Compositio Mathematica **134:** 87–111, 2002.

The Maximum or Minimum Number of Rational Points on Genus Three Curves over Finite Fields

KRISTIN LAUTER with an Appendix by JEAN-PIERRE SERRE
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, U.S.A.
e-mail:klauter@microsoft.com

(Received: 25 July 2001; accepted: 17 August 2001)

Abstract. We show that for all finite fields $\mathbb{F}_q$, there exists a curve C over $\mathbb{F}_q$ of genus 3 such that the number of rational points on C is within 3 of the Serre–Weil upper or lower bound. For some q, we also obtain improvements on the upper bound for the number of rational points on a genus 3 curve over $\mathbb{F}_q$.

Mathematics Subject Classifications (2000). 11G20, 14G05, 14G10, 14G15.

Key words. curve, rational points, zeta function, Serre bound.

1. Introduction

More than half a century ago, André Weil proved a formula for the number of rational points, $N(C)$, on a smooth projective algebraic curve C of genus g over a finite field $\mathbb{F}_q$. This formula, along with his proof of what is referred to as the Riemann hypothesis for curves, provides upper (resp. lower) bounds on the maximum (resp. minimum) number of rational points possible

$$q + 1 - 2g\sqrt{q} \leqslant N \leqslant q + 1 + 2g\sqrt{q}.$$

There are many cases in which the Weil upper and lower bounds cannot be attained. Some are trivial: for example, when the bound is not an integer. Also, when the field size, q, is small with respect to the genus, g, the lower bound will be negative and thus cannot be attained. In [21], Serre made a nontrivial improvement to the Weil bound (which we will refer to hereafter as the Serre–Weil bound):

$$q + 1 - gm \leqslant N \leqslant q + 1 + gm, \quad m = [2\sqrt{q}],$$

and introduced the explicit formulae method to provide better bounds for large genus. Since then there has been considerable interest in determining the actual maximum and minimum. (cf. [2, 3, 9–13, 15, 16, 20–24, 27, 28])

In the present paper we are concerned with the following question which was posed in [22]: for which genus, g, is the difference between the upper bound and the actual maximum $N_q(g)$ bounded as q varies? For genus 1 and any q, the difference is either or 0 or 1 ([29]). For genus 2, Serre determined $N_q(2)$ for all q, and

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

showed that the difference from the Serre–Weil bound is always less than or equal to 3 ([21]); for genus 3, he determined the maximum for $q \leqslant 25$ ([23]). The present paper is devoted to showing that for genus 3 and all q, either the maximum or the minimum is within 3 of the Serre–Weil upper or lower bound.

The techniques involved in the proof of the main theorem include Serre's theory of Hermitian modules as well as 'glueing' of polarizations on Abelian varieties. The theory of Hermitian modules is detailed in the Appendix. This theory provides an equivalence of categories between Abelian varieties over $\mathbb{F}_q$ which are isogenous to a product of copies of an ordinary elliptic curve, and torsion-free modules of finite type over a ring which is defined in terms of the Frobenius of the elliptic curve. A polarization on the Abelian variety then translates to a Hermitian form on the module. Thus the classification of Hermitian forms over rings can be used to determine the existence or nonexistence of the corresponding polarized Abelian variety.

To determine whether there is a curve whose number of points is close to the Weil bound, we first make a list of the possible zeta functions for such a curve as in [13]. The numerator of the zeta function of a curve is given by the characteristic polynomial of Frobenius acting on the Jacobian of the curve. From Tate's theorem we know that the isogeny type of an Abelian variety over a finite field is determined by the characteristic polynomial of Frobenius. For each zeta function, we investigate the corresponding isogeny type using the equivalence of categories provided by Serre's theory. Since not all Jacobians of curves we consider are isogenous to the product of one elliptic curve with itself, we are naturally led to consider the glueing of polarizations on Abelian varieties of different isogeny types. In some cases, the glueing is possible; in others, it is not. When it is not, we obtain improvements on the upper bounds. In all cases we are able to conclude by making use of the Torelli theorem in dimension 3 that there exists a curve whose number of points is within 3 of the Serre–Weil upper or lower bound.

Serre invoked the theory of Hermitian modules to treat the genus 2 case in [22] and [23], but did not give details. In [24], the full proof of the genus 2 case is given, including more explanation of the equivalence of categories. More recent work on this subject was done by Everett Howe ([6]), who translated the notion of principal polarization working with Deligne's more general equivalence of categories. The notion of the glueing of polarizations on Abelian varieties has also been employed by several authors recently for various purposes ([4, 7]).

The proof of the main theorem of this paper is divided into cases which correspond naturally to the existence or nonexistence of indecomposable Hermitian forms over certain rings of a given discriminant. In each case we treat finite fields $\mathbb{F}_q$ with q of a special form, which leads to a number of interesting diophantine problems.

The paper is organized as follows: Section 2 contains the statement of the main theorems of the paper. Section 3 contains a description of how the theory of Hermitian modules will be used in the proofs of the main theorems and also recalls the short list of possible zeta function for curves with the number of points under consideration. Section 4 contains the proofs of the main theorems.

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

2. Statement of Results

Let $q = p^e$, with p prime, $e \geqslant 1$. By a *curve* over the finite field $\mathbb{F}_q$, we mean a smooth, projective, absolutely irreducible curve. For such a curve, C, let $g = g(C)$ denote the genus, and $N = N(C)$ denote the number of rational points over $\mathbb{F}_q$.

DEFINITION. For fixed g and q, let $N_q(g)$ (resp. $M_q(g)$) denote the maximum (resp. minimum) of $N(C)$ as C runs through all curves of genus g over $\mathbb{F}_q$.

Throughout we write $q = p^e$ uniquely in the form $q = x^2 + x + a$, where x is the largest integer whose square is less than or equal to q, and a is an integer such that $-x \leqslant a \leqslant x$.

Let $m = [2\sqrt{q}]$, and $d = m^2 - 4q$. Note that

$$m = \begin{cases} 2x & \text{if} \quad -x \leqslant a \leqslant 0, \\ 2x + 1 & \text{if} \quad 0 < a \leqslant x \end{cases}$$

and

$$d = \begin{cases} -4(x + a) & \text{if} \quad -x \leqslant a \leqslant 0, \\ 1 - 4a & \text{if} \quad 0 < a \leqslant x. \end{cases}$$

THEOREM 1. *Suppose $q = x^2 + x + a$, $a = 1$ or $a = 3$, with $a \leqslant x$. Then*

$$N_q(3) \leqslant q + 1 + 3m - 3 \quad \text{and} \quad M_q(3) \geqslant q + 1 - 3m + 3.$$

Furthermore, there exists a curve C of genus $g(C) = 3$ over $\mathbb{F}_q$ such that

$$|N(C) - (q + 1)| = 3m - 3.$$

Note 2.1. For example, if we write $q = 5$ in the form $q = x^2 + x + 3$, with $x = 1$ and $a = 3$, then x is not the greatest integer part of the square root of q and a does not satisfy the inequality $a \leqslant x$; so instead we write q in the form $q = x^2 + 1$, $a = -1$. Nor do we write $q = 9$ in the form $q = x^2 + x + 3$, since it would not satisfy $a \leqslant x$.

THEOREM 2. *Suppose $q = x^2 + b$, $b = 1$ or $b = 2$, with $a = b - x$ satisfying $-x \leqslant a \leqslant 0$. Then $N_q(3) \leqslant q + 1 + 3m - 2$. Furthermore, there exists a genus 3 curve C over $\mathbb{F}_q$ such that $|N(C) - (q + 1)| = 3m - 2$.*

Note 2.2. For example, $q = 3$ is *not* of the form $q = x^2 + 2$ with $2 \leqslant x$; instead it is of the form $q = x^2 + x + 1$.

Together, Theorems 1 and 2 can be used to establish the following result:

THEOREM 3. *For any prime power $q = p^e$, there exists a curve C of genus $g(C) = 3$ over $\mathbb{F}_q$ such that $|N(C) - (q + 1)| \geqslant 3m - 3$.*

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

In other words, Theorem 3 says that for all q, at least one of the following holds:

(i) $|q+1+3m-N_q(3)| \leqslant 3$,

(ii) $|q+1-3m-M_q(3)| \leqslant 3$.

3. Background

3.1. HERMITIAN MODULES

In the Appendix, Serre gives an equivalence between the following two categories: the category of Abelian varieties over $\mathbb{F}_q$ which are isogenous over $\mathbb{F}_q$ to a product of copies of E, where E is an ordinary elliptic curve over $\mathbb{F}_q$; and the category of torsion-free R_d-modules of finite type, where $R_d = \mathbb{Z}[\pi]$, π is the Frobenius of E, and $d = a^2 - 4q$, where $\#E(\mathbb{F}_q) = q+1-a$. The equivalence holds under the assumption that d is the discriminant of an imaginary quadratic field. In that case, R_d is equal to the ring of integers in the field; thus it is a Dedekind domain, and the modules under consideration are projective. If d is not the discriminant of an imaginary quadratic field, then R_d is an order in the ring of integers. Although the equivalence of categories does not necessarily hold under those conditions, we will still use the same notation and make use of the functor S given in the Appendix. In most cases there will be no conflict with the notation from Section 2 since we will let $a = m$; in all other cases, we will use the notation d'. The condition that E be ordinary is equivalent to requiring that a be prime to q. Throughout the paper we will use the notation E_m to denote an elliptic curve with $q+1+m$ points over the field $\mathbb{F}_q$.

