LMS J. Comput. Math. 13 (2010) 192–207 © 2010 Author
doi:10.1112/S1461157009000576

Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves

Christophe Ritzenthaler

Abstract

Let k be a field of characteristic other than 2. There can be an obstruction to a principally polarized abelian threefold (A, a) over k, which is a Jacobian over $\bar{k}$, being a Jacobian over k; this can be computed in terms of the rationality of the square root of the value of a certain Siegel modular form. We show how to do this explicitly for principally polarized abelian threefolds which are the third power of an elliptic curve with complex multiplication. We use our numerical results to prove or refute the existence of some optimal curves of genus 3.

1. *Introduction*

Let p be a prime and let $q = p^n$ for $n > 0$. For $g \geqslant 0$, it is well known that the maximal number of points of a (smooth, absolutely irreducible, projective) curve of genus g over $\mathbb{F}_q$ is less than or equal to the Serre–Weil bound $q + 1 + gm$ where $m = \lfloor 2\sqrt{q} \rfloor$. However, finding the precise value of this maximum, denoted by $N_q(g)$, is a longstanding problem. It is difficult even to know whether, for given q and g, there is a genus-g curve over $\mathbb{F}_q$ that attains the Serre–Weil bound (such a curve is said to be *optimal*). Closed formulas for any q are known only for $g = 1$ (see [**4, 32**]) and $g = 2$ (see [**30**]). When $g \geqslant 3$, we know $N_q(g)$ only for some q that are square or small (see [**12, 26, 31**] for $g = 3$ and [**6**] or the web page www.manypoints.org for $g \leqslant 50$). Only very recently have infinitely many optimal genus-3 curves been constructed over $\mathbb{F}_{2^n}$ with n non-square (see [**27**]). Still, for $g = 3$, there is a general result due to Lauter [**22**] which says that for any q there exists a genus-3 curve C over $\mathbb{F}_q$ such that

$$|\#C(\mathbb{F}_q) - q - 1| \geqslant 3m - 3. \tag{1.1}$$

Hence there is a curve whose number of points is not more than three away from the Serre–Weil bound or up to three greater than the minimum number of points $q + 1 - 3m$. This ambiguity, which prevents one from getting a quasi-optimal result, is actually a consequence of a general theorem derived from a precise form of Torelli's theorem; here we state a version of it due to Serre.

Theorem 1.1 [**21**, Appendix]. *Let (A, a) be a principally polarized abelian variety of dimension $g \geqslant 1$ over a field k. Assume that (A, a) is isomorphic over $\bar{k}$ to the Jacobian of a curve C_0 of genus g defined over $\bar{k}$. Then one of the following holds.*

(i) *If C_0 is hyperelliptic, there is a unique curve C/k isomorphic to C_0 over $\bar{k}$ such that (A, a) is k-isomorphic to $(\mathrm{Jac}(C), j)$ where j is the canonical polarization on $\mathrm{Jac}(C)$.*

(ii) *If C_0 is not hyperelliptic, there is a unique curve C/k isomorphic to C_0 over $\bar{k}$ and a unique quadratic character*

$$\epsilon : \mathrm{Gal}(k^{\mathrm{sep}}/k) \longrightarrow \{\pm 1\}$$

such that the twisted abelian variety $(A, a)_\epsilon$ is k-isomorphic to $(\mathrm{Jac}(C), j)$.

Received 21 December 2009.

2000 Mathematics Subject Classification 11G20 (primary), 14H45, 14H40 (secondary).

This work was partially supported by grant MTM2006-11391 from the Spanish MEC and grant ANR-09-BLAN-0020-01 from the French ANR.

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

Let us explain how this applies to the context of curves with many points over $k = \mathbb{F}_q$. In order to prove the existence of a curve with a certain number of points N, one strategy is to construct an abelian variety over k whose Frobenius endomorphism has trace $1 + q - N$ and then prove that this abelian variety is actually a Jacobian. When $g < 4$, this method is geometrically tractable because every abelian variety with an (indecomposable) polarization is isomorphic over $\bar{k}$ to a Jacobian (see [11, 28] and Theorem 3.3). Any genus-2 curve is hyperelliptic, so there is no obstruction and one is able to describe exactly which isogeny classes of abelian surfaces over k contain a Jacobian (see [10]). However, as Theorem 1.1 shows, as soon as $g = 3$, curves can be non-hyperelliptic and there may exist an obstruction to an abelian variety being a Jacobian over k. Moreover, if it is the quadratic twist that is a Jacobian, then the corresponding trace is $-(1 + q - N)$, which explains the absolute value in (1.1).

Serre not only pointed out this obstruction but also suggested a strategy for computing it when $g = 3$ and k is a field of characteristic other than 2 (see [18, Letter to Top]). Roughly speaking, an absolutely indecomposable principally polarized abelian threefold (A, a) over k is a Jacobian if the value of a certain Siegel modular form χ_{18} at the 'moduli point' (A, a) with respect to a rational basis of regular differentials is a square in k. This assertion was motivated by a formula of Klein [17] that relates χ_{18} to the square of the discriminant of plane quartics, which more or less gives the 'only if' part of the claim. In [19], Serre's assertion was proved for the case where k is a number field.

In the present article, we go back to the initial motivation of Serre's letter, that is, the problem of existence of optimal curves of genus 3. In § 2, we show that the ideas developed in [19] can be applied over finite fields as well (Proposition 2.4). For a different approach, see [23]. However, it is not known how to directly compute this value over finite fields. Therefore, as Serre suggested, we shall lift (A, a) over a number field and then use the analytic expression of χ_{18} in terms of Thetanullwerte. If the computation is done with enough precision, we can recognize this value as an algebraic number. Finally, we reduce it to the initial finite field to obtain the obstruction (see Proposition 2.5 for a more precise formulation).

As the Jacobian of an optimal curve is isogenous to the power of an elliptic curve E, we make this procedure explicit in the particular case where $A = E^3$. Let a_0 be the product principal polarization on E^3 and let $M = a_0^{-1} a \in M_3(\mathrm{End}(E))$. When $\mathrm{End}(E)$ is an order in an imaginary quadratic field, it is well known that M is the matrix of a principal polarization on E^3 if and only if M is a positive definite hermitian matrix with determinant 1 (Proposition 3.2). In § 3, where E is defined over a number field, we show how to translate the data $(E^3, a_0 M)$ into a period matrix of the corresponding torus in order to compute the analytic expression for χ_{18}.

For certain orders, the set of such matrices M (up to isomorphisms) has been explicitly computed; see [29]. This enables us to give in § 4 tables of values of χ_{18} on E^3 for certain CM elliptic curves E with class number 1. As an application, we show in Corollary 4.2 that there is an optimal genus-3 curve over $\mathbb{F}_q$ for $q = 47, 61, 137$ or 277 but not for $q = 311$. Note that for $q = 47$ and $q = 61$ this result was already obtained in [31] by means of explicit models. Using recent results of Guàrdia and our data, we give 'universal models' for Top's curves.

Besides showing how Serre's strategy works, the purpose of this article is to present data to support future conjectures on the primes dividing χ_{18} and their exponent. Indeed, while analytic computations can work out the value of $N_q(3)$ case by case, obtaining a general formula for $N_q(3)$ will require a deep understanding of χ_{18}. In a forthcoming article, we will relate the divisibility of χ_{18} by a prime to the type (singular, decomposable or hyperelliptic) of the reduction of (A, a) at this prime.

Conventions and notation. If A and B are varieties over a field k, when we speak of a morphism from A to B we will always mean a morphism *defined over* k. So, for instance, $\mathrm{End}(A)$ is the ring of endomorphisms defined over k, and $A \sim B$ means that A is isogenous to B over k. If (A, a) and (B, b) are polarized abelian varieties, then by an isomorphism between them we shall always mean an isomorphism as polarized abelian varieties.

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

2. *Serre's obstruction over finite fields*

2.1. *Reduction properties*

In this section we shall recall some notation and results from [14] and [19]. Let $g \geqslant 2$ be an integer. Let $\mathsf{M}_g := \mathsf{M}_{g,1}$ be the moduli stack of smooth and proper curves of genus g, and let $\mathsf{A}_g := \mathsf{A}_{g,1}$ be the moduli stack of principally polarized abelian schemes of relative dimension g. Let $\pi : \mathsf{C}_g \to \mathsf{M}_g$ be the universal curve and $\boldsymbol{\lambda} = \bigwedge^g \pi_* \Omega^1_{\mathsf{C}_g/\mathsf{M}_g}$ the Hodge bundle on M_g. Similarly, let $\pi : \mathsf{V}_g \to \mathsf{A}_g$ be the universal abelian scheme and $\boldsymbol{\omega} = \bigwedge^g \pi_* \Omega^1_{\mathsf{V}_g/\mathsf{A}_g}$ the Hodge bundle on A_g.

