

https://doi.org/10.4153/CJM-2007-016-6 Published online by Cambridge University Press

Proof The content of the table is an immediate consequence of Propositions 2.3, 3.2 and 3.3. The other assertions on sgn $\tilde{Q}$ are a consequence of Propositions 3.3 and 3.4. For instance, in the cases when $\dim U/(k+\tilde{W}) = 2$, the quadratic form $\tilde{Q}$ has either one or three zeros on this space; the minus sign corresponds to the case $\tilde{Q}(u) = 1$ for all $u \in U/(k+\tilde{W})$, $u \neq 0$, and by Proposition 3.4, this is equivalent to $Q(z) = 1$ for all $z \in Z$, which is equivalent to $\ell_c(z) = \operatorname{Tr}(1) + 1$ for all $z \in Z$ by Proposition 2.8.

We leave the case $w = \tilde{w} = 4$ to the reader. ■

We have obtained an explicit computation of the zeta function of any supersingular curve, except for the sign of Q when $V = W$. From the computational point of view, once you know $\pm a_1$ and a_2, the sign of a_1 is easy to determine by computing iterates of a random divisor in the jacobian. We can consider a deterministic algorithm too by evaluating Q on a simplectic basis of k/W with respect to $\langle\, ,\rangle_R$.

4 Zeta functions of supersingular curves of genus 2

In this section we compute all possible zeta functions arising from supersingular curves of genus 2 and we find formulas for the number of k-isomorphism classes of curves that have the same zeta function. We proceed in a constructive way, by applying the results of the previous sections to all supersingular curves. Hence, our results can be used to exhibit curves with prescribed zeta function.

For any pair of integers (a_1, a_2) we shall denote by $\mathcal{C}_{(a_1,a_2)}$ the set of k-isomorphism classes of smooth projective curves of genus 2 defined over k, whose zeta function is given by (11), or equivalently, whose number of points N_1, N_2 over k and k_2 satisfy

$$N_1 = q + 1 + a_1, \quad N_2 = q^2 + 1 + 2a_2 - a_1^2.$$

The hyperelliptic twist sets a bijection between $\mathcal{C}_{(a_1,a_2)}$ and $\mathcal{C}_{(-a_1,a_2)}$, which is the identity if $a_1 = 0$ by the remark at the end of Section 1.

We work with supersingular curves given by equation (1), depending on four parameters (a, b, c, d) with $b = 0$ or $b = a$. We keep the notations $w, W, V, Q, \ell, \tilde{w}, \tilde{W}, \tilde{V}, \tilde{Q}$ introduced in the last section. We remind the reader that

$$\ell_c = L_{c\,|W}, \text{ if } b = 0, \quad \ell_c = L_{c+a\,|W}, \text{ if } b = a.$$

We deal first with the case m odd.

4.1 $P_{ab}(x) = (1)(4)$

By Proposition 2.3 we have $w = 1$, $\tilde{w} = 2$ in this case. If $z \in k$ is the only root of $P_{ab}(x)$ in k, we have $W = \{0, z\}$.

Let us study first the case $b = 0$. Since $(k^*)^5 = k^*$, we can assume $a = 1$ by (4), so that $z = 1$. By Proposition 2.5, $P_{10}(x) = (1)(4)$. By Propositions 2.8, 3.2 and Theorem 3.5, for any $c \in k$ we have

$$\text{(15)} \qquad \begin{aligned} \ell_c(z) = 0 &\implies \operatorname{sgn}(Q) = \operatorname{sgn}(\tilde{Q}) = 0, \\ \ell_c(z) \neq 0 &\implies \operatorname{sgn}(Q) = \pm, \operatorname{sgn}(\tilde{Q}) = +. \end{aligned}$$

By Lemma 2.9, the different values of (c, d) lead to three k-isomorphism classes represented by $(1, 0, 0, 0)$ and a couple of twisted curves, $(1, 0, 1, 0)$, $(1, 0, 1, 1)$. The first one has $(N_1, N_2) = (q + 1, q^2 + 1)$ and the other two $(N_1, N_2) = (q + 1 \pm \sqrt{2q}, q^2 + 1 + 2q)$. Thus, we get one curve in each of the sets $\mathcal{C}_{(0,0)}$, $\mathcal{C}_{(\sqrt{2q},2q)}$, $\mathcal{C}_{(-\sqrt{2q},2q)}$.