In Section 5 of the Appendix, polarizations on Abelian varieties are translated into positive definite Hermitian forms on R-modules, and the polarization is principal if and only if the Hermitian form has discriminant 1. The Jacobian of a curve has a canonical principal polarization which corresponds to the theta divisor. For an absolutely irreducible curve, the theta divisor is irreducible, so the canonical polarization corresponds to an indecomposable Hermitian module with discriminant 1.

We will use this correspondence in two directions. In cases where we can show that there is no indecomposable Hermitian module of discriminant 1, we can conclude that no curve of that type exists. In cases where we find an indecomposable Hermitian module of discriminant 1, we can use the theorem of Torelli in its precise form (see the Appendix to [13]) to conclude that a curve of that type (or of the opposite type) exists.

3.2. ZETA FUNCTIONS

In each case, we identify the zeta function of the curve we are searching for. The zeta function determines the isogeny type of the Jacobian of the curve.

DEFINITION 1. A curve has zeta function of type $[x_1, \dots x_g]$ if

$$x_i = -(\alpha_i + \bar{\alpha}_i), \quad i = 1, \dots, g,$$

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

where $\{\alpha_i, \bar{\alpha}_i\}$ is the family of g conjugate pairs of eigenvalues of Frobenius acting on the Jacobian of the curve over $\mathbb{F}_q$.

DEFINITION 2. A curve C has defect k if $N(C) = q + 1 + gm - k$, $m = [2\sqrt{q}]$.

Fact 3.1 (Defect 0). We recall from [21] that a curve which meets the Serre-Weil bound has zeta function of type $[m, m, \ldots, m]$. When $g = 3$, by statement 7.1 in the Appendix, there does not exist a curve of type $[m, m, m]$ if

$$d = m^2 - 4q = -3, -4, -8, \text{or} - 11.$$

Fact 3.2 (Defect 1). We recall from [23] that a curve whose number of points is equal to $q + gm$ must have $g \leqslant 2$.

Fact 3.3 (Defect 2). We recall from [24] or [13] that if the fractional part of $2\sqrt{q}$, (which we denote by $\{2\sqrt{q}\}$), satisfies $\{2\sqrt{q}\} < \sqrt{3} - 1$, $(g \neq 4)$, then a curve whose number of points is equal to $q + gm - 1$ is of type $[m, m, \ldots, m-2]$.

4. Proofs of Theorems

This section is organized as follows. We will prove the theorems from Section 2 in the order they were stated. For each possible zeta function to be treated via the equivalence of categories, we must check the condition that the trace be relatively prime to the characteristic, and deal with special cases where this fails.

To begin, we notice that except for one special case $(q = 2)$, none of the fields in Theorems 1 and 2 have characteristic 2.

Fact 4.1. If $q = p^e$, $e > 1$, then $p \neq 2$ if q is of any of the following forms:

(i) $q = x^2 + 1$,

(ii) $q = x^2 + 2$,

(iii) $q = x^2 + x + 1$,

(iv) $q = x^2 + x + 3$.

Proof. In case (i), if q were a power of 2 then x would be odd, and so $x^2 \equiv 1 (\mathrm{mod}\, 8)$, which implies $q \equiv 2 (\mathrm{mod}\, 8)$. Thus $q = 2$, $e = 1$ is the only possibility.

In case (ii), x would be even, and we would have $x^2 \equiv 0 (\mathrm{mod}\, 4)$, which implies $q \equiv 2 (\mathrm{mod}\, 4)$.

In cases (iii) and (iv), $x^2 + x$ is always even, so q is odd. □

4.1. PROOF OF THEOREM 1

Write $q = p^e = x^2 + x + a$, $a = 1$ or $a = 3$, with $a \leqslant x$. Then $m = 2x + 1$, and $d = -3$ for $a = 1$, and $d = -11$ for $a = 3$.

PROPOSITION 1. *If q is of the form $q = p^e = x^2 + x + a$, $a = 1$ or $a = 3$, $a \leqslant x$, then m is prime to p unless $q = 3$.*

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

Proof. **a = 1.** Write $q = p^e = x^2 + x + 1$ with $m = 2x + 1$. Suppose p divides m, then $p^e = mx - (x^2 - 1)$ implies that p divides $(x^2 - 1)$. If p divides $(x + 1)$, then p divides x, which is impossible. So p divides $(x - 1)$. Thus p also divides $(x + 2)$ and 3. But Nagell and Ljunggren (see [19], for example) have shown that the only solution to $p^e = x^2 + x + 1$, $e \geqslant 3$, e odd, is $p = 7$, $e = 3$, $x = 18$. So no odd power of 3, $e \geqslant 3$, is of the form $x^2 + x + 1$. So $q = 3$ is the only exception. Indeed in that case $m = 3$.

a = 3. Write $q = p^e = x^2 + x + 3$ and $m = 2x + 1$. Again suppose p divides m. Then $p^e - 3m = x(x - 5)$ is divisible by p. We cannot have p divides x since then we would also have p divides $(x + 1)$. So in fact, p divides $(x - 5)$. In addition, $2p^e - mx = x + 6$ is divisible by p. Thus we must have $p = 11$. However, there are no solutions to the equation $11^e = x^2 + x + 3$ since there are no solutions modulo 5. □

PROPOSITION 2. *If q is of the form $q = p^e = x^2 + x + a$, $a = 1$ or $a = 3$, $a \leqslant x$, then $m - 2$ is prime to p unless $q = 343$ or possibly $p = 5$.*

Proof. **a = 1.** Write $q = p^e = x^2 + x + 1$ with $m = 2x + 1$. Suppose p divides $m - 2$. Then $2p^e - (m - 2)x = 3x + 2$ implies that p divides $3x + 2$ and $x + 3$ and $x - 4$. So $p = 7$. If $e = 1$, then $p = 7$ does not divide $2x - 1$. If e is odd, $e \geqslant 3$, then due to the result of Nagell and Ljunggren cited above, the only solution is $p = 7$, $e = 3$, $x = 18$. In that case, $p = 7$ divides 35, so $q = 343$ is an exception.

a = 3. Write $q = p^e = x^2 + x + 3$ and $m = 2x + 1$. Again suppose p divides $m - 2$. Then $(m - 2)^2 - 4p^e = -8x - 11$ is divisible by p, and so is $8x - 4$, which implies that p divides 15. If $p = 3$, then the only powers of p, e odd, which are of the form $x^2 + x + 3$ are 3 and $3^5 = 243$. This can be proved (as Serre pointed out to me) by Skolem's ℓ-adic method with $\ell = 5$ (in [26], Skinner attempted to give an ℓ-adic proof with $\ell = 11$, but his argument is incomplete). Neither $q = 3$ nor $q = 243$ satisfy the divisibility condition '3 divides $2x - 1$'. It would not be necessary to exclude $p = 5$ in the hypotheses if there were no solutions to the equation $5^e = x^2 + x + 3$ with $e \geqslant 3$, e odd and 5 dividing $2x - 1$. I have checked with the help of PARI that there are no solutions for $e < 1600$. □

4.1.1. $q = 3$

To prove Theorem 1, first consider the case $q = 3$. If $q = 3$, then $m = 3$, and the explicit formula bound is $N(C) \leqslant 10$. In fact, a curve C of genus 3 and defect 3 over $\mathbb{F}_3$ with $N(C) = 10 = q + 1 + 3m - 3$ was given in [24] with the equation $y^3 - y = x^4 - x^2$. Its zeta funtion is of type $[m, m, m - 3]$.

4.1.2. $q \neq 3$

By Fact 3.1, defect 0 is not possible because there is no indecomposable rank 3 Hermitian module of discriminant 1 when $d = -3$ or $d = -11$ (cf. [5]). By Fact 3.2, defect 1 is never possible for $g > 2$.

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

PROPOSITION 3. *If q is of the form $q = p^e = x^2 + x + a$, $a = 1$ or $a = 3$ with $a \leqslant x$, then a defect 2 curve of genus 3 is of type $[m, m, m-2]$.*

Proof. By Fact 3.3, it suffices to check that the fractional part of $2\sqrt{q}$ satisfies $\{2\sqrt{q}\} < \sqrt{3} - 1$. Suppose that $\{2\sqrt{q}\} \geqslant \sqrt{3} - 1$. We can write

$$\{2\sqrt{q}\} = \{\sqrt{4x^2 + 4x + 4a}\} = \sqrt{4x^2 + 4x + 4a} - (2x + 1),$$

so

$$\sqrt{4x^2 + 4x + 4a} \geqslant 2x + \sqrt{3}$$

and then

$$4a - 3 \geqslant 4x(\sqrt{3} - 1).$$

For $a = 1$, this implies $x = 0$, which is not possible. For $a = 3$, this implies $x \leqslant 3$, which does not occur for any q (see Note 2.1). □

PROPOSITION 4. *There is no indecomposable, rank 2, Hermitian module of discriminant 2 over R_d when $d = -3$ or $d = -11$.*

Proof. Since the class number of R_d is 1, projective R_d modules are free, so we can express a module P with a Hermitian form H as a matrix whose *ij*th entry is $H(e_i, e_j)$ where $\{e_i\}$ is a basis for P over R_d. A change of basis will give an equivalent matrix. We will work with the matrix in a reduced form. A rank 2 Hermitian form in 'reduced' form can be written as

$$\begin{bmatrix} \lambda & \bar{\alpha} \\ \alpha & \mu \end{bmatrix}$$

with $0 < \lambda \leqslant \mu \in \mathbb{Z}$, $\alpha \in R_d$. The condition that $H(x, y) = \overline{H(y, x)}$ implies that λ, $\mu \in \mathbb{Z}$, and we assume that e_1 is chosen with λ minimal so that $\lambda \leqslant \mu$. We are interested in Hermitian forms which are positive definite, so $\lambda > 0$.