For any $h \geqslant 0$ and any $\mathbb{Z}$-algebra R, we write

$$T_{g,h}(R) = \Gamma(\mathsf{M}_g \otimes R, \boldsymbol{\lambda}^{\otimes h})$$

for the R-module of *Teichmüller modular forms* and

$$\mathbf{S}_{g,h}(R) = \Gamma(\mathsf{A}_g \otimes R, \boldsymbol{\omega}^{\otimes h})$$

for the R-module of *geometric Siegel modular forms.*

If one has $C \in \mathsf{M}_g \otimes R$ and $f \in \mathbf{T}_{g,h}(R)$, then for any basis of regular differentials $\omega_1, \ldots, \omega_g$ of $\Omega^1[C] \otimes R$ we can define an element

$$f(C, \lambda) = f(C)/\lambda^{\otimes h} \in R$$

where $\lambda = \omega_1 \wedge \ldots \wedge \omega_g \in \boldsymbol{\lambda} \otimes R$. Analogously, if one has $(A, a) \in \mathsf{A}_g \otimes R$ and $f \in \mathbf{S}_{g,h}(R)$, then for any basis of regular differentials $\omega_1, \ldots, \omega_g$ of $\Omega^1[A] \otimes R$ we can define an element

$$f((A, a), \omega) = f(A, a)/\omega^{\otimes h} \in R$$

where $\omega = \omega_1 \wedge \ldots \wedge \omega_g \in \boldsymbol{\omega} \otimes R$.

Lemma 2.1 [5, p. 138 (i)]. *The association*

$$C \mapsto f(C, \omega)$$

is compatible with arbitrary pull-backs and isomorphisms, and so is the association

$$(A, a) \mapsto f((A, a), \omega)$$

We now assume that $R = k \subset \mathbb{C}$ is a number field. As usual, let us write

$$\mathbb{H}_g = \{\tau \in \mathsf{GL}_g(\mathbb{C}) : \tau \text{ is symmetric and } \operatorname{Im}(\tau) > 0\}$$

and let $\widetilde{f}$ belong to the usual vector space $\mathbf{R}_{g,h}(\mathbb{C})$ of *analytic Siegel modular forms* of weight h on $\mathbb{H}_g$, which consists of complex holomorphic functions $\phi(\tau)$ on $\mathbb{H}_g$ satisfying

$$\phi(M.\tau) = \det(\gamma\tau + \delta)^h \phi(\tau)$$

for any $M = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$ in the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$. Let (A, a) be a principally polarized abelian variety of dimension g defined over k. Let $\omega_1, \ldots, \omega_g$ be a basis of $\Omega^1[A] \otimes k$ and let $\omega = \omega_1 \wedge \ldots \wedge \omega_g \in \boldsymbol{\omega}[A] \otimes k$. Let $\gamma_1, \ldots \gamma_{2g}$ be a symplectic basis for the polarization a. We say that the matrix

$$\Omega_a = \begin{pmatrix} \int_{\gamma_1} \omega_1 & \ldots & \int_{\gamma_{2g}} \omega_1 \\ \vdots & & \vdots \\ \int_{\gamma_1} \omega_g & \ldots & \int_{\gamma_{2g}} \omega_g \end{pmatrix}$$

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

is a *period matrix associated to* a. If we write $\Omega_a = [\Omega_1, \Omega_2]$ with $\Omega_i \in M_g(\mathbb{C})$, then the Riemann conditions [2, p. 75] imply that $\tau_a = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_g$. We call τ_a a *Riemann matrix associated to* a.

PROPOSITION 2.2 [19, Proposition 1.1.2]. *With the previous notation, we have*

$$f(A, a) = (2i\pi)^{gh} \frac{\widetilde{f}(\tau_a)}{\det \Omega_2^h} \omega^{\otimes h} \in \mathbf{S}_{g,h}(\mathbb{C}).$$

Moreover, the map $\widetilde{f} \mapsto f$ *from* $\mathbf{R}_{g,h}(\mathbb{C})$ *to* $\mathbf{S}_{g,h}(\mathbb{C})$ *is an isomorphism.*

Let S be the localization of the ring of integers $\mathcal{O}_k$ of k at a prime $\mathfrak{p}$ over a prime $p \neq 2$, and let $F = S/\mathfrak{p}$ be the finite residue field. Assume that the principally polarized abelian variety (A, a) over k has a model over S with good reduction at $\mathfrak{p}$. We denote this model by $(\tilde{A}, \tilde{a})$. Let $\omega_1, \ldots, \omega_g$ be a basis of regular differentials of $\Omega^1[\tilde{A}] \otimes S$ and let $\omega = \omega_1 \wedge \ldots \wedge \omega_g$. Then, by Lemma 2.1, for $f \in \mathbf{S}_{g,h}(S)$ we have

$$f((\tilde{A}, \tilde{a}) \otimes F, \omega \otimes F) = f((A, a), \omega \otimes k) \pmod{\mathfrak{p}}.$$

Hence, using Lemma 2.1 and Proposition 2.2, we get the following proposition.

PROPOSITION 2.3.

$$f((\tilde{A}, \tilde{a}) \otimes F, \omega \otimes F) = (2i\pi)^{gh} \frac{\widetilde{f}(\tau_a)}{\det \Omega_2^h} \pmod{\mathfrak{p}}.$$

2.2. *The modular form* χ_h

Following [2], we recall the definition of theta functions with (entire) characteristics

$$[\boldsymbol{\varepsilon}] = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} \in \mathbb{Z}^g \oplus \mathbb{Z}^g.$$

The *(classical) theta function* is given, for $\tau \in \mathbb{H}_g$ and $z \in \mathbb{C}^g$, by

$$\theta \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} (z, \tau) = \sum_{n \in \mathbb{Z}^g} \exp(i\pi(n + \varepsilon_1/2)\tau^t(n + \varepsilon_1/2) + 2i\pi(n + \varepsilon_1/2)^t(z + \varepsilon_2/2)).$$

The *Thetanullwerte* are the values at $z = 0$ of these functions. Recall that a characteristic is *even* if $\varepsilon_1{}^t\varepsilon_2 \equiv 0 \pmod 2$ and *odd* otherwise. For $g \geqslant 2$, we put $h = 2^{g-2}(2^g + 1)$ and

$$\widetilde{\chi}_h(\tau) = \frac{(-1)^{gh/2}}{2^{2^{g-1}(2^g-1)}} \cdot \prod_{\boldsymbol{\varepsilon}} \theta \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} (0, \tau),$$

where $\boldsymbol{\varepsilon}$ runs over the even characteristics with coefficients in $\{0, 1\}$.

In [16] Igusa proved that if $g \geqslant 3$, then $\widetilde{\chi}_h(\tau) \in \mathbf{R}_{g,h}(\mathbb{C})$. Starting from the analytic Siegel modular form $\widetilde{\chi}_h$, by Proposition 2.2 we can define a geometric Siegel modular form

$$\chi_h(A, a) = (2i\pi)^{gh} \cdot \frac{\widetilde{\chi}_h(\tau_a)}{\det(\Omega_2)^h} (\omega_1 \wedge \ldots \wedge \omega_g)^{\otimes h} \in \mathbf{S}_{g,h}(\mathbb{C}).$$

Ichikawa proved in [14, Proposition 3.4] that, since χ_h has rational integral Fourier coefficients, χ_h is actually defined over $\mathbb{Z}$; that is, $\chi_h \in \mathbf{S}_{g,h}(\mathbb{Z})$. He also showed that χ_h is *primitive*; that is, its reduction modulo any prime is non-zero.

2.3. *The case* $g = 3$

We now specialize to the $g = 3$ case, that is,

$$\chi_{18}(A, a) = \frac{(2\pi)^{54}}{2^{28}} \cdot \frac{\prod_{\boldsymbol{\varepsilon}} \theta[\boldsymbol{\varepsilon}](0, \tau_a)}{\det(\Omega_2)^{18}} (\omega_1 \wedge \omega_2 \wedge \omega_3)^{\otimes 18} \in \mathbf{S}_{3,18}(\mathbb{Z}). \tag{2.1}$$

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

In [15] Ichikawa proved that there exists a Teichmüller modular form $\mu_{3,9}\in\mathbf{T}_{3,9}(\mathbb{Z})$ of weight 9 such that if $t:\mathsf{M}_3\to\mathsf{A}_3$ is the Torelli map, then

$$t^*(\chi_{18})=(\mu_{3,9})^2. \tag{2.2}$$

Using this equality, we can adapt the proof of [19, Theorem 1.3.3] to the case of finite fields.