Let us study now the case $a = b \neq 0$. By Corollary 2.7, there are $(q/2)-1$ values of a leading to $P_{aa}(x) = (1)(4)$ and by (4) they correspond to different k-isomorphism classes. Let us fix one of these values of a. As before, (15) holds and the different values of (c, d) provide three k-isomorphism classes, represented by $(a, a, 0, 0)$, $(a, a, c, 0)$, $(a, a, c, 1)$, where $\ell_c(z) \neq 0$, and they are distributed into the same three zeta functions.

We have altogether a contribution of $q/2$ k-isomorphism classes in each of the sets $\mathcal{C}_{(0,0)}$, $\mathcal{C}_{(\sqrt{2q},2q)}$, $\mathcal{C}_{(-\sqrt{2q},2q)}$.

4.2 $P_{ab}(x) = (2)(3)$

By Proposition 2.3 we have $w = 1$, $\tilde{w} = 2$ in this case. If $x^2 + vx + t$ is the quadratic irreducible factor of $P_{ab}(x)$ we have $W = \{0, v\}$.

By Proposition 2.5, we have necessarily $b \neq 0$ and we can assume $a = b$. By Corollary 2.7, we have $(q+1)/3$ values of a leading to this factorization of $P_{aa}(x)$. We fix one of these values of a. By Propositions 2.8, 3.2 and Theorem 3.5, for any $c \in k$ we have

$$\ell_c(v) = 0 \implies \operatorname{sgn}(Q) = 0,\ \operatorname{sgn}(\tilde{Q}) = +,$$
$$\ell_c(v) \neq 0 \implies \operatorname{sgn}(Q) = \pm, \operatorname{sgn}(\tilde{Q}) = 0$$

By Lemma 2.9, the different values of (c, d) lead to three k-isomorphism classes represented by $(a, a, a, 0)$, $(a, a, c, 0)$, $(a, a, c, 1)$, where $\ell_c(v) \neq 0$. The first one has $(N_1, N_2) = (q + 1, q^2 + 1 + 2q)$ and the other two $(N_1, N_2) = (q + 1 \pm \sqrt{2q}, q^2 + 1)$. Thus, we get $(q + 1)/3$ curves in each of the sets $\mathcal{C}_{(0,q)}$, $\mathcal{C}_{(\sqrt{2q},q)}$, $\mathcal{C}_{(-\sqrt{2q},q)}$.

4.3 $P_{ab}(x) = (1)(1)(1)(2)$

By Proposition 2.3 we have $w = 3$, $\tilde{w} = 4$ in this case. We have $W = \langle z_1, z_2, z_3\rangle$, where z_1, z_2, z_3 are the roots of $P_{ab}(x)$ in k. The quadratic irreducible factor of $P_{ab}(x)$ is $x^2 + vx + t$, with $v = z_1 + z_2 + z_3$.

By Proposition 2.5, we have necessarily $b \neq 0$ and we assume $a = b$. By Corollary 2.7 we have $(q - 2)/6$ values of a leading to this factorization of $P_{aa}(x)$. For any such fixed value of a, the linear form $\ell\colon W \to \mathbb{F}_2$ introduced in Proposition 2.8 is determined by $\ell(z_1) = \ell(z_2) = \ell(z_3) = 1$.