The proof of the proposition relies on the following lemma:

LEMMA 1. *If d is square-free, satisfies $d \equiv 1 (\mathrm{mod}\, 4)$ and R_d has class number one, then we can find a basis for P over R_d such that the matrix for a Hermitian form in reduced form satisfies*

$$\frac{\alpha\bar{\alpha}}{\lambda^2} \leqslant \left(\frac{|d| + 1}{4}\right)^2 \frac{1}{|d|}.$$

Proof. If $\alpha\bar{\alpha}/\lambda^2$ is too large, we can replace α by $\alpha + \lambda r$ for any $r \in R_d$ by replacing the basis element e_2 by $e_2' = e_2 + \bar{r}e_1$. As a complex number,

$$(\alpha + \lambda r)\overline{(\alpha + \lambda r)} = |(\alpha + \lambda r)|^2,$$

and $|\lambda| = \lambda$, so it suffices to show that r can be chosen so that

$$|\frac{\alpha}{\lambda} + r|^2 \leqslant \left(\frac{|d| + 1}{4}\right)^2 \frac{1}{|d|}.$$

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

So it is enough to show that for every $z \in \mathbb{C}$, there exists an element $r \in R_d$ such that the distance squared from z to r is less than the bound. A $\mathbb{Z}$-basis for R_d is $\{1, (1+\sqrt{d})/2\}$. We look for the point in the complex plane which is furthest from a lattice point, or in other words, the smallest radius so that circles centered at the lattice points will cover the plane. It suffices to consider points in the right triangle with vertices $(0,0)$, $(\frac{1}{2},0)$, $(\frac{1}{2},\sqrt{|d|}/2)$, since we can then extend the argument by symmetry to the rest of the fundamental domain. We look for the point $(\frac{1}{2},a)$ in the triangle which is equidistant from the two lattice points, $(0,0)$ and $(\frac{1}{2},\sqrt{|d|}/2)$. Setting

$$\frac{\sqrt{|d|}}{2} - a = \sqrt{\frac{1}{4}+a^2},$$

we find

$$a = \frac{(|d|-1)}{4}\frac{1}{\sqrt{|d|}}.$$

Calculating the distance squared from this point to the origin we find exactly the bound stated in the lemma, and this point is the furthest possible distance away from the closest lattice point. □

Suppose that $\lambda\mu - \alpha\bar{\alpha} = 2$. The form $\left[\begin{smallmatrix}1 & 0\\ 0 & 2\end{smallmatrix}\right]$ is decomposable. If $\lambda = 1$, then

$$\alpha\bar{\alpha} \leqslant \left(\frac{|d|+1}{4}\right)^2\frac{1}{|d|} = \begin{cases}\frac{1}{3} & \text{if } d=-3,\\ \frac{9}{11} & \text{if } d=-11,\end{cases}$$

which implies that $\alpha = \bar{\alpha} = 0$ and thus $\mu = 2$. So it suffices to show $\lambda = 1$. Suppose $\lambda \geqslant 2$. For $d=-3$,

$$\mu \leqslant \frac{2+\alpha\bar{\alpha}}{\lambda} \leqslant \frac{2}{\lambda}+\frac{\lambda}{3},$$

which is less than λ if $\lambda \geqslant 2$. This contradicts the fact that $\lambda \leqslant \mu$. For $d=-11$,

$$\lambda^2 \leqslant \lambda\mu = 2+\alpha\bar{\alpha} \leqslant 2+\tfrac{9}{11}\lambda^2.$$

Thus $\lambda^2 \leqslant 11$, so $\lambda = 2$ or 3.

If $\lambda = 2$, then $\alpha\bar{\alpha} \equiv 0 \pmod 2$, and since $\alpha\bar{\alpha}/4 < 1$, we have $\alpha\bar{\alpha} = 2$ or $\alpha\bar{\alpha} = 0$. But 2 is not the norm of an element of R_{-11}, so $\alpha\bar{\alpha} = \alpha = 0$. Then we must have $\mu = 1$, and this contradicts $\lambda \leqslant \mu$.

If $\lambda = 3$, then $\alpha\bar{\alpha} \leqslant \frac{9}{11}9 < 8$.

But then $3\mu = 2+\alpha\bar{\alpha} \leqslant 9$ implies that $\mu = 3$ and $\alpha\bar{\alpha} = 7$. Again this is impossible since 7 is not the norm of an element of R_{-11}. □

Note 4.1.2. Proposition 4 can also be deduced from the results of Otremba (see [18]). In that paper, she proves (via the mass formula) that some Hermitian forms are ‘alone in their genus’; i.e. any lattice which is locally isomorphic to the given one

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

is globally isomorphic. See especially (for rank 2) pp. 9 and 13. These computations imply Proposition 4, provided one checks that every lattice with discriminant 2 is in the same genus as the decomposable one (the 1,2 lattice, in Otremba's notation).

4.1.3. *Glueing Criteria*

The following section is translated from [25]. Suppose that B and C are two polarized Abelian varieties over a perfect field k with polarization b: $B \to B^*$ and c: $C \to C^*$. Suppose that the polarizations have the same degree, n, and that n is prime to the characteristic, p, of k (if the characteristic is $\neq 0$). Denote by N_b and N_c the kernels of b and c; these are finite étale group schemes of order n^2. We will identify them with their $\bar{k}$ points. The Galois group $G = \mathrm{Gal}(\bar{k}/k)$ operates on these groups.

Let μ be the group of roots of unity, written additively. According to Mumford, [[14], p. 227], the polarizations b and c define nondegenerate, alternating bilinear forms on N_b and N_c, with values in μ, and compatible with the action of G. We will denote them by $(x, y) \mapsto \langle x, y\rangle$. Let f be a map f: $N_b \to N_c$ verifying the following conditions:

(1) *f is an isomorphism of G-modules*;
(2) $\langle f(x), f(y)\rangle = -\langle x, y\rangle$ *for all* $(x, y) \in N_b \times N_b$.

To the data (B, b, C, c, f) given above, we can now associate *an Abelian variety, A, isogenous to $B \times C$, equipped with a polarization a of degree* 1 as follows:

Let $B \times C$ have the polarization which is the product of the polarizations b and c. The kernel of $B \times C \to B^* \times C^*$ is $N_b \times N_c$. Let F be the subgroup of this kernel which is the graph of the isomorphism f. Property (2) above shows that F is totally isotropic; property (1) shows that F is stable by the action of G, i.e. that it is a finite étale k-subgroup of $B \times C$. According to Mumford [14], the polarization on $B \times C$ passes to the quotient by F. In other words, if we set $A = (B \times C)/F$, there exists a polarization a on A such that (b, c) factors through a

$$B \times C \to A \xrightarrow{a} A^* \to B^* \times C^*.$$

Comparing the degrees, we see that $\deg(a) = 1$, so a is principal.

This is how we obtain a polarized Abelian variety A by 'glueing' (B, b) to (C, c) via f.

4.1.4. $q \neq 3$ (*continued*)

The general framework for the glueing of polarized Abelian varieties can be applied in both backwards and forward directions. The following theorem works in the backwards direction ('unglueing').

THEOREM 4. *Suppose $q = p^e$, $q \neq 3$, $q \neq 343$, $p \neq 5$ and that q is of the form $q = x^2 + x + a$, $a = 1$ or $a = 3$ with $a \leqslant x$. Let $m = [2\sqrt{q}]$, $d = m^2 - 4q$. Let A be an Abelian variety over $\mathbb{F}_q$ isogenous to $E_m \times E_m \times E_{m-2}$ which has an indecomposable* *principal polarization. Then there exists a rank* 2 *indecomposable positive definite Hermitian form of discriminant* 2 *on* $\mathbb{Z}[\pi]$, $\pi = (-m + \sqrt{d})/2$.

Proof. We have that $m = 2x + 1$ and Propositions 1 and 2 show that the assumptions of the theorem imply that m and $m - 2$ are prime to the characteristic. In fact, the restriction $p \neq 5$ is not necessary if there are no solutions to the equation $5^e = x^2 + x + 3$ satisfying $e \geqslant 3$, e odd and 5 dividing $2x - 1$.

So all Abelian varieties in this proof are ordinary. Due to Fact 4.1, we also know that 2 is prime to the characteristic, so the group schemes we work with will be étale. Thus we will identify finite group schemes with their $\overline{\mathbb{F}_q}$-points. In the cases at hand, we have $d = -3$ or $d = -11$, so in particular, d is the discriminant of an imaginary quadratic field of class number one.

By the equivalence of categories given in the Appendix, it suffices to show that the indecomposable principal polarization on A induces an indecomposable polarization on $E_m \times E_m$ of degree 2, where E_m is an elliptic curve with $q + 1 + m$ points over $\mathbb{F}_q$.