Proposition 2.4. *Let (A,a) be a principally polarized abelian threefold defined over a finite field F of characteristic other than 2. Let $\{\omega_1,\omega_2,\omega_3\}$ be a basis for $\Omega^1[A]\otimes F$ and let $\omega=\omega_1\wedge\omega_2\wedge\omega_3$. Then (A,a) is isomorphic to the Jacobian of a non-hyperelliptic genus-3 curve if and only if $\chi_{18}((A,a),\omega)$ is a non-zero square in F. Moreover, if $\chi_{18}((A,a),\omega)$ is a non-square in F, then (A,a) is not a Jacobian.*

Proof. If (A,a) is isomorphic over F to the Jacobian of a non-hyperelliptic genus-3 curve C/F, then by using (2.2) we get

$$\chi_{18}((A,a),\omega)=t^*(\chi_{18})(C,\lambda)=\mu_{3,9}^2(C,\lambda)$$

with $\lambda=\theta^*\omega$. So $\chi_{18}((A,a),\omega)$ is a square. Moreover, it is non-zero; indeed, by the definition of $\mu_{3,9}$ (see [13, p. 1059]), this form is zero precisely on the hyperelliptic locus. Now, assume that $\chi:=\chi_{18}((A,a),\omega)$ is a non-zero square. By [16, Lemmas 10 and 11] we know that the modular form χ_{18} is zero on $(\mathsf{A}_3\backslash t(\mathsf{M}_3))\otimes\mathbb{C}$, hence this is true also on the schematic closure and therefore over finite fields. From this we deduce that $(A,a)\in t(\mathsf{M}_3\otimes\bar{F})$ and, since $\chi\neq 0$, we even know that (A,a) is geometrically the Jacobian of a non-hyperelliptic genus-3 curve. By Theorem 1.1, we know that either (A,a) is a Jacobian or its quadratic twist (A',a') is (and exactly one of these alternatives holds). Suppose that (A,a) is not a Jacobian. Let $\{\omega_1',\omega_2',\omega_3'\}$ be a basis for $\Omega^1[A']\otimes F$ and set $\omega'=\omega_1'\wedge\omega_2'\wedge\omega_3'$. From what we have just proved, $\chi_{18}((A',a'),\omega')$ is a non-zero square in F. Then, from [19, Corollary 1.2.3] we know that there exists a non-square $c\in F$ such that

$$\chi_{18}((A,a),\omega)=c^9\cdot\chi_{18}((A',a'),\omega').$$

Hence χ is not a square and we get a contradiction. □

This proposition alone is, however, useless for applications, because so far we have no way of directly computing $\chi_{18}((A,a),\omega)$. This is why we employ Serre's initial idea of lifting a principally polarized abelian threefold over a local field of characteristic 0, using the analytic expression (2.1) and then reducing the result to get the obstruction by Propositions 2.3 and 2.4. Note that we can always lift a principally polarized abelian threefold. Indeed, from Theorem 3.3 we see that, up to a possible quadratic twist, any principally polarized abelian threefold (A,a) over a finite field F is a product of Jacobians $(\mathrm{Jac}(C_i),j_i)$. It thus suffices to lift each of the curves C_i to the curve $\tilde{C}_i$ and consider the principally polarized abelian threefold $\prod(\mathrm{Jac}(\tilde{C}_i),\tilde{j}_i)$. If necessary, we apply a quadratic twist to get a lift of (A,a). Let us summarize the procedure.

Proposition 2.5. *Let (A,a) be a principally polarized abelian threefold over a finite field F of characteristic other than 2, and let $(\tilde{A},\tilde{a})$ be a lift of (A,a) defined over a local ring S of a number field k with residue field F. Then, for any choice of a basis of regular differentials $\omega_1,\omega_2,\omega_3\in\Omega^1[\tilde{A}]\otimes S$,*

$$\chi:=\chi_{18}((\tilde{A},\tilde{a}),\omega_1\wedge\omega_2\wedge\omega_3)=\frac{(2\pi)^{54}}{2^{28}}\cdot\frac{\prod_{\varepsilon}\theta[\varepsilon](0,\tau_{\tilde{a}})}{\det(\Omega_2)^{18}}$$

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

belongs to S. Let $\mathfrak{p}$ be such that $F = S/\mathfrak{p}$. Then (A, a) is the Jacobian of a non-hyperelliptic genus-3 curve if and only if $\chi \pmod{\mathfrak{p}}$ is a non-zero square in F. Moreover, if $\chi \pmod{\mathfrak{p}}$ is a non-square in F, then (A, a) is not a Jacobian.

3. *Polarizations on powers of elliptic curves*

3.1. *Polarization and hermitian forms*

Let (A, a_0) be a principally polarized abelian variety of dimension $g > 0$ over a field k. There exists an ample line bundle $\mathcal{L}_0 \in \mathrm{Pic}_{\bar{k}}(A)$ such that $a_0 = \phi_{\mathcal{L}_0} : A \to \hat{A}$. Let $\mathrm{NS}(A)$ be the Néron–Severi group of A. The map $\mathcal{L} \mapsto \phi_{\mathcal{L}}$ from $\mathrm{NS}_{\bar{k}}(A)$ to $\mathrm{Hom}_{\bar{k}}(A, \hat{A})$ is injective. If we compose this map with $\phi_{\mathcal{L}_0}^{-1}$, we obtain an injection $\mathrm{NS}_{\bar{k}}(A) \hookrightarrow \mathrm{End}_{\bar{k}}(A)$.

Proposition 3.1 [**24**, p. 137]. *Let (A, a_0) be a principally polarized abelian variety over a field k with all endomorphisms defined over k. Let $\dagger$ be the Rosati involution induced by a_0 (that is, $b \in \mathrm{End}(A) \mapsto a_0^{-1} \circ \hat{b} \circ a_0 \in \mathrm{End}(A)$). Let $\mathrm{End}(A)^s$ be the sub-ring of endomorphisms that are stable by the Rosati involution $\dagger$. Then the map*

$$\mathcal{L} \mapsto a_0^{-1} \circ \phi_{\mathcal{L}}$$

is a group isomorphism from $\mathrm{NS}_{\bar{k}}(A)$ to $\mathrm{End}_{\bar{k}}(A)^s$.

In particular, we see that if $\mathrm{End}(A) = \mathrm{End}_{\bar{k}}(A)$, then $\mathrm{NS}_{\bar{k}}(A) = \mathrm{NS}(A)$. In what follows we assume that all endomorphisms of A are defined over k.

To describe the polarizations on A, it is therefore enough to understand the image of the ample line bundles by the previous map. According to [**25**, p. 209], this image corresponds to totally positive elements of the formally real Jordan algebra $\mathrm{NS}(A) \otimes \mathbb{R} \simeq \mathrm{End}(A)^s \otimes \mathbb{R}$.

With our applications in mind, we make this characterization more explicit in the following special situation. We restrict ourselves to the case of $A = E^g$, where $E : y^2 + a_1xy + a_3y = f(x)$ with $a_1, a_3 \in k$ and $f \in k[x]$ is an elliptic curve with all endomorphisms defined over k. We assume that $\mathrm{End}(E)$ is an order $\mathcal{O}$ in the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K, and we identify it with such an $\mathcal{O} \subset \mathcal{O}_K \subset \mathbb{C}$ via its action on the regular differential $\omega_E = dx/(2y + a_1x + a_3)$. Let a_E be the principal polarization on E and $a_0 = (a_E \times \ldots \times a_E) : A \to \hat{A}$ the product principal polarization on A. We denote by $\bar{\ }$ the Rosati involution on $\mathrm{End}(E)$ associated to a_E; it is equivalent to complex conjugation of K through the identification of $\mathrm{End}(E)$ with $\mathcal{O}$. In the same way, by identifying $\mathrm{End}(A)$ with $\mathsf{M}_g(\mathcal{O})$, we see that the Rosati involution $\dagger$ associated to a_0 is $M \mapsto {}^t\bar{M}$. We say that $M \in \mathsf{M}_g(\mathcal{O})$ is *hermitian* if $M = {}^t\bar{M}$, that is, $M \in \mathrm{End}(A)^s$.

