ANNALES

DE

L’INSTITUT FOURIER

Eyal Z. GOREN & Kristin E. LAUTER

Class Invariants for Quartic CM Fields

Tome 57, nº 2 (2007), p. 457-480.

<http://aif.cedram.org/item?id=AIF_2007__57_2_457_0>

Ann. Inst. Fourier, Grenoble
57, 2 (2007) 457-480

CLASS INVARIANTS FOR QUARTIC CM FIELDS

by Eyal Z. GOREN & Kristin E. LAUTER

Abstract. — One can define class invariants for a quartic primitive CM field K as special values of certain Siegel (or Hilbert) modular functions at CM points corresponding to K. Such constructions were given by de Shalit-Goren and Lauter. We provide explicit bounds on the primes appearing in the denominators of these algebraic numbers. This allows us, in particular, to construct S-units in certain abelian extensions of a reflex field of K, where S is effectively determined by K, and to bound the primes appearing in the denominators of the Igusa class polynomials arising in the construction of genus 2 curves with CM, as conjectured by Lauter.

Résumé. — On peut définir des invariants de classe pour un corps CM quartique primitif K comme valeurs spéciales de certaines fonctions modulaires de Siegel (ou Hilbert) aux points CM associés à K. De telles constructions ont été décrites par de Shalit-Goren et Lauter. Nous donnons des bornes explicites pour les idéaux premiers divisant les dénominateurs de ces nombres algébriques. Cela nous permet, en particulier, de construire des S-unités dans certaines extensions abéliennes d'un corps réflexe de K, où S est explicitement determiné par K, et de borner les nombres premiers apparaissant aux dénominateurs des polynômes de classe d'Igusa qui interviennent dans la construction des courbes CM de genre 2, comme dans la conjecture de Lauter.

1. Introduction

One of the main problems of algebraic number theory is the explicit description of ray class fields of a number field K. Besides the case of the field of rational numbers, the theory is most advanced in the case where K is a complex multiplication (CM) field. Effective constructions are available using modular functions generalizing the elliptic modular function j; one constructs modular functions as quotients of two modular forms on a Siegel upper half space and evaluates at CM points corresponding to K. The

Keywords: Class invariant, modular form, complex multiplication, polarization, superspecial abelian variety, units, Igusa invariants, quaternion algebra.
Math. classification: 11G15, 11G16, 11G18, 11R27.

values lie in an explicitly determined extension of the reflex field K^* of K, that depends on the field over which the Fourier coefficients of the modular function are defined, on the level of the modular function, on the conductor of the order of K corresponding to the CM point, and on the CM type. We loosely call magnitudes constructed this way *"class invariants"* of K. The terminology is proposed because when the Fourier coefficients are rational and the level is 1 the values of the modular function at CM points lie in ray class fields of K^*.

An outstanding problem is the effective construction of units in abelian extensions of number fields, even in the case of complex multiplication. A solution of this problem is expected to have significant impact on obtaining additional cases of Stark's conjecture. The case of cyclotomic units and elliptic units is well developed, but in higher dimensional cases little was known. The essential problem is that divisors of modular functions cannot be supported at the boundary of the moduli space. In this paper we provide explicit bounds on the primes appearing in the denominators of class invariants of a primitive quartic CM field K. This yields, in particular, an explicit bound on the primes dividing the invariants $u(\mathfrak{a}, \mathfrak{b})$ constructed in [24], thus yielding S-units lying in a specific abelian extension of K^* for an explicit finite set of primes S. To the best of our knowledge, excluding very particular fields, this is the first time such a result has been obtained for primitive CM fields of degree 4.

In [9], Gross and Zagier give factorization formulae for differences of CM values of the modular j-function. The factorization formulae are interpreted in later work in terms of heights of Heegner points and are related to certain special values of L-functions. One may view a special case of their work as studying the Hilbert class polynomial of a quadratic imaginary field and the norm of its value at a CM point associated to another quadratic imaginary field. The Hilbert class polynomial has integer coefficients, but this is not the case in higher-dimensional situations. Motivated by the work of Gross and Zagier, it is reasonable to expect similar results for Siegel modular functions, where now there is no canonical choice analogous to the j-function. Nonetheless, Igusa defined certain Siegel modular functions which give the invariants of genus 2 curves and so are, in some sense, canonical. One is led to consider the class polynomials associated to the Igusa functions. Our bound on the primes appearing in the denominators of class invariants gives an explicit bound, closely related to the discriminant of the primitive quartic CM field, on the primes appearing in the denominators of the Igusa class polynomials arising in the construction of genus 2 curves with CM, as conjectured in [17]. In this same spirit but using different methods, Bruinier and Yang [1] have recently obtained very interesting factorization formulae for genus 2 Hilbert modular functions averaged over CM cycles for a certain class of primitive quartic CM fields. Their results do not give bounds on the primes in the denominators of Igusa class polynomials; however, they have conjectural expressions for intersection numbers which would imply such bounds. In Section 5.2, we will compare our bound to the conjectural bounds of [1] and [17]. Villegas has explained in private correspondence how to obtain factorization formulae for the split CM case of bi-quadratic fields, (see also his example worked out in [23]), but his methods do not generalize to the case of primitive quartic CM fields.