Let F be the Frobenius endomorphism on A and V the Verschiebung, so that $\phi = F + V$ has eigenvalues $-m, -m, -m, -m, -(m-2), -(m-2)$. Let

$$B = \text{the connected component of the kernel of } \phi + m,$$

and

$$C = \text{the connected component of the kernel of } \phi + m - 2.$$

Then since $\mathbb{Q}(\sqrt{d})$ has class number one, $B \simeq E_m \times E_m$ and $C \simeq E_{m-2}$. We have A is isogenous to $B \times C$. We write $f\colon (B \times C) \to A$, with kernel Δ isomorphic to the intersection of B and C, $\Delta \simeq B \cap C$. The polarization λ on A induces polarizations b on B and c on C. It suffices to show that b is indecomposable of degree 2.

Let $N_b = \mathrm{Ker}(b)$, $N_c = \mathrm{Ker}(c)$. Together (b, c) is the induced polarization on $B \times C$, with kernel $N_b \times N_c$, and so we must have $B \cap C \subset N_b \times N_c$, embedded diagonally. We want to show that N_b has order 4.

By the definition of B and C, we know that $B \cap C$ is killed by 2, so it is contained in $C[2]$, which has order 4. In addition, $B \cap C$ is stable under the action of Frobenius, so it is an R-module, where $R = \mathbb{Z}[\pi] = \mathbb{Z}[x]/(x^2 - mx + q)$. But (2) is inert in R, so $R/2R \simeq \mathbb{F}_4$. So $B \cap C$ is an $\mathbb{F}_4$-vector space of order less than or equal to 4. $B \cap C$ cannot be trivial, or else A would be split and the polarization would be decomposable. So $B \cap C$ must have order 4 and the polarization (b, c) has degree 4. Since $B \cap C$ is embedded diagonally into $N_b \times N_c$, it follows that N_b has order 4.

In addition, B is orthogonal to C with respect to the skew-symmetric bilinear pairing $\langle , \rangle$ defined by the polarization of A on the ℓ-adic Tate module associated to A. This follows from the fact that ϕ is Hermitian with respect to the pairing, since

$$\phi^* = (F + V)^* = F^* + V^* = V + F = \phi.$$

Thus for elements $b \in T_l B$ and $c \in T_l C$ of the ℓ-adic Tate modules associated to B and C, we have

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

$$2\langle b, c\rangle = \langle b, 2c\rangle = \langle b, (\phi + m)c\rangle = \langle(\phi + m)b, c\rangle = 0.$$

This shows that they are orthogonal since $\mathbb{Z}_\ell(1)$ is torsion-free. Thus $B \cap C$ is maximal isotropic with respect to the pairing.

Finally, the polarization b is indecomposable, else λ would not be. □

COROLLARY 1. *There are no defect* 2 *curves in genus* 3 *over* $\mathbb{F}_q$ *if* q *is of the form* $q = x^2 + x + a$, $a = 1$ *or* $a = 3$ *with* $a \leqslant x$.

Proof. This is a direct consequence of Propositions 3 and 4 and Theorem 4. The exceptional cases can be handled individually. If $q = 3$, there is no defect 2 curve (see Section 4.1.1). If $q = 343$, then $m - 2 = 35$, so there is no elliptic curve over $\mathbb{F}_q$ with trace $\pm(m - 2)$. Thus there is no curve of type $[m, m, m - 2]$ over $\mathbb{F}_{343}$. Similiarly, if a solution to the equation $5^e = x^2 + x + 3$ exists with $e \geqslant 3$, e odd and 5 dividing $2x - 1$, then a curve of type $[m, m, m - 2]$ over $\mathbb{F}_{5^e}$ would fail to exist for the same reason. □

Thus we have established that $N_q(3) \leqslant q + 1 + 3m - 3$ for such q. To finish the proof of Theorem 1, we must show that there exists a curve C of genus $g(C) = 3$ over $\mathbb{F}_q$ such that $|N(C) - (q + 1)| = 3m - 3$.

PROPOSITION 5. *Let* $q = p^e = x^2 + x + a$, $a = 1$ *or* $a = 3$, *with* $a \leqslant x$, *and* $q \neq 3$, $q \neq 3^5$. *Then there exists a curve C of genus* $g(C) = 3$ *over* $\mathbb{F}_q$ *with zeta function of type* $\pm[m - 1, m - 1, m - 1]$.

Proof. Define $d' = (m - 1)^2 - 4q$. Recall that

$$d = m^2 - 4q = -3 \quad \text{or} \quad -11.$$

We first show that $(m - 1)$ is prime to p and $d' \notin \{-3, -4, -8, -11\}$.

To check that $(m - 1)$ is prime to p, write $m - 1 = 2x$. By Fact 4.1 we know that $p \neq 2$. So if p divides $(m - 1)$ then p must divide x. For $p^e = x^2 + x + 1$ this is impossible. If $p^e = x^2 + x + 3$ and p divides x, then $p = 3$. As explained in Proposition 2 above, the only powers of 3, e odd, of the form $3^e = x^2 + x + 3$ are 3 and $3^5 = 243$.

To show that $d' \notin \{-3, -4, -8, -11\}$ we write $d' = d - 2m + 1$, where $d = -3$ or $d = -11$. If $d = -3$, then $d' = -2m - 2$. So $d' \in \{-3, -4, -8, -11\}$ only if $m = 1$ or $m = 3$, which occurs only for $q = 3$, $m = 3$. Indeed, we assumed that $q \neq 3$, since in that case $[m - 1, m - 1, m - 1]$ is not possible. If $d = -11$, then $d' = -2m - 10$, which is not in the set $\{-3, -4, -8, -11\}$ for any $m > 1$.

Now we can apply the theory of Hermitian modules. By Theorem 8.2 in [5], there exists an indecomposable, positive definite, unimodular Hermitian module over $R_{d'}$ of rank 3. Applying the functor S from the Appendix to this module, we obtain an Abelian variety A isogenous to $E_{m-1} \times E_{m-1} \times E_{m-1}$ with an indecomposable principal polarization. Then by the Torelli theorem (cf. [13], Appendix), there exists a genus 3 curve X over $\mathbb{F}_q$ whose Jacobian is isomorphic either to A or to the quadratic twist of A; hence X is of type $\pm[m - 1, m - 1, m - 1]$. □

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

Note 4.1.4. Indeed if $q = 243$, there is no curve of type $\pm[m-1,\ m-1,\ m-1]$ since $m-1 = 30$, and Honda-Tate theory shows that there is no Abelian variety of dimension 3 over $\mathbb{F}_{243}$ corresponding to that trace of Frobenius (see [29]).

COROLLARY 2. *For $q = 7$ or $q = 13$, we have $N_q(3) = q + 1 + 3m - 3$.*

Proof. This was noted in [24]. It follows from Proposition 5 and the fact that a Frobenius with the opposite sign is not possible because the corresponding curve would have a negative number of points.

PROPOSITION 6. *Let $q = 3^5 = 243$. Then there exists a curve C of genus 3 over $\mathbb{F}_q$ with $|N(C) - (q+1)| = 3m - 3$.*

Proof. The only possible zeta function for defect 3 in this case is $[m, m, m-3]$. Since $m = 31$ is prime to 3, there exist elliptic curves E_m and E_{m-3}. Take the polarization b on $B = E_m \times E_m$ of discriminant 3 given by the matrix $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right]$. For the polarization on $C = E_{m-3}$ we take 3 times the canonical polarization. To glue B to C we must find an isomorphism of the kernels of b and c *as group schemes*, and since the order is not prime to the characteristic, it is not enough to consider $\overline{\mathbb{F}_q}$-points. The kernel of B is isomorphic to the 3-torsion of E_m. So both kernels are of (étale, local) type: $\mathbb{Z}/3\mathbb{Z} \times \mu_3$ (twisted), and there is only one choice for the pairing up to sign. □

Note 4.1.5. An explicit search for a genus 3 curve over $\mathbb{F}_{243}$ with the maximum or minimum number of points currently seems out of reach. Even counting the points on each of the approximately 243^6 homogeneous plane quartics in the variables x^2, y^2, z^2 using the naive method would take 3^{40} steps. A computation of this size is currently infeasible. A more fruitful approach may be to generate the equations of the elliptic curves E_m and E_{m-3}, which we can easily do, and to try to glue them together explicitly.

4.2. PROOF OF THEOREM 2

Suppose $q = x^2 + b$, $b = 1$ or $b = 2$ with b satisfying $b \leqslant x$. Again by Fact 3.1 there are no defect 0 curves since $d = -4$ or -8. By Fact 3.2, defect 1 curves do not exist for $g > 2$. It follows that $N_q(3) \leqslant q + 1 + 3m - 2$. It remains to show that there exists a curve C over $\mathbb{F}_q$ such that $|N(C) - (q+1)| = 3m - 2$.

PROPOSITION 7. *Suppose $q = x^2 + b$, $b = 1$ or $b = 2$ with b satisfying $b \leqslant x$. Then $(m, p) = 1$ and $(m-2, p) = 1$ unless $q = 2$.*

Proof. By Fact 4.1, p is not equal to 2 unless $e = 1$. Suppose that $q \neq 2$. Write $m = 2x$ and $m - 2 = 2(x-1)$.

If p divides m, then since $p \neq 2$ we have p divides x, which is not possible for either $b = 1$ or $b = 2$.