Proposition 3.2 [**25**, p. 209]. *The morphism $M \mapsto a_0M : \mathsf{M}_g(\mathcal{O}) \to \mathrm{NS}(A)$ restricts to a bijection between positive definite hermitian matrices of determinant 1 and principal polarizations on A.*

Remark 1. Similar results were used in [**20**] to study the number of principal polarizations on products of elliptic curves over $\mathbb{C}$ without complex multiplication.

3.2. *Indecomposable polarizations*

Recall that for any abelian variety A, a polarization a on A is said to be *decomposable* if there exist two polarized abelian varieties (A_1, a_1) and (A_2, a_2) together with an isomorphism $\psi : A \to A_1 \times A_2$ such that $a = \hat{\psi} \circ (a_1 \times a_2) \circ \psi$. One says that A is *absolutely indecomposable* if it is not decomposable over $\bar{k}$.

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

When $g \leqslant 3$, an indecomposable principal polarization is a necessary and sufficient condition for being geometrically a Jacobian.

THEOREM 3.3 [**11, 28**]. *Let (A, a) be a principally polarized abelian variety of dimension $g \leqslant 3$ over an algebraically closed field k. Then (A, a) is a Jacobian if and only if a is indecomposable.*

With the notation and assumptions of § 3.1, we can give a partial characterization of indecomposability in terms of the matrix M over an arbitrary field k.

PROPOSITION 3.4. *Let $A = E^g$ as before, let a be a principal polarization on A and let $M = a_0^{-1} a \in \mathsf{M}_g(\mathcal{O})$. If the polarization a is absolutely indecomposable, then M is indecomposable, that is, there do not exist a matrix $P \in \mathsf{GL}_g(\mathcal{O})$ and two square matrices $M_i \in \mathsf{GL}_{g_i}(\mathcal{O})$ with $g_1 + g_2 = g$ such that*

$$M = {}^t\bar{P} \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} P. \tag{3.1}$$

Proof. Let us assume that such P, M_1 and M_2 do exist and take ψ to be the automorphism of E^g associated to P. Let $a_i = a_{0|E^{g_i}} M_i : E^{g_i} \mapsto \hat{E}^{g_i}$. As ${}^t\bar{P} = \psi^\dagger = a_0^{-1}\hat{\psi} a_0$, relation (3.1) becomes

$$M = a_0^{-1} a = a_0^{-1} \hat{\psi}(a_1 \times a_2)\psi,$$

so $a = \hat{\psi} \circ (a_1 \times a_2) \circ \psi$. Since M is the matrix of a principal polarization, Proposition 3.2 tells us that the M_i are, too, and so the a_i are principal polarizations on $A_i = E^{g_i}$. Thus we see that a is decomposable. □

When k is a finite field, Serre gave in [**22**, Appendix] a beautiful description of abelian varieties and their polarizations in the case where A is only *isogenous* to E^g and E is an ordinary elliptic curve for which $\mathcal{O}_K = \mathcal{O} \simeq \operatorname{End}(E) = \mathbb{Z}[\pi]$, with π being the Frobenius endomorphism of E over k. If we write $L = \operatorname{Hom}(E, A)$ and $L^* = \operatorname{Hom}_{\bar{\mathcal{O}}_K}(L, \mathcal{O}_K)$, a polarization a on A induces a sesquilinear form $h : L \to L^*$,

$$\begin{array}{rcccccc} h: & L = \operatorname{Hom}(E, A) & \to & \operatorname{Hom}(E, \hat{A}) & \to & L^* \\ & f & \mapsto & af & \mapsto & (g \mapsto a_E^{-1} \hat{g} a f), \end{array}$$

whose associated bilinear form is a positive definite hermitian form $L \times L \to \mathcal{O}_K$. Its relation with Proposition 3.2 in the case where $A = E^g$ is the following. If $M = a_0^{-1} a \in \operatorname{End}(A)$ is the matrix of a polarization given by Proposition 3.2, then we can define

$$\begin{array}{rcccccccc} h: & L = \operatorname{Hom}(E, A) & \to & L = \operatorname{Hom}(E, A) & \to & \operatorname{Hom}(E, \hat{A}) & \to & L^* \\ & f & \mapsto & Mf & \mapsto & a_0 M f & \mapsto & (g \mapsto a_E^{-1} \hat{g} a_0 M f). \end{array}$$

Now, if we identify L with $\mathcal{O}_K^g$, we can write

$$(a_E^{-1} \hat{g} a_0) M f = {}^t\bar{g} M f.$$

Thus, in this basis, the matrix of the bilinear form associated to h is exactly M. So, in the case where $A = E^g$ over a finite field, we can conflate the two points of view and use the following results.

PROPOSITION 3.5 [**22**, Appendix]. *Assume that $\mathcal{O}_K$ is principal. If A is isogenous to E^g, then A is actually isomorphic to E^g.*

PROPOSITION 3.6 [**22**, Appendix]. *Assume that $\mathcal{O}_K$ is principal. With the notation of Proposition 3.4, a is absolutely indecomposable if and only if M is indecomposable.*

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

3.3. *The case of $A = E^g$ over $\mathbb{C}$*

Let $k \subset \mathbb{C}$. As in § 3.1, we suppose that $E : y^2 + a_1xy + a_3y = f(x)$ with $a_1, a_3 \in k$ and $f \in k[x]$ is an elliptic curve with all endomorphisms defined over k and that $\mathrm{End}(E)$ is an order $\mathcal{O}$ in the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K.

Let us choose a basis $\{\delta_1, \delta_2\}$ for $H_1(E, \mathbb{Z})$ such that the periods $w_i = \int_{\delta_i} dx/(2y + a_1x + a_3)$ satisfy $\tau = w_1/w_2 \in \mathbb{H}_1$. Let $\Omega_E = [w_1, w_2]$ and let $a_E = \phi_{\mathcal{L}_E}$ be the principal polarization on E. We denote by I_g the identity matrix of $\mathbb{C}^g$ and let

$$J_{2g} = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Since a_E is given by the intersection product $T = J_2$, by [2, Lemma 4.2.3] its first Chern class is the hermitian form

$$H_E := c_1(\mathcal{L}_E) = 2i(\bar{\Omega}_E T^{-1}\,{}^t\Omega_E) = \frac{1}{\mathrm{Im}(\omega_1\bar{\omega}_2)} I_1.$$

Now let $A = E^g = \mathbb{C}^g/\Omega_0\mathbb{Z}^{2g}$, where

$$\Omega_0 = \begin{pmatrix} w_1 & & & w_2 & & \\ & \ddots & & & \ddots & \\ & & w_1 & & & w_2 \end{pmatrix}.$$

Let $a_0 = a_E^g = \phi_{\mathcal{L}_0}$ be the product polarization on A. An easy computation shows that

$$H_0 = c_1(\mathcal{L}_0) = \frac{1}{\mathrm{Im}(w_1\bar{w}_2)} I_g.$$

We now consider $M \in \mathsf{M}_g(\mathcal{O})$ defining a principal polarization $a = a_0M = \phi_{\mathcal{L}}$ on A. By [2, Lemma 2.4.5],

$$H := c_1(\mathcal{L}) = {}^tMH_0 = \frac{1}{\mathrm{Im}(w_1\bar{w}_2)}\,{}^tM.$$

The imaginary part of H is an alternating form with integral values on the lattice $\Lambda = \Omega_0\mathbb{Z}^{2g}$. Its matrix in the chosen basis of Λ is

$$T = \mathrm{Im}({}^t\Omega_0 H\bar{\Omega}_0) = \mathrm{Im}\begin{pmatrix} w_1H\bar{w}_1 & w_1H\bar{w}_2 \\ w_2H\bar{w}_1 & w_2H\bar{w}_2 \end{pmatrix}.$$