Our methods are geometric in nature and in order to prove our bounds, we reformulate the question of primes of bad reduction for genus 2 CM curves over a number field in terms of a solution to a certain embedding problem of a CM field into the two-by-two matrices with entries in a quaternion algebra. We provide an explicit bound on the primes of bad reduction for genus 2 CM curves over a number field which is related to the discriminant of the CM field. In the process, we are led to study the arithmetic of definite quaternion algebras and we show that elements of small norm belong to a commutative sub-algebra. As a consequence, we provide an alternate proof for Gross and Zagier's bound on the primes dividing the difference of singular moduli.

2. Elements of small norm in a definite quaternion algebra

2.1. A volume estimate and elements of small norm

Let $B = B_{p,\infty}$ be "the" quaternion algebra over $\mathbb{Q}$ ramified at $\{p, \infty\}$. Concrete models for B can be found in e.g. [29, p. 98]. Let Tr and $\mathbf{N}$ be the (reduced) trace and norm on B and $x \mapsto \overline{x} = \mathrm{Tr}(x) - x$ its canonical involution. Let R be a maximal order of B. The discriminant of R is p^2; if we choose a $\mathbb{Z}$-basis $v_1, \dots, v_4$ for R then $\det(\mathrm{Tr}(v_i\overline{v_j})) = p^2$; cf. [21, Prop. 1.1]. Further, using this basis we may identify $B \otimes \mathbb{R}$ with $\mathbb{R}^4$. The bilinear form $\langle \alpha, \beta \rangle = \mathrm{Tr}(\alpha\overline{\beta})$ is represented with respect to this basis by an integral symmetric 4×4 matrix M with even diagonal entries, which is positive definite and satisfies $\det(M) = p^2$. It defines an inner product on $\mathbb{R}^4$. We let $\|r\| = \sqrt{\langle r, r \rangle} = \sqrt{2\mathbf{N}(r)}$. Note that the co-volume of R (the absolute value of the volume of a fundamental parallelepiped) is p.

Lemma 2.1.1. — *Let K_i, $i = 1, 2$, be quadratic imaginary subfields of B. We assume that one of the following equivalent conditions holds: (i) $K_1 \neq K_2$; (ii) K_1 does not commute with K_2; (iii) $K_1 \cap K_2 = \mathbb{Q}$.*

Let R be a maximal order of B. Let $k_i \in K_i$ be elements such that $\{1, k_i\}$ is a basis for K_i over $\mathbb{Q}$ and $k_i \in R$. Let L be the $\mathbb{Z}$-lattice spanned by $\{1, k_1, k_2, k_1k_2\}$. Then L is a full-rank sublattice of R and its co-volume satisfies

$$\text{co-vol}(L) \leqslant \|1\| \cdot \|k_1\| \cdot \|k_2\| \cdot \|k_1k_2\| = 4 \cdot \mathbf{N}(k_1) \cdot \mathbf{N}(k_2). \tag{2.1}$$

Proof. — Straightforward. □

Corollary 2.1.2 (Elements of small norm commute). — *If $k_1, k_2 \in R$ and $\mathbf{N}(k_1), \mathbf{N}(k_2) < \sqrt{p}/2$ then $k_1k_2 = k_2k_1$.*

Proof. — If $k_1k_2 \neq k_2k_1$ then the fields $K_i = \mathbb{Q}(k_i)$ satisfy the assumptions of Lemma 2.1.1. The co-volume of the lattice L is then strictly less than p, by (2.1). On the other hand, since $L \subseteq R$ we have $\text{co-vol}(L) \geqslant \text{co-vol}(R) = p$, which is a contradiction. □

Corollary 2.1.3. — *There is an order $\mathcal{O}_1$ of a quadratic imaginary field K_1, $\mathcal{O}_1 \subset R$, such that all elements of R of norm less than $\sqrt{p}/2$ belong to $\mathcal{O}_1$.*