If p divides $(m-2)$, then p must divide $(x-1)$. If $b=1$, then this is impossible since $p^e=(x-1)(x+1)+2$ and $p\neq 2$. If $b=2$ and p divides $(x-1)$, then p divides $(q-3)$, so $p=3$. But there are no solutions to the equation $q=3^e=x^2+2$, meeting the congruence condition $x\equiv 1(\mathrm{mod}\,3)$ with $e>1$, since by [1] there exist at most two solutions to such an equation and in this case they are $e=1$, $x=1$ and $e=3$, $x=5$. The second solution does not satisfy the congruence condition and the first solution does not matter since we do not write $q=3$ in the form x^2+2 (see Note 2.2).

4.2.1. $q=2$

When $q=2$, a curve C of genus 3 and defect 2 over $\mathbb{F}_2$ was given in [24]. Its equation is:

$$x^3y+y^3z+z^3x+x^2y^2+y^2z^2+z^2x^2+x^2yz+y^2xz=0$$

and it has 7 points, which is defect 2 since $m=2$. It has zeta function of type

$$\left[m+1-4\cos^2\left(\frac{\pi}{7}\right), m+1-4\cos^2\left(\frac{2\pi}{7}\right), m+1-4\cos^2\left(\frac{3\pi}{7}\right)\right].$$

This is possible because

$$2\sqrt{2}>1-4\cos^2\left(\frac{3\pi}{7}\right),$$

and it is the only zeta function possible for this case. It is a twist of the Klein curve which becomes isomorphic to the Klein curve over the field $\mathbb{F}_{2^7}$.

It is interesting to note that when $q=2$, the zeta function type $[m,m,m-2]$ is not possible because the curve would have 7 points over $\mathbb{F}_2$ but only 1 point over $\mathbb{F}_8$. Alternatively, we can show that the glueing of the supersingular elliptic curves is not possible by examining the group schemes in question and showing there is no isomorphism between them.

The zeta function type $[m, m+\sqrt{3}-1, m-\sqrt{3}-1]$ is not possible because the curve would have 7 points over $\mathbb{F}_2$ but only 5 points over $\mathbb{F}_4$.

4.2.2. $q\neq 2$

Now assume $q\neq 2$. In order to have a genus 3 curve of type $[m,m,m-2]$, there must exist an indecomposable Hermitian module of rank 2 and discriminant 2 over R_d. When $d=-4$ or $d=-8$, an indecomposable Hermitian module of rank 2 and discriminant 2 exists and is given for $d=-4$ by

$$\begin{bmatrix} 2 & 1+i \\ 1-i & 2 \end{bmatrix}$$

and for $d=-8$ by

$$\begin{bmatrix} 2 & -\sqrt{-2} \\ \sqrt{-2} & 2 \end{bmatrix}.$$

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

In both cases, the module is indecomposable because all the values taken by the Hermitian form are divisible by 2, so 1 is not represented. But if the form were equivalent to $\left[\begin{smallmatrix}1 & 0\\ 0 & 2\end{smallmatrix}\right]$, then 1 would be represented.

The next theorem shows that in this case it is possible to glue two Abelian varieties together to obtain the Jacobian of a genus 3 curve with the desired property.

THEOREM 5. *Suppose $q = x^2 + j$, $j = 1$ or $j = 2$ with j satisfying $j \leqslant x$, and suppose $q \neq 2$. Then there exists an Abelian variety A over $\mathbb{F}_q$, isogenous to $E_m \times E_m \times E_{m-2}$, with an indecomposable principal polarization.*

Proof. By Fact 4.1, the characteristic of the field is not equal to 2, and by Proposition 7, there exist Abelian varieties $B = E_m \times E_m$ and $C = E_{m-2}$.

$\mathbf{j = 1}$. Let b be the polarization on B corresponding to the positive definite indecomposable Hermitian module

$$\begin{bmatrix} 2 & 1+i \\ 1-i & 2 \end{bmatrix}.$$

Let c be two times the canonical polarization on C. It has kernel equal to the 2-torsion of C. We proceed by calculating the kernel of b and then glueing it to the kernel of c. The order of (the $\overline{\mathbb{F}}_q$ points of) these group schemes is 4, which is prime to the characteristic. By Mumford's criteria, we need to find an isomorphism of the Galois modules which is an anti-isometry with respect to the pairings. If necessary, we will replace C by an isogenous elliptic curve.

The kernel of b is $E_m[\lambda] \times E_m[\lambda]$, where $E_m[\lambda]$ is the λ-torsion of E_m, and $\lambda = 1 + i$. The λ-torsion of the elliptic curve is contained in the 2-torsion, since $2 = (1+i)(1-i)$. The Frobenius of E_m acts on the 2-torsion of E_m by fixing one of the three nontrivial points and by exchanging the other two. This can be seen by looking at the 2×2 matrix which represents the action of Frobenius on the ℓ-adic Tate module when $\ell = 2$. The characteristic polynomial of Frobenius is $t^2 + mt + q$, where $-m$ is the trace of the matrix and q is the determinant. In this case, $q = x^2 + 1$ and $m = 2x$, with x even since q is odd. Thus we have $m \equiv 0 \pmod 4$. So the number of points on the elliptic curve over $\mathbb{F}_q$, $N(E_m)$, satisfies

$$N(E_m) = q + 1 + m \equiv 2 \pmod 4.$$

Similarly,

$$N(E_{m-2}) = q + 1 + m - 2 \equiv 0 \pmod 4.$$

In both cases, the trace is even and the determinant is odd, so the possibilities for the matrix of Frobenius (mod 2) are:

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

The first three of these matrices act on the 2-torsion by fixing one of the three nontrivial points and by exchanging the other two. The last one is the identity matrix and fixes all three nontrivial 2-torsion points. But the identity matrix is only possible if $N(E) \equiv 0 (\mathrm{mod}\, 4)$, while the first three are possible in either case. This follows by writing the matrix with entries $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, the number of points on E as

$$N(E) = (ad - bc) + 1 - (a + d),$$

and considering all the possibilities for the entries (mod 4).

So we only need to chose C to be an elliptic curve E_{m-2} with Frobenius fixing one of its 2-torsion points and switching the other two. It suffices to take an elliptic curve with endomorphism ring $\mathbb{Z}[\pi] \subset R'$ such that $(\pi - 1)/2 \notin R'$. It follows from Deuring that such a curve exists. By chosing C in this way we can find an isomorphism of $C[2]$ with the kernel of b which respects the action of Frobenius. Finally, the Galois module isomorphism must be an anti-isometry with respect to the pairings. The pairings take values ± 1.

j = 2. The proof is almost the same except in this case $\lambda = \sqrt{2}$ and the polarization on B is given by the matrix

$$\begin{bmatrix} 2 & -\sqrt{-2} \\ \sqrt{-2} & 2 \end{bmatrix}.$$

Again we have

$$N(E_m) = q + 1 + m = x^2 + 3 + 2x \equiv 2 \ (\mathrm{mod}\, 4),$$

and

$$N(E_{m-2}) = q + 1 + m - 2 = x^2 + 1 + 2x \equiv 0 \ (\mathrm{mod}\, 4),$$

since x is odd. So the same argument works. □

COROLLARY 3. *If $q = x^2 + j$, $j = 1$ or $j = 2$ with j satisfying $j \leqslant x$, and $q \neq 2$, then there exists a curve of type $\pm[m, m, m - 2]$.*

Proof. This follows from Theorem 5 and the fact that (see [17]): if A is a principally polarized indecomposable Abelian variety of dimension 3, over an algebraically closed field, then A is the Jacobian of a curve. The 'precise Torelli' theorem in the Appendix to [13] allows descent from the algebraically closed field to any field at the cost of quadratic twist, as is explained there.

EXAMPLE. An example of a genus 3 curve corresponding to this type of glueing was found by Van der Geer and Van der Vlugt. It can be described as the curve over $\mathbb{F}_{27}$ obtained by taking the fiber product of $y^2 = x^3 + 2x^2 + 2x$ with $y^2 = 2x^3 + 2\alpha^4 x^2 + \alpha^8 x$, where $\alpha^3 + 2\alpha^2 + 1 = 0$. It is a defect 2 curve with 56 points (instead of 58 as stated in [3]).

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

4.3. PROOF OF THEOREM 3

Let $q = p^e$ be a power of a prime. We divide the proof into two cases: e even and e odd.

e *even*. First suppose $e = 2r$ is even. Then Ibukiyama has shown [8] that, for p an odd prime, there exists a curve C of genus 3 over $\mathbb{F}_p$ such that

$$\#C(\mathbb{F}_{p^{2r}}) = 1 + p^{2r} + (-1)^{r+1} 6p^r.$$

Thus for all q an even power of an odd prime, there exists a genus 3 curve attaining either the Weil maximum or the Weil minimum.

Now suppose that $p = 2$, so that $q = 2^{2r}$. Then $m = 2^{r+1}$, and $(m-1)$ is prime to p. If we let $d' = (m-1)^2 - 4q$, then $d' = -2^{r+2} + 1$, and so we see that for $r \geqslant 1$,

$$d' \notin \{-3, -4, -8, -11\}.$$

By Theorem 8.2 in [5], there exists an indecomposable, positive definite, unimodular Hermitian module over $R_{d'}$ of rank 3. Applying the functor S from the Appendix to this module, we obtain an Abelian variety isogenous to $E_{m-1} \times E_{m-1} \times E_{m-1}$ with an indecomposable principal polarization. Then by the Torelli theorem, (see the Appendix to [13]) there exists a genus 3 curve over $\mathbb{F}_q$ which is of type $\pm[m-1, m-1, m-1]$.