We can make this computation a bit more explicit. In the case where H has real coefficients, we very easily find that

$$T = \begin{pmatrix} 0 & M \\ -M & 0 \end{pmatrix}.$$

Otherwise, using the fact that ${}^tM = \bar{M}$, we obtain

$$\begin{aligned} T &= \begin{pmatrix} |w_1|^2 \,\mathrm{Im}\, H & \mathrm{Re}(w_1\bar{w}_2)\,\mathrm{Im}\, H + \mathrm{Im}(w_1\bar{w}_2)\,\mathrm{Re}\, H \\ \mathrm{Re}(w_1\bar{w}_2)\,\mathrm{Im}\, H - \mathrm{Im}(w_1\bar{w}_2)\,\mathrm{Re}\, H & |w_2|^2\,\mathrm{Im}\, H \end{pmatrix} \\ &= \begin{pmatrix} \dfrac{-\mathrm{Im}\,{}^tM}{\mathrm{Im}\, 1/\tau} & \dfrac{\mathrm{Re}\,\tau}{\mathrm{Im}\,\tau}\,\mathrm{Im}\,{}^tM + \mathrm{Re}\,{}^tM \\ \dfrac{\mathrm{Re}\,\tau}{\mathrm{Im}\,\tau}\,\mathrm{Im}\,{}^tM - \mathrm{Re}\,{}^tM & \dfrac{\mathrm{Im}\,{}^tM}{\mathrm{Im}\,\tau} \end{pmatrix} \\ &= \begin{pmatrix} \dfrac{\mathrm{Im}\, M}{\mathrm{Im}\, 1/\tau} & \mathrm{Re}\, M - \dfrac{\mathrm{Re}\,\tau}{\mathrm{Im}\,\tau}\,\mathrm{Im}\, M \\ -{}^t\left(\mathrm{Re}\, M - \dfrac{\mathrm{Re}\,\tau}{\mathrm{Im}\,\tau}\,\mathrm{Im}\, M\right) & -\dfrac{\mathrm{Im}\, M}{\mathrm{Im}\,\tau} \end{pmatrix}. \end{aligned} \tag{3.2}$$

As T is a non-degenerate alternating form associated to the principal polarization a, there is a matrix $B \in \mathsf{M}_{2g}(\mathbb{Z})$ such that $BT{}^tB = J_{2g}$. The matrix B is defined up to the action of the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$. The columns of ${}^tB\mathbb{Z}^{2g}$ form a symplectic basis for the polarization a. Hence $\Omega_a = \Omega_0{}^tB$ is a period matrix associated to a and, if we write $\Omega_a = [\Omega_1, \Omega_2]$ with $\Omega_i \in M_g(\mathbb{C})$, $\tau_a = \Omega_2^{-1}\Omega_1$ is a Riemann matrix associated to a.

Note that if $\Omega_0 = [Z_1, Z_2]$ with Z_2 invertible and if, as usual, we write $B = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$ and $\tau_0 = Z_2^{-1}Z_1$, then $\tau_a = B.\tau_0 := (\alpha\tau_0 + \beta)(\gamma\tau_0 + \delta)^{-1}$.

4. *Explicit computations of χ_{18} and optimal curves*

We recall the hypotheses of §§ 3.1 and 3.3. Let k be a number field and let

$$E : y^2 + a_1xy + a_3y = f(x) \quad \text{with } a_1, a_3 \in k \text{ and } f \in k[x]$$

be an elliptic curve with CM by an order $\mathcal{O}$ contained in the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ where $d > 0$ is square-free. We assume that all endomorphisms of E are defined over k. Let $\omega_E = dx/(2y + a_1x + a_3)$ be a regular differential on E. Proposition 3.4 shows that $A = E^3$ can be a Jacobian over $\mathbb{C}$ if there exists an indecomposable positive definite hermitian form $M \in \mathsf{M}_3(\mathcal{O})$ of determinant 1. For such an M, we want to compute

$$\chi := \chi_{18}((A, a_0M), \omega_0)$$

where

$$\omega_0 = p_1^*(\omega_E) \wedge p_2^*(\omega_E) \wedge p_3^*(\omega_E),$$

with $p_i : E^3 \to E$ denoting the ith projection.

We will give examples in the case where $\mathcal{O}$ is equal to $\mathcal{O}_K$ and is principal. This gives the possibilities $d = 3, 4, 7, 8, 11, 19, 43, 67$ or 163. By [9, p. 418], there is no form M as above if $d = 3, 4, 8$ or 11. Thus we restrict ourselves to the cases which are left.

4.1. *Choice of the models for E*

First, let us make an elementary remark. If $u : E \to E'$ is an isomorphism such that $u^*\omega_{E'} = \alpha\omega_E$, then

$$\chi_{18}((E'^3, a'), \omega_0') = \alpha^{54}\chi_{18}((E^3, u^*a), \omega_0) \quad \text{with } \omega_0' = p_1^*(\omega_{E'}) \wedge p_2^*(\omega_{E'}) \wedge p_3^*(\omega_{E'}).$$

Hence we need to fix a precise model for our computations and choose it carefully so as to have 'small' results.

We denote by $E(d)$ the elliptic curve with CM by the maximal order of $\mathbb{Q}(\sqrt{-d})$ with minimal conductor, which is d^2 (see [7, p. 21]), and take $E = E(d)$. We recall the equations from [7, pp. 82–84] in Table 1.

TABLE 1. *The models $E(d)$ of Gross* [7].

d	Model	Discriminant
7	$y^2 + xy = x^3 - x^2 - 2x - 1$	-7^3
19	$y^2 + y = x^3 - 2 \cdot 19x + \dfrac{19^2 - 1}{4}$	-19^3
43	$y^2 + y = x^3 - 2^2 \cdot 5 \cdot 43x + \dfrac{3 \cdot 7 \cdot 43^2 - 1}{4}$	-43^3
67	$y^2 + y = x^3 - 2 \cdot 5 \cdot 11 \cdot 67x + \dfrac{7 \cdot 31 \cdot 67^2 - 1}{4}$	-67^3
163	$y^2 + y = x^3 - 2^2 \cdot 5 \cdot 23 \cdot 29 \cdot 163x + \dfrac{7 \cdot 11 \cdot 19 \cdot 127 \cdot 163^2 - 1}{4}$	-163^3

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

We use these models for two reasons. One is that, with a view to applying our results to optimal curves, we need a nice formula for the trace of E. As we can see from Lemma 4.1, the curves $E(d)$ have the simplest expression among all their twists. Another, more important, reason is that for such a choice we expect the value of χ to be in $\mathcal{O}_K$ and 'minimal'. Indeed, since only d divides the discriminant of $E(d)$, $E(d)$ is actually an abelian scheme over $\mathbb{Z}[1/d]$, so the value of χ is in $\mathcal{O}_K[1/d]$. In a forthcoming article we will show that, by using a good arithmetic compactification $\bar{\mathsf{A}}_3$ of A_3, we can consider $E(d)$ as a semi-abelian scheme so that it defines a point of $\bar{\mathsf{A}}_3 \otimes \mathbb{Z}$. Hence, intuitively, the value of χ is actually in $\mathcal{O}_K$. In the same way, we conjecture that χ_{18} can be extended as zero on the border of the compactification; so if a prime divides the discriminant of E, we conjecture that this prime also appears in χ (and this is always the case in our examples). By choosing $E(d)$, which has minimal conductor, we hope for a 'minimal result'.

Lemma 4.1 [7, p. 32]. *Let $d = 7, 19, 43, 67$ or 163. Let $E(d)$ be the elliptic curve given in Table 1. The trace of Frobenius π of $E(d) \otimes \mathbb{F}_p$, where p is a prime different from d, is:*

- 0 *if* $(p/d) = -1$;
- a_p *if* $(p/d) = 1$, *where a_p is the unique integer such that*

$$4p = a_p^2 + db_p^2, \quad \left(\frac{2a_p}{d}\right) = 1.$$

4.2. *Details of the computations in the case where $d = 7$*

Let δ_1 and δ_2 be generators of $H_1(E(7) \otimes \mathbb{C}, \mathbb{Z})$. We can choose these generators so that the periods $[w_1, w_2] = [\int_{\delta_1} dx/(2y + x), \int_{\delta_2} dx/(2y + x)]$ satisfy $w_1/w_2 \in \mathbb{H}_1$ (here we have chosen $w_1/w_2 = \tau := (1 + i\sqrt{7})/2$). According to the data in [29],

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & \bar{\tau} \\ 1 & \tau & 2 \end{pmatrix}$$

is, up to isomorphisms, the unique indecomposable positive definite hermitian form of determinant 1 in $\mathsf{M}_3(\mathcal{O}_K)$. Using (3.2), we get

$$T = \begin{pmatrix} 0 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 2 & 1 & 2 & 1 \\ 0 & -2 & 0 & 1 & 0 & 2 \\ -2 & -1 & -1 & 0 & 0 & 0 \\ -1 & -2 & 0 & 0 & 0 & 1 \\ -1 & -1 & -2 & 0 & -1 & 0 \end{pmatrix}.$$

We can now ask MAGMA what the Frobenius form of this matrix is:

$$J, B := \texttt{FrobeniusForm}(T) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -2 & 4 & 0 & 0 \\ 1 & 0 & -2 & -3 & 3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 \\ 2 & -1 & -3 & -2 & 4 & 0 \end{pmatrix},$$

where B is a matrix such that $BT^tB = J = J_6$. Thus, with the notation of § 3.3, if $a = a_0 M$, then $\Omega_a = [\Omega_1, \Omega_2] = \Omega_0{}^tB$ and

$$\tau_a = \begin{pmatrix} 2\tau & \tau & 0 \\ \tau & -3 + 2\tau/3 & 2/3 \\ 0 & 2/3 & \tau/6 \end{pmatrix}.$$

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

The Riemann matrix τ_a gives poor convergence for the computation of Thetanullwerte. In order to speed up the computation, we use the MAPLE function `Siegel`(τ_a) (see [3]). This returns a Riemann matrix τ' and $B' \in \mathrm{Sp}_6(\mathbb{Z})$ such that $\tau' = B'.\tau_a$. We then let

$$\Omega' = [\Omega'_1, \Omega'_2] = \Omega_a{}^t B'.$$

Again, we use MAPLE to compute the 36 even Thetanullwerte with a given precision and then an approximation of the expression

$$\chi := 2^{26} \cdot \pi^{54} \cdot \frac{\prod_{\varepsilon} \theta[\varepsilon](0, \tau')}{\det(\Omega'_2)^{18}}.$$

Doing this to 50 digits of precision, we guess that $\chi = (7^7)^2$.