For any $c \in k$, let N be the number of z_i such that $\ell_c(z_i) = 0$. Note that $N = 0$ if and only if $\ell_c = \ell$ and N is even if and only if $\ell_c(v) = 1$. By Propositions 2.8, 3.2 and

Theorem 3.5, we have

$$N = 0 \implies \operatorname{sgn}(Q) = \pm, \operatorname{sgn}(\tilde{Q}) = 0,$$

$$N = 1 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = +,$$

$$N = 2 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = 0,$$

$$N = 3 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = -.$$

There are eight possibilities for ℓ_c, one with $N = 0$ or $N = 3$ and three with $N = 1$ or $N = 2$. By Lemma 2.9, the different values of (c, d) lead to 2, 3, 3, 1 k-isomorphism classes corresponding respectively to $N = 0, 1, 2, 3$. The number of points of these curves is respectively $(N_1, N_2) = (q + 1 \pm 2\sqrt{2q}, q^2 + 1), (q+1, q^2+1+4q)$, $(q + 1, q^2 + 1), (q + 1, q^2 + 1 - 4q)$. Thus, we get a contribution of respectively $(q - 2)/6$, $(q - 2)/6$, $(q - 2)/2$, $(q - 2)/2$, $(q - 2)/6$ curves in each of the sets $\mathcal{C}_{(2\sqrt{2q},4q)}$, $\mathcal{C}_{(-2\sqrt{2q},4q)}$, $\mathcal{C}_{(0,2q)}$, $\mathcal{C}_{(0,0)}$, $\mathcal{C}_{(0,-2q)}$.

From now on we deal with the case m even.

4.4 $P_{ab}(x)$ Irreducible

By Proposition 2.3, we have $w = \tilde{w} = 0$ and $W = \tilde{W} = \{0\}$. We have thus $\operatorname{sgn}(Q) = \pm$, and $\operatorname{sgn}(\tilde{Q}) = +$, by Theorem 3.5. On the other hand, since $E_{ab} \colon k \to k$ has a trivial kernel, we have $E_{ab}(k) = k$ and we can always assume that $c = 0$ by (4).

Let us study first the case $b = 0$. By Proposition 2.5, $P_{a0}(x)$ is irreducible if and only if $m \equiv 0 \pmod 4$ and $a \notin (k^*)^5$. In this case, we have eight k-isomorphism classes represented by $(a, 0, 0, 0)$, $(a, 0, 0, d_0)$, where a runs on the four non-trivial classes of $k^*/(k^*)^5$. They have $(N_1, N_2) = (q+1 \pm \sqrt{q}, q^2+1+q)$ and they contribute with four curves in each of the sets $\mathcal{C}_{(-\sqrt{q},q)}$, $\mathcal{C}_{(\sqrt{q},q)}$.

In the case $a = b \neq 0$ there are $\frac{2}{5}(q + 1 - [2]_{4|m})$ values of a leading to $P_{aa}(x)$ irreducible, by Corollary 2.7. As before, for each fixed value of a we obtain one curve in each of the sets $\mathcal{C}_{(-\sqrt{q},q)}$, $\mathcal{C}_{(\sqrt{q},q)}$.

We have altogether a contribution of $\frac{2}{5}(q + 1 + [8]_{4|m})$ k-isomorphism classes in each of the sets $\mathcal{C}_{(-\sqrt{q},q)}$, $\mathcal{C}_{(\sqrt{q},q)}$.

4.5 $P_{ab}(x) = (1)(1)(3)$

By Proposition 2.3, we have $w = \tilde{w} = 2$ and $W = \langle z_1, z_2 \rangle$, where z_1, z_2 are the roots of $P_{ab}(x)$ in k. By Proposition 2.5, we have necessarily $b \neq 0$ and we assume $a = b$. By Corollary 2.7, we have $(q - 1)/3$ values of a leading to this factorization of $P_{aa}(x)$. For any such fixed value of a, the linear form ℓ on W vanishes.