For example, over $\mathbb{F}_4$, the equation of the Klein curve is given in [24] to show that $N_4(3) = 14$. It is a curve of type $[m-1, m-1, m-1]$.

e *odd*. Now suppose that e is odd. As usual, write $q = x^2 + x + a$, with $-x \leqslant a \leqslant x$. We divide the proof according to the value of $d = m^2 - 4q$. If $d \in \{-3, -4, -8, -11\}$, then these cases have been treated in Theorems 1 and 2.

If d is not in the set$\{-3, -4, -8, -11\}$, we check whether m is prime to p. If $(m, p) = 1$, then a curve of type $[m, m, m]$ or $[-m, -m, -m]$ exists. If not, then $(m-1)$ is prime to p. It remains to check that

$$d' = (m-1)^2 - 4q \notin \{-3, -4, -8, -11\}.$$

Since $d' = d - 2m + 1$ and $d \equiv 0 \text{ or } 1 \pmod 4$, this could only occur for $d = -7$ and $m = 1$, but $m > 1$, so it does not occur. Thus there exists a curve of type $[m-1, m-1, m-1]$ or of type $[-(m-1), -(m-1), -(m-1)]$ in this case. □

Acknowledgements

I would like to thank J-P. Serre for his letters on Hermitian modules which inspired this project, and for his generous help and time spent working on it. This paper is based on work supported by a Mentoring Grant from the Association for Women in Mathematics. I would also like to thank Jim Milne and René Schoof for helpful discussions and Fritz Beukers for the reference to Apéry's paper.

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

Appendice: Modules hermitiens et courbes algébriques, J-P. Serre, 1999

1. NOTATIONS

On note k un corps fini à q éléments de caractéristique p. On se donne un entier a et l'on pose $d = a^2 - 4q$. On suppose:

(1.1) *a est premier à p;*
(1.2) $d < 0$**;**
(1.3) *d est le discriminant d'un corps quadratique imaginaire.*

On pose $R = \mathbb{Z}[X]/(X^2 - aX + q)$. Vu les hypothèses ci-dessus, R est l'anneau des entiers du corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{d})$, dans lequel p est décomposé.

(L'hypothèse (1.3) n'est pas indispensable pour la suite; il est souvent commode de ne pas la faire; on doit alors travailler avec des 'ordres' non maximaux de K.)

On choisit une courbe elliptique E sur k dont les valeurs propres de Frobenius sont $\frac{1}{2}(a \pm \sqrt{d})$ (son nombre de points est donc $q + 1 - a$). On sait qu'il en existe.

2. LA CATÉGORIE Ab(a,q)

On note Ab(a,q) la catégorie des variétés abéliennes sur k ayant les propriétés équivalentes suivantes:

(2.1) *A est k-isogène à un produit de copies de E.*
(2.2) *Si F_A et V_A désignent respectivement le Frobenius et le 'Verschiebung' de A, on a $F_A + V_A = a$ dans* $\mathrm{End}(A)$
(2.3) *Les valeurs propres de F_A sont celles de F_E, répétées g fois où $g = \dim A$.*

(L'équivalence de ces propriétés résulte de théorèmes de Tate.) On aura besoin plus loin de la propriété suivante:

(2.4) *Si A,B appartiennent à Ab(a,q), et si f: $A \to B$ est un homomorphisme défini sur une extension k' de k, alors f est défini sur k.*

En effet, on peut supposer que k' est une extension finie de k. Soit $m \geqslant 1$ son degré. Puisque f est défini sur k', il commute à la puissance m-ème du Frobenius. Mais si π est le Frobenius (i.e. le générateur 'X' de R), l'anneau $\mathbb{Z}[\pi^m]$ est unsous-anneau *d'indice fini* de $R = \mathbb{Z}[\pi]$. La commutation avec π^m entraîne donc celle avec π.

3. UNE ÉQUIVALENCE DE CATÉGORIES

Notons Mod(R) la catégorie des R-modules sans torsion de type fini (i.e. projectifs de type fini, vu que R est un anneau de Dedekind, grâce à (1.3)).

Noter que R opère sur toute variété A de Ab(a,q); de plus, d'après (2.4), tout f: $A \to B$ est un R-homomorphisme.

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

Si $A \in \mathrm{Ab}(a, q)$, notons $T(A)$ le R-module $\mathrm{Hom}(E,A)$. C'est un élément de $\mathrm{Mod}(R)$.

(3.1) *Le foncteur* T: $Ab(a, q) \to \mathrm{Mod}(R)$ *est une équivalence de catégories.*

On a en particulier un isomorphisme naturel:

$$\mathrm{Hom}(A, B) = \mathrm{Hom}_R(T(A), T(B)).$$

On peut expliciter un foncteur S: $\mathrm{Mod}(R) \to \mathrm{Ab}(a, q)$ qui est 'inverse' au foncteur T: si $L \in \mathrm{Mod}(R)$, on définit $S(L)$ comme la variété abélienne $L \otimes_R E$, 'produit tensoriel' de L par E (de tels produits tensoriels existent dans toute catégorie abélienne; on écrit L comme conoyau d'un homomorphisme $R^N \to R^M$ et l'on définit $L \otimes_R E$ comme le conoyau de l'homomorphisme correspondant: $E^N \to E^M$).

Les assertions ci-dessus entraînent en particulier:

(3.2) *Toute variété abélienne* A *appartenant à* $Ab(a,q)$ *peut s'écrire sous la forme* $L \otimes_R E$ *avec* $L = \mathrm{Hom}(E, A)$.

(Dans ce qui suit, j'abrègerai $L \otimes_R E$ en A_L.)

Bien sûr, on a:

(3.3) $\mathrm{rang}(L) = \dim A_L$.

(3.4) $A_R = E$.

Si M est un sous-module d'indice fini de L, l'inclusion $M \to L$ définit un morphisme f: $A_M \to A_L$ qui est une *isogénie*; de plus:

(3.5) *Le degré de* f *est égal à* $(L : M)$

EXEMPLE: *le cas où* $\dim A = 1$.

Ce cas correspond à $\mathrm{rang}(L) = 1$; autrement dit L est un R-module inversible. Les classes de tels modules correspondent aux éléments de $\mathrm{Cl}(R) = \mathrm{Pic}(R)$; leur nombre est le *nombre de classes* $h(d)$ de l'anneau R. On conclut de là que le nombre des classes d'isomorphisme de courbes elliptiques k-isogènes à E est égal à $h(d)$; on retrouve un résultat bien connu.

4. DUALITÉ

Si A appartient à $\mathrm{Ab}(a,q)$ il en est de même de sa *duale* A^*, puisque A et A^* sont k-isogènes.

Si L appartient à $\mathrm{Mod}(R)$, notons L^* son *anti-dual*, autrement dit l'ensemble des homomorphismes f: $L \to R$ qui sont anti-linéaires, i.e. tels que $f(rx) = \bar{r}f(x)$ pour $r \in R$ et $x \in L$.

Les foncteurs $A \mapsto A^*$ et $L \mapsto L^*$ se correspondent par le dictionnaire du §3. Autrement dit:

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

(4.1) *Si $A \in \mathrm{Ab}(a, q)$ correspond au module L, sa duale A^* correspond au module L^*.*

(Le fait que l'on prenne l' *anti*-dual, et non le dual, provient de ce que la transposition sur $\mathrm{End}(E) = R$ est la conjugaison complexe.)

5. POLARISATIONS

Une polarisation est un morphisme φ: $A \to A^*$ qui provient d'un diviseur ample sur A (cf. [14]). Si A correspond au module L, φ correspond par (4.1) à un morphisme $L \to L^*$, autrement dit à une forme sesquilinéaire H: $L \times L \to R$. De plus:

(5.1) *H est une forme hermitienne définie > 0.*

(Autrement dit on a $H(x,y)$ = conjugué de $H(y,x)$ pour $x, y \in L$, et $H(x, x) > 0$ si $x \neq 0$.)

Inversement:

(5.2) *Toute forme hermitienne définie > 0 sur L définit une polarisation de A.*

Une polarisation φ a un degré $\deg(\varphi)$ défini par:

$$\deg(\varphi)^2 = \text{ordre du schéma en groupes fini } \mathrm{Ker}(\varphi).$$

En termes de L et de la forme hermitienne h: $L \to L^*$, ceci se traduit par:

(5.3) $\deg(\varphi)^2 = (L^* : hL)$.

En particulier:

(5.4) *Pour que φ soit une polarisation principale* (*i.e.* $\deg(\varphi) = 1$), *il faut et il suffit que $hL = L^*$* (auquel cas on dit que H est R-non dégénérée, ou encore que le discriminant du module hermitien L est égal à 1).

Lorsque L est un R-module libre (ce qui est toujours le cas si $h(d) = 1$) et qu'on en choisit une base (e_i), la forme H est donnée par une matrice hermitienne (r_{ij}) et la condition que le discriminant soit 1 se traduit par $\det((r_{ij})) = 1$.

6. POLARISATIONS PRINCIPALES INDÉCOMPOSABLES

Soit $L \in \mathrm{Mod}(R)$, muni d'une forme hermitienne > 0 de discriminant 1. Soit A la variété abélienne polarisée correspondante. Vu le §5, on a:

(6.1) *Pour que A soit indécomposable* (comme variété abélienne polarisée), *il faut et il suffit que L soit indécomposable comme module hermitien.*

Noter que, à cause de (2.4), la notion d'indécomposabilité pour A a le même sens sur k, ou sur toute extension de k. Il s'ensuit qu'un module hermitien

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

indécomposable donne une variété abélienne polarisée qui est ‘absolument’ indécomposable.