Remark 2. We recognize the square of the discriminant of the Klein quartic with equation $X_{7,1} : x^3y + y^3z + z^3x = 0$ (see [19, § 2] for a definition of the canonical discriminant). This is an example of Klein's formula (see [19, Theorem 2.2.3]) and should come as no surprise since it is known that $\mathrm{Jac}(X_{7,1}) \simeq_{\mathbb{Q}(\sqrt{-7})} (E(7)^3, a_0M)$.

4.3. *The tables*

In Tables 2 and 3, we gather the results we found for when $d = 7, 19, 43$ or 67, $A = E(d)^3 \otimes \mathbb{Q}$ and M runs over the indecomposable positive definite hermitian forms of dimension 3 and determinant 1 with coefficients in $\mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-d})/2$, up to isomorphisms (see [29]). As there are more than 100 possibilities for $d = 163$, we include only two cases: one with trivial automorphism group and the other with the only automorphism group of order 12. Let us make a few comments on the content of these tables.

(1) The first column contains the discriminant d and the index of M from the tables of [29].

(2) The computation of $\chi_{18}((A, a_0M), \omega_0)$ is as described in § 4.2. Note that since (A, a_0M) is defined over $\mathbb{Z}[\tau]$, this value may not be in $\mathbb{Z}$. In the tables we use $[a, b]$ to denote the element $a + b\tau$. Also, the second line gives the primes below $a + b\tau$ in the same order. For all these irrational cases, we find that there is a form in [29] for which we obtain the conjugate value. This form could have been taken as $\bar{M}$, but this is not the case in [29]. Thus the first column contains a second index for the form corresponding to the conjugate value.

(3) The third column gives the order of the automorphism group G of M, that is, the set of $Q \in \mathsf{GL}_3(\mathbb{Z}[\tau])$ such that ${}^t\bar{Q}MQ = M$. It is easy to see that such an automorphism Q is actually an automorphism of the principally polarized abelian variety (A, a). When (A, a) is geometrically the Jacobian of a non-hyperelliptic curve C, Torelli's theorem shows that the order of the automorphism group of C is half the order of G.

(4) To validate the values in the table from their approximations, we would need further information such as integrality, divisors bounds etc. So far, these values have to be treated as conjectural.

Remark 3. Similar computations can be done in the non-principal case. For instance, if one considers the curve

$$E(15) : y^2 = x^3 + \left(\frac{15}{32} + \frac{219}{32}\sqrt{5}\right)x - \left(\frac{77}{16} + \frac{385}{32}\sqrt{5}\right)$$

with CM by $\sqrt{-15}$ and the form 15 (dim.3.1) #2 from Schiemann's tables [29],

$$M = \begin{pmatrix} 2 & -1 & -1+\bar{\tau} \\ -1 & 2 & 1-\bar{\tau} \\ -1+\tau & 1-\tau & 3 \end{pmatrix} \quad \text{with } \tau = \frac{1+\sqrt{-15}}{2},$$

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

one gets

$$\begin{aligned}\chi = {} & 22\,769\,095\,299\,822\,142\,340\,569\,171\,645\,771\,726\,299/4\\ & + 10\,182\,522\,603\,020\,834\,484\,863\,085\,151\,244\,322\,675 \cdot \sqrt{5}/4\\ & + 4462\,640\,909\,353\,821\,881\,995\,695\,647\,429\,476\,869 \cdot \sqrt{-15}/4\\ & + 9978\,330\,617\,922\,886\,443\,823\,982\,755\,114\,202\,445 \cdot \sqrt{-3}.\end{aligned}$$

Note that the corresponding curve must have 24 automorphisms.

We now give a dual point of view which was suggested to us by Serre. Let $E_{d,i}$ be the quadratic twist of $E(d)$ by the non-square part δ of the value of χ corresponding to the form M in line $d, \#i$ of our tables. By the remark at the beginning of § 4.1, we see that

TABLE 2. *Computation of* χ.

d	M	$\chi := \chi_{18}((A, a_0M), \omega_0)$	$\#\mathrm{Aut}(A, a_0M)$
7, # 1	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & \bar{\tau} \\ 1 & \tau & 2 \end{pmatrix}$	$(7^7)^2$	$2 \cdot 168$
19, # 1	$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\bar{\tau} & 3 \end{pmatrix}$	$(2^5 \cdot 19^7)^2 \cdot (-2)$	$2 \cdot 6$
43, # 1	$\begin{pmatrix} 3 & 1 & 1-\bar{\tau} \\ 1 & 4 & 2 \\ 1-\tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 43^7)^2 \cdot (-47 \cdot 79 \cdot 107 \cdot 173)$	$2 \cdot 1$
43, # 2	$\begin{pmatrix} 3 & 1+\bar{\tau} & 2-\bar{\tau} \\ 1+\tau & 5 & 2-\bar{\tau} \\ 2-\tau & -2-\tau & 5 \end{pmatrix}$	$(2^5 \cdot 3^4 \cdot 43^7)^2 \cdot (-2 \cdot 3 \cdot 7)$	$2 \cdot 6$
43, # 3	$\begin{pmatrix} 2 & -1 & 1 \\ -1 & 4 & 1+\bar{\tau} \\ 1 & 1-\tau & 4 \end{pmatrix}$	$(2^6 \cdot 5^3 \cdot 43^7)^2 \cdot (-487)$	$2 \cdot 2$
43, # 4, 5	$\begin{pmatrix} 3 & 1 & -1-\bar{\tau} \\ 1 & 3 & -1 \\ -1-\tau & -1 & 5 \end{pmatrix}$	$-2^{11} \cdot 3^9 \cdot [1,2]^{27} \cdot [5,-2] \cdot [7,-2] \cdot [17,-4]$ $= -2^{11} \cdot 3^9 \cdot 43^{13} \cdot (43 \cdot 59 \cdot 79 \cdot 397)^{1/2}$	$2 \cdot 2$
67, # 1, 2	$\begin{pmatrix} 5 & -1-\bar{\tau} & -\bar{\tau} \\ -1-\tau & 5 & 2 \\ -\tau & 2 & 6 \end{pmatrix}$	$2^{11} \cdot [-1,2]^{28} \cdot [1,2] \cdot [-11,2] \cdot [-15,2]$ $\cdot [3,4] \cdot [1,6] \cdot [23,2] \cdot [21,4] \cdot [-49,2]$ $\cdot [43,6] \cdot [55,6] \cdot [53,16]$ $= 2^{11} \cdot 67^{14} \cdot (71 \cdot 167 \cdot 263 \cdot 293$ $\cdot 619 \cdot 643 \cdot 797 \cdot 2371 \cdot 2719 \cdot 3967 \cdot 8009)^{1/2}$	$2 \cdot 1$
67, # 3	$\begin{pmatrix} 5 & -2+\bar{\tau} & -1-\bar{\tau} \\ -2+\tau & 6 & -2 \\ -1-\tau & -2 & 7 \end{pmatrix}$	$(2^6 \cdot 3^6 \cdot 67^7)^2(-13 \cdot 53 \cdot 71 \cdot 131 \cdot 3319)$	$2 \cdot 1$
67, # 4, 5	$\begin{pmatrix} 3 & -1 & 1 \\ -1 & 4 & -\bar{\tau} \\ 1 & -\tau & 5 \end{pmatrix}$	$2^{12} \cdot 3^9 \cdot [-1,2]^{27} \cdot [-5,2] \cdot [-7,2] \cdot [-3,4]$ $\cdot [1,4] \cdot [-13,4] \cdot [-15,8] \cdot [-33,8] \cdot [23,10]$ $= 2^{12} \cdot 3^9 \cdot 67^{13} \cdot (67 \cdot 83 \cdot 103 \cdot 269$ $\cdot 277 \cdot 389 \cdot 1193 \cdot 1913 \cdot 2459)^{1/2}$	$2 \cdot 1$

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

$\chi_{18}((E_{d,i}^3, a_0 M), \omega_0) = \delta^{27} \cdot \chi$ is now a square in $K = \mathbb{Q}(\sqrt{-d})$, so there is a genus-3 curve $X_{d,i}$ defined over K such that $\mathrm{Jac}(X_{d,i}) \simeq E_{d,i}^3$.