For any $c \in k$, let N be the number of z_i such that $\ell_c(z_i) = 0$. Note that $N = 2$ if and only if $\ell_c = \ell$. By Propositions 2.8, 3.2 and Theorem 3.5, we have

$$N = 0 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = -,$$

$$N = 1 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = +,$$

$$N = 2 \implies \operatorname{sgn}(Q) = \pm, \operatorname{sgn}(\tilde{Q}) = +.$$

There are four possibilities for ℓ_c, one with $N = 0$ or $N = 2$ and two with $N = 1$. By Lemma 2.9, the different values of (c, d) lead to 1, 2, 2 k-isomorphism classes corresponding respectively to $N = 0, 1, 2$. The number of points of these curves is respectively $(N_1, N_2) = (q+1, q^2+1-2q), (q+1, q^2+1+2q), (q+1\pm 2\sqrt{q}, q^2+1+2q)$. Thus, we get a contribution of respectively $(q-1)/3, 2(q-1)/3, (q-1)/3, (q-1)/3$ curves in each of the sets $\mathcal{C}_{(0,-q)}, \mathcal{C}_{(0,q)}, \mathcal{C}_{(-2\sqrt{q},3q)}, \mathcal{C}_{(2\sqrt{q},3q)}$.

4.6 $P_{ab}(x) = (1)(2)(2)$

By Proposition 2.3, we have $w = 2$, $\tilde{w} = 4$ in this case. If $P_{ab}(x) = (x+z)(x^2+v_1x+t_1)(x^2+v_2x+t_2)$, we have $v_1 + v_2 = z$ and $W = \{0, z, v_1, v_2\}$.

Let us study first the case $b = 0$. By Proposition 2.5, $P_{a0}(x) = (1)(2)(2)$ if and only if $4 \nmid m$. In this case, $(k^*)^5 = k^*$ and we can assume $a = 1$ by (4). The linear form ℓ on W is determined by $\ell(v_1) = \ell(v_2) = 1$.

For any $c \in k$, let N be the number of v_i such that $\ell_c(v_i) = 0$. Note that $N = 0$ if and only if $\ell_c = \ell$. By Propositions 2.8, 3.2 and Theorem 3.5, we have

$$N = 0 \implies \operatorname{sgn}(Q) = \pm, \operatorname{sgn}(\tilde{Q}) = 0,$$

$$N = 1 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = 0,$$

$$N = 2 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = +.$$

There are four possibilities for ℓ_c, one with $N = 0$ or $N = 2$ and two with $N = 1$. By Lemma 2.9, the different values of (c, d) lead to $2, 2, 1$ k-isomorphism classes according to $N = 0, 1, 2$. The number of points of these curves is respectively $(N_1, N_2) = (q + 1 \pm 2\sqrt{q}, q^2 + 1), (q + 1, q^2 + 1), (q + 1, q^2 + 1 + 4q)$. Thus, we get respectively $1, 1, 2, 1$ curves in each of the sets $\mathcal{C}_{(-2\sqrt{q},2q)}, \mathcal{C}_{(2\sqrt{q},2q)}, \mathcal{C}_{(0,0)}, \mathcal{C}_{(0,2q)}$.

In the case $a = b \neq 0$, there are $(q/4) - [1]_{4\nmid m}$ values of a leading to $P_{aa}(x) = (1)(2)(2)$, by Corollary 2.7. As before, for any such fixed value of a we get respectively $1, 1, 2, 1$ curves with the same zeta functions as above.

We have altogether a contribution of $q/4$, $q/4$, $q/2$, $q/4$ k-isomorphism classes in each of the sets $\mathcal{C}_{(-2\sqrt{q},2q)}, \mathcal{C}_{(2\sqrt{q},2q)}, \mathcal{C}_{(0,0)}, \mathcal{C}_{(0,2q)}$.

4.7 $P_{ab}(x) = (1)(1)(1)(1)(1)$

By Proposition 2.3 we have $w = \tilde{w} = 4$ in this case and $W = \langle z_1, z_2, z_3, z_4 \rangle$, where $z_1, z_2, z_3, z_4, z_1 + z_2 + z_3 + z_4$ are the roots of $P_{ab}(x)$ in k.

Let us study first the case $b = 0$. By Proposition 2.5, $P_{a0}(x)$ splits completely in $k[x]$ if and only if $4 \mid m$ and $a \in (k^*)^5$. In this case we can assume $a = 1$ by (4), so that $W = \mathbb{F}_{16}$. The linear form ℓ vanishes.