On peut donner des exemples d’anneaux R qui n’ont aucun module hermitien indécomposable (de discriminant 1) en dimension g égale à 2 ou 3. D’après Hoffmann (cf [5]), ce sont:

(6.2) *Pour* $g = 2$, *les cas* $d = -3, -4, -7$;
(6.3) *Pour* $g = 3$, *les cas* $d = -3, -4, -8, -11$.

Hoffmann a également montré que, pour $g = 2, 3$ les valeurs ci-dessus sont les *seules valeurs* de d pour lesquelles tous les modules hermitiens de discriminant 1 sont décomposables.

7. APPLICATION AUX COURBES ALGÉBRIQUES

Ce qui précède s’applique à la jacobienne J d’une courbe de genre g définie sur k (et dont les valeurs propres de Frobenius sont celles de E répétées g fois). Comme J est munie d’une polarisation principale indécomposable, on déduit de là:

(7.1) *Pour* $g = 2, 3$ *il n’existe aucune courbe* C *dont la jacobienne appartienne à* $Ab(a,q)$, *si* $d = a^2 - 4q$ *a l’une des valeurs données dans* (6.2) *et* (6.3).

Posons, comme d’habitude $m = [2q^{1/2}]$ et supposons $m \neq 0 \pmod{p}$. Supposons que le nombre N de points de la courbe soit égal à $q + 1 + gm$. On sait que J appartient alors à $\mathrm{Ab}(a, q)$, avec $a = -m$. On déduit de là et de (7.1) que la courbe en question n’existe pas lorsque:

$$g = 2, \quad m^2 - 4q = -3, -4, \text{ou} -7;$$

$$g = 3, \quad m^2 - 4q = -3, -4, -8, \text{ou} -11.$$

(Même résultat si $N = q + 1 - gm$, car cela ne fait que changer le signe de a.)

Ainsi, par exemple, il n’existe aucune courbe de genre 3 sur $\mathbf{F}_{27}$ ayant 58 points, car une telle courbe donnerait $d = -8$.

On peut aussi procéder en sens inverse, et utiliser des modules hermitiens indécomposables de rang 2 ou 3 pour construire (ou plutôt pour prouver l’existence...) de courbes. En effet, soit L un R-module hermitien indécomposable R-non dégénéré de rang 2 (resp. 3). En appliquant le théorème de Torelli à A_L, on en déduit:

(7.2) *Si* $g = 2$, *il existe une courbe* C *sur* k *dont la jacobienne est isomorphe à* A_L (et qui a donc $q + 1 - 2a$ points).

(7.3) *Si* $g = 3$, *il existe une courbe* C *sur* k *dont la jacobienne est isomorphe soit à* A_L, *soit à la ‘tordue quadratique’ de* A_L (et qui a donc $q + 1 - 3a$ points dans le premier cas et $q + 1 + 3a$ points dans le second cas).

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

De plus, dans le cas $g = 3$, si la courbe considérée n'est pas hyperelliptique le cas '$-3a$' exclut le cas '$+3a$'. Autre propriété de ce cas (conséquence de Torelli, ici aussi): si C est la courbe considérée, supposée non hyperelliptique, son groupe d'automorphismes $\mathrm{Aut}(C)$ est un sous-groupe d'indice 2 de $\mathrm{Aut}(L)$; de façon plus précise, on a $\mathrm{Aut}(L) = \{\pm 1\} \times \mathrm{Aut}(C)$.

Par contre, si $g = 2$, ou si $g = 3$ et C est hyperelliptique, on a $\mathrm{Aut}(L) = \mathrm{Aut}(C)$.

EXEMPLE. Prenons $q = 41$, $g = 3$, $a = \pm m = \pm 12$, de sorte que $d = -20$. D'après Hoffmann, il y a deux possibilités pour L, avec chaque fois $\mathrm{Aut}(L) = \{\pm 1\} \times S_3$. D'où l'existence de courbes de genre 3 sur $\mathbf{F}_{41}$, ayant soit 78 points (ce qui serait le maximum), soit 6 points (ce qui serait le minimum). Chacune de ces deux courbes a un groupe d'automorphismes qui est, soit $\{\pm 1\} \times S_3$, soit S_3.

Remarque. On peut utiliser (7.2) et (7.3) pour démontrer certains cas de (6.2) et (6.3). Prouvons par exemple que, pour $d = -8$, $g = 3$, il n'y a pas de module hermitien indécomposable de discriminant 1. S'il y en avait un, par (7.3) appliqué à $q = 3$, $a = 2$, il y aurait:

soit une courbe C dont les valeurs propres de Frobenius sont $1 \pm \sqrt{-2}$ (répétées 3 fois): son nombre de points serait $q + 1 - 3a = 3 + 1 - 6 = -2$, ce qui est impossible;

soit une courbe dont les valeurs propres de Frobenius seraient les opposées des précédentes; sur $\mathbf{F}_{27}$, ce seraient $-(1 \pm \sqrt{-2})^3 = 5 \pm \sqrt{-2}$, et le nombre de points serait $27 + 1 - 30 < 0$, ce qui est encore impossible!

---

chère Kristin,
Voici quelques compléments sur le texte 'Modules hermitiens...' que je vous avais envoyé en janvier.

Un certain nombre d'énoncés avaient été laissés sans démonstrations. Je vais les reprendre:

1. Le plus important est:

(3.1) *Le foncteur* T: $Ab(a, q) \to \mathrm{Mod}(R)$ *est une équivalence de catégories.*

J'avais donné une partie de l'argument, à savoir la construction d'un foncteur appelé 'S' qui transforme $L \in \mathrm{Mod}(R)$ en la variété abélienne $A_L = L \otimes_R E$. Ce foncteur a des propriétés agréables, et faciles à démontrer, par exemple

$$\mathrm{Hom}(S(L), S(L')) = \mathrm{Hom}_R(L, L').$$

Cela montre déjà que $T \circ S$ est l'identité, et donc que T est injectif. Pour montrer que $S \circ T = 1$ (avec un certain abus de notation!), on est ramené à prouver l'énoncé:

(3.2) *Toute variété abélienne* $A \in Ab(a, q)$ *est de la forme* A_L *pour un* L *convenable.*

C'est là le point essentiel. Il va résulter de:

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

(3.6) *Soit $A \to B$ une isogénie dans $Ab(a, q)$. Si B est de la forme A_L, alors il en est de même de A* (pour un module L' convenable).

(D'après (2.1), A est isogène à $E \times \cdots \times E$; on applique alors (3.6) à $B = E \times \cdots \times E$, qui est de la forme A_L, avec $L = R \times \cdots R$.)

Pour prouver (3.6), il nous faut contrôler les isogénies de variétés abéliennes, et c'est ici que l'hypothèse 'ordinaire' vaêtre essentielle. Il me faut rappeler des choses connues. Plaçons-nous d'abord sur un corps algébriquement clos k (on prendra ensuite pour k une clôture algébrique du corps fini k). Soit A une variété abélienne sur k, de dimension n. Si l est un nombre premier $\neq$ caractéristique k, on sait ce qu'est le l-ième *module de Tate* $T_l(A)$ de A: c'est la limite projective des points de l^m-division de A. C'est un $\mathbf{Z}_l$-module libre de rang $2n$. Ce module 'contrôle' les isogénies $A' \to A$ de degré une puissance de l, au sens suivant: une telle isogénie correspond bijectivement à un sous-$\mathbf{Z}_l$-module d'indice fini de $T_l(A)$ (à savoir l'image de $T_l(A')$ dans $T_l(A)$). Dans notre cas (k fini et k clôture algébrique de k), on voit en outre que les k-isogénies correspondent aux sous-modules de $T_l(A)$ qui sont stables par l'action de Galois, i.e. par le Frobenius π: puisqu'on a supposé $A \in \mathrm{Ab}(a, q)$, cela veut dire que le sous-module en question est stable par R. Finalement, on voit que les k-isogénies $A' \to A$ qui sont de degré une puissance de l sont classifiées par les sous-R_l-modules de $T_l(A)$, où $R_l = R \otimes \mathbf{Z}_l$. Dans le cas particulier $A = E$, on constate que $T_l(E)$ est un *R_l-module libre de rang 1* (regarder les rangs!). Si A est de la forme A_L, on constate aussi que $T_l(A) = T_l(E) \otimes_R L = T_l(E) \otimes L_l$, où le produit tensoriel est pris sur R_l et L_l désigne $\mathbf{Z}_l \otimes L = R_l \otimes_R L$. Il est alors immédiat que les R_l-sous-modules de $T_l(A)$ d'indice fini sont de la forme $T_l(E) \otimes L'$ où L' est un sous-R-module de L d'indice une puissance de l, et l'on a alors $A' = E \otimes L'$. Autrement dit, *l'énoncé (3.6) est vrai si le degré de l'isogénie est de la forme l^m avec $l \neq p$.*

On est donc ramené à regarder le cas où le degré est une puissance de la caractéristique p, Evidemment, tout revient ici encore à contrôler les isogénies. Pour une variété abélienne quelconque, cela peut se faire au moyen d'un *module de Dieudonné* convenable. Heureusement, les variétés abéliennes qui nous intéressent ici sont *ordinaires*, et cela simplifie beaucoup la situation. En effet, pour une telle variété A, on peut définir un 'p-ième module de Tate' $T_p(A)$ qui a exactement les mêmes propriétés que les T_l, à savoir: c'est un $\mathbf{Z}_p$-module libre de rang $2n = 2.\dim(A)$, et il contrôle les p-isogénies comme ci-dessus. Ce module est somme directe de deux modules de rang n:

$$T_p(A) = T_p(A)_e \oplus T_p(A)_i$$

(e = étale; i = infinitésimal).