EXAMPLE 1. Let us consider the case 19, #1. The quadratic twist by -2 of $E(19)$ is

$$E_{19,1} : y^2 = x^3 - 152x - 722.$$

Using the construction of [8] applied to our period matrix, it is possible to compute a model $f = 0$ for the curve $X_{19,1}$. Guàrdia found that

$$\begin{aligned} f = {} & U^4 + 2U^3V - 2U^3W + (6 - 3i\sqrt{19})U^2V^2 + 18U^2VW + (6 + 3i\sqrt{19})U^2W^2 \\ & + (5 - 3i\sqrt{19})UV^3 + (15 + 3i\sqrt{19})UV^2W + (-15 + 3i\sqrt{19})UVW^2 \\ & + (-5 - 3i\sqrt{19})UW^3 + \tfrac{1}{2}(3 - 3i\sqrt{19})V^4 + (12 + 4i\sqrt{19})V^3W - 30V^2W^2 \\ & + (12 - 4i\sqrt{19})VW^3 + \tfrac{1}{2}(3 + 3i\sqrt{19})W^4. \end{aligned}$$

TABLE 3. *Computation of* χ.

d	M	$\chi := \chi_{18}((A, a_0 M), \omega_0)$	$\#\mathrm{Aut}(A, a_0 M)$
67, # 6	$\begin{pmatrix} 5 & -1+\bar{\tau} & \bar{\tau} \\ -1+\tau & 5 & 2 \\ \tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 5^3 \cdot 67^7)^2 \cdot 83 \cdot 211 \cdot 1637 \cdot 2441$	$2 \cdot 1$
67, # 7	$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 3 & -2+\bar{\tau} \\ -1 & -2+\tau & 7 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 67^7)^2 \cdot (-2 \cdot 7 \cdot 31)$	$2 \cdot 6$
67, # 8, 9	$\begin{pmatrix} 3 & -1 & -2+\bar{\tau} \\ -1 & 4 & 0 \\ -2+\tau & 0 & 7 \end{pmatrix}$	$2^{11} \cdot 7^6 \cdot [-1, 2]^{27} \cdot [1, 2]^2$ $\cdot [-37, 6] \cdot [-71, 12] \cdot [-71, 30]$ $= 2^{11} \cdot 7^6 \cdot 67^{13} \cdot (67 \cdot 71^2 \cdot 1759$ $\cdot 6637 \cdot 18211)^{1/2}$	$2 \cdot 2$
67, # 10, 12	$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 4 & -1+\bar{\tau} \\ 0 & -1+\tau & 5 \end{pmatrix}$	$-2^{11} \cdot 3^9 \cdot 5^6 \cdot [-1, 2]^{27}$ $\cdot [-3, 2] \cdot [3, 2] \cdot [-21, 2] \cdot [-31, 2]$ $= -2^{11} \cdot 3^9 \cdot 5^6 \cdot 67^{13}$ $\cdot (67 \cdot 71 \cdot 83 \cdot 467 \cdot 967)^{1/2}$	$2 \cdot 2$
67, # 11	$\begin{pmatrix} 5 & \bar{\tau} & -2 \\ \tau & 6 & 2+\bar{\tau} \\ -2 & 2+\tau & 6 \end{pmatrix}$	$(2^6 \cdot 3^4 \cdot 5^3 \cdot 67^7)^2 \cdot (-3 \cdot 7 \cdot 8731)$	$2 \cdot 2$
67, # 13	$\begin{pmatrix} 3 & 1 & -1 \\ 1 & 5 & -3+\bar{\tau} \\ -1 & -3+\tau & 5 \end{pmatrix}$	$(2^8 \cdot 5^4 \cdot 67^7)^2 \cdot (-2 \cdot 5 \cdot 9769)$	$2 \cdot 2$
163, # 3, 4	$\begin{pmatrix} 7 & 3-\bar{\tau} & 2+\bar{\tau} \\ 3-\tau & 82 & -3+\bar{\tau} \\ 2+\tau & -3+\tau & 14 \end{pmatrix}$	$-2^{12} \cdot [-1, 2]^{27} \cdot [-5, 2] \cdot [15, 4] \cdot [31, 2]$ $\cdot [67, 8] \cdot [-137, 8] \cdot [-39, 28] \cdot [-49, 44]$ $\cdot [-743, 94] \cdot [-169, 164] \cdot [-907, 158]$ $\cdot [445, 406] \cdot [-2507, 342] \cdot [-3029, 244]$ $\cdot [-2777, 388] \cdot [4043, 74]$ $= -2^{12} \cdot 63^{27} \cdot (179 \cdot 941 \cdot 1187 \cdot 7649$ $\cdot 20\,297 \cdot 32\,573 \cdot 79\,621 \cdot 844\,483$ $\cdot 1103\,581 \cdot 1702\,867 \cdot 7136\,971$ $\cdot 10\,223\,179 \cdot 10\,876\,741$ $\cdot 12\,806\,557 \cdot 16\,869\,547)^{1/2}$	$2 \cdot 1$
163, # 85	$\begin{pmatrix} 2 & 1 & -\bar{\tau} \\ 1 & 2 & 1-\bar{\tau} \\ -\tau & 1-\tau & 28 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 11^4 \cdot 163^7)^2 \cdot (-2 \cdot 7 \cdot 11 \cdot 19 \cdot 127)$	$2 \cdot 6$

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

One can check that the discriminant of $-f/2$ is $2^{19} \cdot 19^7$, which is indeed a square root of

$$\chi_{18}((E^3_{19,1}, a_0 M), \omega_0) = (-2)^{27} \cdot (2^5 \cdot 19^7)^2 \cdot (-2).$$

Note that this curve can be descended over $\mathbb{Q}$, and after some simplifications one finds

$$X_{19,1} : x^4 + (1/9)y^4 + (2/3)x^2y^2 - 190y^2 - 570x^2 + (152/9)y^3 - 152x^2y - 1083 = 0.$$

EXAMPLE 2. In the same way,

$$\begin{aligned} X_{43,3} : -\frac{20}{43}x^3y - 84x^2y - \frac{4377}{10}x^2y^2 - \frac{105}{4}xy + \frac{190\,361}{20}xy^3 + \frac{20}{1849}x^4 + 1806xy^2 \\ + \frac{2205}{64} + \frac{105}{86}x^2 + \frac{96\,879}{32}x^2 - \frac{1849}{2}y^3 - \frac{12\,571\,351}{320}y^4 + \frac{989}{2}y = 0. \end{aligned}$$

One can check that the discriminant of $-f$ is $2^6 \cdot 5^3 \cdot 43^7 \cdot 487^{14}$.

4.4. *Application to optimal genus-3 curves*

Here we give an example to explain how our ideas apply. We want to prove that there is a genus-3 curve C over $F = \mathbb{F}_{47}$ whose number of rational points attains the Serre–Weil bound, that is, $\#C(F) = p + 1 + 3\lfloor 2\sqrt{p} \rfloor = 87$. According to [**21**], if such a curve exists, its Jacobian must be isogenous to the third power of an elliptic curve E/F with trace $-\lfloor 2\sqrt{p} \rfloor = -13$. This means that the elliptic curve E is ordinary and thus such a curve exists. Moreover, if π denotes the Frobenius endomorphism of E, then $\mathbb{Z}[\pi] \simeq \mathbb{Z}[(13 + \sqrt{13^2 - 4 \cdot 47})/2] = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-19})/2$. So $\mathrm{End}(E) = \mathbb{Z}[\pi]$ is the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-19})$. Note that since $(-19/47) = 1$, all endomorphisms are defined over F. Moreover, since the class number of $\mathcal{O}_K$ is 1, E is unique up to isomorphisms.