For any $c \in k$, let N be the number of z_i such that $\ell_c(z_i) = 0$. Note that $N = 5$ if and only if $\ell_c = \ell$. By Propositions 2.8, 3.2 and Theorem 3.5, we have

$$N = 1 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = -, \tag{16}$$

$$N = 3 \implies \operatorname{sgn}(Q) = 0, \operatorname{sgn}(\tilde{Q}) = +,$$

$$N = 5 \implies \operatorname{sgn}(Q) = \pm, \operatorname{sgn}(\tilde{Q}) = -.$$

https://doi.org/10.4153/CJM-2007-016-6 Published online by Cambridge University Press

We cannot now apply Lemma 2.9, but it is easy to check that the different values of (c, d) lead to $1, 2, 2$ k-isomorphism classes according to $N = 1, 3, 5$. The number of points of these curves is respectively $(N_1, N_2) = (q+1, q^2+1-4q)$, $(q+1, q^2+1+4q)$, $(q+1 \pm 4\sqrt{q}, q^2+1-4q)$. Thus, we get respectively $1, 2, 1, 1$ curves in each of the sets $\mathcal{C}_{(0,-2q)}$, $\mathcal{C}_{(0,2q)}$, $\mathcal{C}_{(-4\sqrt{q},6q)}$, $\mathcal{C}_{(4\sqrt{q},6q)}$.

In the case $a = b \neq 0$ there are $\frac{q-4}{60} - [\frac{1}{5}]_{4|m}$ values of a leading to $P_{aa}(x) = (1)(1)(1)(1)(1)$, by Corollary 2.7. For any such fixed value of a, (16) holds. There are 16 possibilities for ℓ_c, five with $N = 1$, ten with $N = 3$ and one with $N = 5$. By Lemma 2.9, we get respectively $5, 10, 1, 1$ curves with the same zeta functions as above.

We have altogether a contribution of $\frac{q-4}{12}$, $\frac{q-4}{6}$, $\frac{q-4}{60} + [\frac{4}{5}]_{4|m}$, $\frac{q-4}{60} + [\frac{4}{5}]_{4|m}$ k-isomorphism classes in each of the sets $\mathcal{C}_{(0,-2q)}$, $\mathcal{C}_{(0,2q)}$, $\mathcal{C}_{(-4\sqrt{q},6q)}$, $\mathcal{C}_{(4\sqrt{q},6q)}$.

5 Jacobians in Isogeny Classes of Supersingular Abelian Surfaces

Let A be a supersingular abelian surface defined over k. Let $f_A(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2$ be the characteristic polynomial of its Frobenius endomorphism. The k-isogeny class of A is determined by this polynomial, that is, by the pair of integers (a_1, a_2).

It is easy to list all pairs (a_1, a_2) that correspond to supersingular abelian surfaces. The k-simple supersingular isogeny classes can be found in [MN, Table 1]. If A is k-isogenous to a product of two supersingular elliptic curves, we have $f_A(t) = f_{E_1}(t) f_{E_2}(t)$, with $f_{E_i}(t) = t^2 + b_it + q$. This gives,

$$a_1 = b_1 + b_2, \quad a_2 = 2q + b_1b_2.$$

On the other hand, the possibilities for the integers b_i were determined by Waterhouse in his thesis [Wat, Theorem 4.1]:

$$b_i \in \{0, \pm\sqrt{2q}\}, \text{ if } m \text{ is odd}; \quad b_i \in \{0, \pm\sqrt{q}, \pm 2\sqrt{q}\}, \text{ if } m \text{ is even}.$$

This gives respectively $6, 15$ k-split supersingular isogeny classes according to m being odd or even.

Gathering the computations of the previous section, we give in the tables below the number of k-isomorphism classes of supersingular curves of genus 2 whose jacobian lies in each k-isogeny class. When in a column indexed as $(\pm a_1, a_2)$ we say that $|\mathcal{C}_{(a_1,a_2)}| = N$, we mean that $|\mathcal{C}_{(a_1,a_2)}| = |\mathcal{C}_{(-a_1,a_2)}| = N$.