La partie étale $T_p(A)_e$ est définie comme la limite projective des points de p^m-division de A; la partie infinitésimale $T_p(A)_i$ peut se définir comme le Hom (dans la catégorie des groupes formels) de $\mathbf{G}_m$ dans A, ou bien comme le $\mathbf{Z}_p$-dual de $T_p(A^*)_e$, où A^* est la duale de A. On démontre que l'on a les mêmes propriétés que ci-dessus pour les T_l. Noter que l'anneau $R_p = \mathbf{Z}_p \otimes R$ est égal à $\mathbf{Z}_p \times \mathbf{Z}_p$ (les

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

deux facteurs étant caractérisés par le fait que π donne une unité dans le premier, et un élément de l'idéal maximal dans le second). Cette décomposition de R_p est compatible avec la décomposition en deux morceaux de $T_p(A)$, ainsi qu'avec le fait que toute p-isogénie se décompose en une isogénie étale et une isogénie radicielle. Bref, tout marche très bien, et l'on arrive ainsi à démontrer (3.6) pour les p-isogénies.

(Une autre façon de justifier (3.2) et (3.6) consiste à utiliser un résultat de Deligne (*Invent. Math.* **8** (1969), 238–243) qui donne une équivalence de la catégorie des variétés abéliennes ordinaires sur $\overline{\mathbf{F}}_p$ avec la catégorie des $\mathbf{Z}$-modules libres de type fini munis d'un endomorphisme F ayant un certain nombre de propriétés raisonnables.

Cet article de Deligne contient quelques références, mais pas beaucoup. La théorie du T_p des variétés ordinaires est connue depuis longtemps (voir par exemple mon article de l'Amer.J. 80 (1958), 715–739), mais n'intéresse pas les spécialistes, car elle est trop simple! Le cas amusant est le cas supersingulier, étudié en détail par Oort: on y trouve des familles 'continues' de p-isogénies.)

2. Il faut parler un peu de la dualité et des isogénies (§§ 4,5). L'énoncé (4.1) ne présente pas de difficultés. Le point essentiel est que, pour la courbe elliptique E, le transposé f^* d'un endomorphisme f de E est égal au *conjugué* $\bar{f}$ de f, lorsqu'on identifie f à un élément de R, qui est une extension quadratique de $\mathbf{Z}$.

Passons aux *polarisations*. Soit φ: $A \to A^*$ un morphisme, et supposons que $A \in Ab(a, q)$ soit associé au module L, auquel cas A^* est associé à l'anti-dual L^* de L. Alors φ correspond à une application R-linéaire h: $L \to L^*$, ou, ce qui revient au même, à une application sesquilinéaire H: $L \times L \to R$.

Si φ est une polarisation, on a $\varphi^* = \varphi$, ce qui se traduit par $h^* = h$, ou encore par le fait que H est une *forme hermitienne*.

Inversement, si H est une telle forme, il lui correspond φ: $A \to A^*$ avec $\varphi^* = \varphi$. Il en résulte (cf. Mumford, *Abelian Varieties*, p. 188, th. 2, et p. 189, Remarque) que φ est de la forme 'φ_D' pour un diviseur D sur A. Dire que φ est une polarisation équivaut à dire que D est *ample*. Pour prouver (5.1) et (5.2) je dois montrer que *cela se produit si et seulement si H est définie > 0.*

Je peux remplacer A par une variété isogène. En effet, si $A' \to A$ est une isogénie, le morphisme φ: $A \to A^*$ définit φ': $A' \to A'^*$ en composant: $A' \to A \to A^* \to A'^*$, et il est facile de voir que φ est une polarisation si et seulement si φ' en est une. Même méthode pour le fait que H soit définie > 0. Ceci permet de choisir pour A' le produit $E \times \cdots E = E^n$, auquel cas son dual est aussi E^n, et φ est donnée par une matrice hermitienne (a_{ij}) à coefficients dans R.

On applique alors un résultat qui se trouve dans Mumford (p.210, lignes 4 à 6). On peut aussi raisonner directement, en utilisant encore une autre isogénie pour se ramener au cas où la matrice (a_{ij}) est une matrice *diagonale* avec des entiers (d_i) sur la diagonale. Le fait que cette matrice donne une polarisation de E^n si (et seulement si) les d_i sont > 0 est immédiat.

Bien à vous.

J-P. SERRE

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

References

1. Apéry, R.: Sur une équation diophantienne, *C.R. Acad. Sci. Paris Sér. A* **251** (1960), 1451–1452.
2. Auer, R.: Ray class fields of global function fields with many rational places, *Acta Arith.* **95**(2) (2000), 97–122.
3. Van der Geer, G. and van der Vlugt, M.: Tables of curves with many points, *Math. Comp.* **69**(230) (2000), 797–810.
4. Frey, G. and Kani, E.: Curves of genus 2 covering elliptic curves and an arithmetical application, *Arithmetic Algebraic Geometry* (*Texel, 1989*), Progr. Math. 89, Birkhäuser, Boston, 1991, pp.153–176.
5. Hoffmann, D. W.: On positive definite hermitian forms, *Manuscripta Math.* **71** (1991), 399–429.
6. Howe, E.: Principally polarized ordinary abelian varieties over finite fields, *Trans. Amer. Math. Soc.* **347**(7) (1995), 2361–2401.
7. Howe, E., Leprévost, F. and Poonen, B.: Large torsion subgroups of split Jacobians of curves of genus two or three, *Forum Math.* **12**(3) (2000), 315–364.
8. Ibukiyama, T.: On rational points of curves of genus 3 over finite fields, *Tôhoku Math J.* **45** (1993), 311–329.
9. Lauter, K.: Ray class field constructions of curves over finite fields with many rational points, In: H. Cohen (ed.), *Algorithmic Number Theory* Lecture Notes in Comput. Sci. 1122, Springer, Berlin, 1996, pp. 187–195.
10. Lauter, K.: A formula for constructing curves over finite fields with many rational points, *J. Number Theory* **74** (1999), 56–72.
11. Lauter, K.: Non-existence of a curve over F_3 of genus 5 with 14 rational points, *Proc. Amer. Math. Soc.* **128** (2000), 369–374.
12. Lauter, K.: Improved upper bounds for the number of rational points on algebraic curves over finite fields, *C.R. Acad. Sci. Paris Sér. I Math.* **328** (1999) p.1181–1185.
13. Lauter, K., with an Appendix by J-P. Serre, Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, *J. Algebraic Geom.* **10**(1) (2001), 19–36.
14. Mumford, D.: *Abelian Varieties*, Tata Inst. Fund. Res. Stud. Math. 5, Oxford Univ. Press, London, 1970.
15. Niederreiter, H. and Xing, C. P.: Cyclotomic function fields, Hilbert class fields and global function fields with many rational places, *Acta Arith.* **79** (1997), 59–76.
16. Niederreiter, H. and Xing, C. P.: Drinfeld modules of rank 1 and algebraic curves with many rational points II, *Acta Arith.* **81** (1997), 81–100.
17. Oort, F. and Ueno, K.: Principally polarized abelian varieties of dimension two or three are Jacobian varieties, *J. Fac. Sci. Univ. Tokyo* **20** (1973), 377–381.
18. Otremba, G.: Zur Theorie der hermiteschen Formen in imaginär-quadratischen Zahlkörpern, *J. Crelle* **249** (1971), 1–19.
19. Ribenboim, P.: *Catalan's Conjecture*, Academic Press, New York, 1994.
20. Schoof, R.: *Algebraic Curves and Coding Theory*, UTM 336, Univ. of Trento, 1990.
21. Serre, J.-P.: Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris Sér. I Math.* **296** (1983), 397–402 (=Oeuvres III, No. 128).
22. Serre, J-P.: *Nombre de points des courbes algébriques sur* $\mathbb{F}_q$, Sém. Théorie Nombres de Bordeaux, 1982/83, exp. no. 22. (= Oeuvres III, No. 129, 664–668).
23. Serre, J-P.: Résumé des cours de 1983–1984 (= Oeuvres III, No. 132, 701–705).
24. Serre, J.-P.: Rational points on curves over finite fields, Notes by F. Gouvea of lectures at Harvard University, 1985.
25. Serre, J.-P.: Letter to K. Lauter, 25 Juin, 1999.

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press

26. Skinner, C.: The Diophantine equation $x^2 = 4q^n - 4q + 1$, *Pacific J. Math.* **139**(2) (1989), 303–309.

27. Stark, H. M.: On the Riemann hypothesis in hyperelliptic function fields, *Proc. Sympos. Pure Math.* **24** (1973), 285–302.

28. Stohr, K. O. and Voloch, J. F.: Weierstrass points and curves over finite fields. *Proc. London Math. Soc.* **52** (1986), 1–19.

29. Waterhouse, W. C.: Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup. sér. 4.* **2** (1969), 521–560.

https://doi.org/10.1023/A:1020246226326 Published online by Cambridge University Press