By Proposition 3.5, we know that $\mathrm{Jac}(C)$ is actually isomorphic to E^3. By Proposition 3.6, the existence of an indecomposable principal polarization on $\mathrm{Jac}(C)$ translates into the existence of an indecomposable positive definite hermitian form $M \in \mathsf{M}_3(\mathcal{O}_K)$ of determinant 1. In [**29**], such forms have been classified up to isomorphisms for some imaginary quadratic orders. In the present case there exists only one, given by

$$M = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\bar{\tau} & 3 \end{pmatrix}.$$

So if C exists, then $\mathrm{Jac}(C) \simeq (E^3, a)$ with $a = a_0 M$.

Let us consider the quadratic twist E' of E and the quadratic twist $(A', a') = (E'^3, a_0 M)$ of (E^3, a). Let $E(19)$ be the model of the elliptic curve with CM by $\sqrt{-19}$ given in Table 1. Using Lemma 4.1, we can see that $\mathrm{Tr}(E(19) \otimes F) = 13$, that is, $E(19) \otimes F = E'$. Since the endomorphism algebra $\mathrm{End}(E(19) \otimes \mathbb{Q})$ is equal to $\mathcal{O}_K$, we can consider the principally polarized abelian variety $(\tilde{A}, \tilde{a}) = (E(19)^3, a_0 M)$, which is a lift of (A', a'). Table 2 asserts that

$$\chi_{18}((\tilde{A}, \tilde{a}) \otimes \mathbb{Q}, \omega_0 \otimes \mathbb{Q}) = (2^5 \cdot 19^7)^2 \cdot (-2).$$

This is not a square over $\mathbb{Q}$, and since $(-2/47) = -1$ it is a non-square over F. Hence Proposition 2.5 gives us that (A', a') is not a Jacobian; therefore by Theorem 1.1 its quadratic twist (A, a) is. In conclusion, we have obtained that there is an optimal curve over $\mathbb{F}_{47}$ but no minimal curve (that is, one whose number of rational points is equal to $p + 1 - 3\lfloor 2\sqrt{p} \rfloor = 9$).

In the same way, we can prove that there is an optimal but not a minimal genus-3 curve over $\mathbb{F}_p$ for $p = 61, 137$ and 277, while there is a minimal but not an optimal genus-3 curve for $p = 311$. A model for each of these curves can be obtained by reducing modulo p the model of $X_{19,1}$ given in § 4.3. This gives us a way to check our results. Note that these values have also been confirmed via explicit computations by Top [**31**] and Alekseenko *et al.* [**1**].

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

Corollary 4.2. *We have* $N_q(3) = q + 1 + 3\lfloor 2\sqrt{q}\rfloor$ *for* $q = 47, 61, 137$ *or* 277.

Remark 4. Using $d = 67$ together with the form #3 and #7, respectively, it seems that there is a minimal and an optimal curve over $\mathbb{F}_{23^3}$.

Acknowledgements. I would like to thank Kristin Lauter, who inspired this project during her visit in June 2008, and Everett Howe, Gilles Lachaud and Alexey Zykin for helpful discussions in the course of writing previous versions of this article. I am also grateful to Jordi Guàrdia who computed models of the curves $X_{19,1}$ and $X_{43,3}$ for me. Finally, it is my pleasure to thank Jean-François Mestre and Jean-Pierre Serre for their stimulating questions and comments on the first version of this article.

References

1. E. Alekseenko, S. Aleshnikov, N. Markin and A. Zaytsev, 'Optimal curves of genus 3 over finite fields with discriminant −19', Preprint, 2009, http://arxiv.org/abs/0902.1901.

2. C. Birkenhake and H. Lange, *Complex abelian varieties*, 2nd edn Grundlehren der Mathematischen Wissenschaften 302 (Springer, Berlin, 2004).

3. B. Deconinck and M. van Hoeij, 'algcurves[Siegel]', 2001, http://www.math.fsu.edu/∼hoeij/RiemannTheta/Siegel.

4. M. Deuring, 'Die Typen der Multiplicatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Univ. Hamburg* 14 (1941) 197–272.

5. G. Faltings and C.-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 22 (Springer, Berlin, 1990).

6. G. Van der Geer and M. van der Vlugt, 'Tables of curves with many points', 2009, http://www.science.uva.nl/∼geer/.

7. B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics 776 (Springer, Berlin, 1980).

8. J. Guàrdia, 'On the Torelli problem and Jacobian Nullwerte in genus three', Preprint, 2009, http://arxiv.org/abs/0901.4376.

9. D. W. Hoffmann, 'On positive definite hermitian forms', *Manuscripta Math.* 71 (1991) 399–429.

10. E. Howe, E. Nart and C. Ritzenthaler, 'Isogeny classes of Jacobians of dimension 2 over finite fields', *Ann. Inst. Fourier (Grenoble)* 59 (2009) 239–289.

11. W. L. Hoyt, 'On products and algebraic families of Jacobian varieties', *Ann. of Math.* 77 (1963) 415–423.

12. T. Ibukiyama, 'On rational points of curves of genus 3 over finite fields', *Tôhoku Math. J.* 45 (1993) 311–329.

13. T. Ichikawa, 'Teichmüller modular forms of degree 3', *Amer. J. Math.* 117 (1995) 1057–1061.

14. T. Ichikawa, 'Theta constants and Teichmüller modular forms', *J. Number Theory* 61 (1996) 409–419.

15. T. Ichikawa, 'Generalized Tate curve and integral Teichmüller modular forms', *Amer. J. Math.* 122 (2000) 1139–1174.

16. J.-I. Igusa, 'Modular forms and projective invariants', *Amer. J. Math* 89 (1967) 817–855.

17. F. Klein, 'Zur Theorie der Abelschen Funktionen', *Math. Ann.* 36 (1889–90); Gesammelte mathematische Abhandlungen XCVII, 388–474.

18. G. Lachaud and C. Ritzenthaler, 'On a conjecture of Serre on abelian threefolds', *Symposium on algebraic geometry and its applications (Tahiti, 2007)* (World Scientific, Singapore, 2008) 88–115.

19. G. Lachaud, C. Ritzenthaler and A. Zykin, 'Jacobians among Abelian threefolds: a formula of Klein and a question of Serre', *Math. Res. Lett.*, to appear.

20. H. Lange, 'Principal polarizations on products of elliptic curves', *The geometry of Riemann surfaces and abelian varieties*, Contemporary Mathematics 397 (American Mathematical Society, Providence, RI, 2006) 153–162.

21. K. Lauter, 'Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields', *J. Algebraic Geom.* 10 (2001) 19–36, with an appendix by J.-P. Serre.

22. K. Lauter, 'The maximum or minimum number of rational points on genus three curves over finite fields', *Compositio Math.* 134 (2002) 87–111, with an appendix by J.-P. Serre.

23. S. Meagher, 'Twists of genus three and their Jacobians', PhD Thesis, Rijksuniversiteit Groningen, 2008, http://irs.ub.rug.nl/ppn/314417028.

24. J. S. Milne, 'Abelian varieties', *Arithmetic geometry*, (eds G. Cornell and J. H. Silverman; Springer, New York, 1986).

25. D. Mumford, *Abelian varieties* (Oxford University Press, Oxford, 1970).

26. E. Nart and C. Ritzenthaler, 'Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2', *Finite Fields Appl.* 14 (2008) 676–702.

27. E. Nart and C. Ritzenthaler, 'Genus 3 curves with many involutions and application to maximal curves in characteristic 2', *Proceedings of AGCT-12*, to appear.

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press

28. F. Oort and K. Ueno, 'Principally polarized abelian varieties of dimension two or three are Jacobian varieties', *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 20 (1973) 377–381.
29. A. Schiemann, 'Classification of hermitian forms with the neighbour method', *J. Symbolic Comput.* 26 (1998) 487–508. See tables at http://www.math.uni-sb.de/ag/schulze/Hermitian-lattices/.
30. J.-P. Serre, 'Nombre de points des courbes algébriques sur $\mathbb{F}_q$', *Séminaire de Théorie des Nombres de Bordeaux*, 1982–83, exp. no. 22 (Oeuvres III, no. 132, 701–705).
31. J. Top, 'Curves of genus 3 over small finite fields', *Indag. Math. (N.S.)* 14 (2003) 275–283.
32. W. C. Waterhouse, 'Abelian varieties over finite fields', *Ann. Sci. École Norm. Sup.* (4) (1969) 521–560.

Christophe Ritzenthaler
Institut de mathématiques de Luminy
UMR 6206
163 Avenue de Luminy Case 907
13288 Marseille
France

ritzenth@iml.univ-mrs.fr

https://doi.org/10.1112/S1461157009000576 Published online by Cambridge University Press