We see that some isogeny classes contain no jacobians. In most of the cases there is a trivial explanation for this fact, but the assertion that

$$\mathcal{C}_{(0,-q)} = \varnothing, \quad \text{when } m \text{ is odd}, \tag{17}$$

is far from trivial and the achievement of this result was the initial motivation for the paper.

Table 1: Split isogeny classes, m odd

(a_1, a_2)	$(0,0)$	$(0,2q)$	$(\pm\sqrt{2q}, 2q)$	$(\pm 2\sqrt{2q}, 4q)$
$\lvert\mathcal{C}_{(a_1,a_2)}\rvert$	$q-1$	$(q-2)/2$	$q/2$	$(q-2)/6$
$b_1,\ b_2$	$\sqrt{2q},\ -\sqrt{2q}$	$0,\ 0$	$0,\ \pm\sqrt{2q}$	$b_1 = b_2 = \pm\sqrt{2q}$

Table 2: Simple isogeny classes, m odd

(a_1, a_2)	$(0,-2q)$	$(0,-q)$	$(0,q)$	$(\pm\sqrt{2q}, q)$
$\lvert\mathcal{C}_{(a_1,a_2)}\rvert$	$(q-2)/6$	0	$(q+1)/3$	$(q+1)/3$

Table 3: Split isogeny classes, m even

(a_1, a_2)	$(0,-2q)$	$(\pm\sqrt{q}, 0)$	$(0,q)$	$(0,2q)$	$(\pm\sqrt{q}, 2q)$
$\lvert\mathcal{C}_{(a_1,a_2)}\rvert$	$(q-4)/12$	0	$2(q-1)/3$	$(5q-8)/12$	0
$b_1,\ b_2$	$2\sqrt{q},\ -2\sqrt{q}$	$\pm(\sqrt{q},\ -2\sqrt{q})$	$\sqrt{q},\ -\sqrt{q}$	$0,\ 0$	$0,\ \pm\sqrt{q}$

(a_1, a_2)	$(\pm 2\sqrt{q}, 2q)$	$(\pm 2\sqrt{q}, 3q)$	$(\pm 3\sqrt{q}, 4q)$	$(\pm 4\sqrt{q}, 6q)$
$\lvert\mathcal{C}_{(a_1,a_2)}\rvert$	$q/4$	$(q-1)/3$	0	$\frac{q-4}{60} + [\frac{4}{5}]_{4\mid m}$
$b_1,\ b_2$	$0, \pm 2\sqrt{q}$	$b_1 = b_2 = \pm\sqrt{q}$	$\pm(\sqrt{q},\ 2\sqrt{q})$	$b_1 = b_2 = \pm 2\sqrt{q}$

Table 4: Simple isogeny classes, m even

(a_1, a_2)	$(0,-q)$	$(0,0)$	$(\pm\sqrt{q}, q)$
$\lvert\mathcal{C}_{(a_1,a_2)}\rvert$	$(q-1)/3$	$q/2$	$\frac{2}{5}(q+1+[8]_{4\mid m})$

References

[CNP] G. Cardona, E. Nart, and J. Pujolàs, *Curves of genus two over fields of even characteristic.* Math. Z. **250**(2005), no. 1, 177–201.

[MN] D. Maisner and E. Nart, *Abelian surfaces over finite fields as Jacobians. With an appendix by Everett W. Howe.* Experimental Math. **11**(2003), no. 3, 321–337.

[VV1] G. van der Geer and M. van der Vlugt, *Reed-Muller codes and supersingular curves. I.* Compositio Math. **84**(1992), no. 3, 333–367.

[VV2] ———, *Supersingular curves of genus* 2 *over finite fields of characteristic* 2. Math. Nachr. **159**(1992), 73–81.
[Wat] W. C. Waterhouse, *Abelian varieties over finite fields.* Ann. Sci. École Norm. Sup. (4) **2**(1969), 521–560.

Departament de Matemàtiques
Universitat Autònoma de Barcelona
Edifici C
08193 Bellaterra
Barcelona
Spain
e-mail: danielm@mat.uab.es
nart@mat.uab.es

https://doi.org/10.4153/CJM-2007-016-6 Published online by Cambridge University Press