2.2. Simultaneous embeddings and a weak form of a result of Gross-Zagier

Lemma 2.2.1. — *Let K_i, $i = 1, 2$, be quadratic imaginary fields of discriminant d_{K_i} contained in B, and let $\mathcal{O}_i$ be the order of conductor m_i of K_i, hence of discriminant $d_{\mathcal{O}_i} = m_i^2 d_{K_i}$. Assume that both $\mathcal{O}_1, \mathcal{O}_2$ are contained in R, a maximal order of B, and that $K_1 \neq K_2$. Then*

$$p \leqslant \frac{(d_{\mathcal{O}_1} - 1)(d_{\mathcal{O}_2} - 1)}{4}. \tag{2.2}$$

Proof. — To obtain optimal bounds one chooses $k_i \in \mathcal{O}_i$ of minimal norm, such that $\{1, k_i\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_i$. Write $K_i = \mathbb{Q}(\sqrt{D_i})$ with D_i a square free integer. One verifies that $k_i = \pm m_i\sqrt{D_i}$ if $D_i \equiv 2, 3 \pmod 4$, $(\pm 1 \pm m_i\sqrt{D_i})/2$ if $D_i \equiv 1 \pmod 4$ and m_i is odd, and $\pm m_i\sqrt{D_i}/2$ if $D_i \equiv 1 \pmod 4$ and m_i is even. The norm of k_i is, respectively, $m_i^2|D_i|/4$ and $m_i^2|D_i|, (1 + m_i^2|D_i|)/4$. Now apply Lemma 2.1.1, using that $p \leqslant \text{co-vol}(L)$. □

Lemma 2.2.1 allows us to draw a corollary that we view as a weak form of results of Gross-Zagier [9] and Dorman [4] on singular moduli. We say "weak" because they get explicit factorization formulae, while we only get a bound of the size of the primes involved in the factorization. Our technique, though, is much easier and also generalizes to higher dimensional situations. Interestingly enough, the bound we get is optimal.

Corollary 2.2.2. — *Let j_i, $i = 1, 2$, be two singular j-invariants, that is, j_i corresponds to an elliptic curve E_i that has complex multiplication by an order $\mathcal{O}_i$ of a quadratic imaginary field $K_i \subset \mathbb{C}$. Suppose that $K_1 \neq K_2$. Let $\mathfrak{p}$ be a prime of $\overline{\mathbb{Q}}$ dividing p. If $(j_1 - j_2) \in \mathfrak{p}$ then $p \leqslant \frac{(d_{\mathcal{O}_1}-1)(d_{\mathcal{O}_2}-1)}{4}$.*

Proof. — If $(j_1 - j_2) \in \mathfrak{p}$ then $E_1 \cong E_2 \pmod{\mathfrak{p}}$. Let $E = E_1 \pmod{\mathfrak{p}}$. Since $K_1 \neq K_2$, E is supersingular and, after fixing an isomorphism $\mathrm{End}(E) \otimes \mathbb{Q} \cong B$, $\mathrm{End}(E)$ is a maximal order of B containing $\mathcal{O}_1, \mathcal{O}_2$. □

Remark 2.2.3. — Corollary 2.2.2 can be extended to the case $K_1 = K_2 = K$ for, say, the maximal order of K. The missing ingredient is that the moduli space of elliptic curves, endowed with an action of $\mathcal{O}_K$ and of a fixed CM type, is étale over $\mathrm{Spec}(\mathcal{O}_K)$. This can be proved using the methods of § 4.4. It implies that different singular j-invariants corresponding to such elliptic curves define non-equivalent optimal embeddings, even upon reduction modulo a prime, and the method above applies.

3. An embedding problem

A number field K is a *CM field* if it is a totally imaginary quadratic extension of a totally real subfield K^+. A *CM type* Φ of K is a subset of $\mathrm{Hom}(K, \mathbb{C})$ such that $\Phi|_{K^+} = \mathrm{Hom}(K^+, \mathbb{C})$. In general, there is a notion of *primitive*, or *simple* CM type. This is a CM type that is not induced from a CM type of a CM subfield of K; see [16, Ch. I, § 2] and [25, Ch. II, § 8] for general information on CM fields and types. We say that K is a *primitive CM field*, if K has no proper CM subfields. Clearly, every CM type of K is then primitive.

Let K be a CM field of degree 4 over $\mathbb{Q}$, and let K^+ its totally real subfield. Write $K^+ = \mathbb{Q}(\sqrt{d})$, for $d > 0$ a square free integer. Write $K = K^+(\sqrt{r})$ with $r \in \mathbb{Z}[\sqrt{d}]$ a totally negative element. Every quartic CM field can be written this way. The following are equivalent: (i) K is primitive, i.e., does not contain a quadratic imaginary field; (ii) K is either non-Galois, or a cyclic Galois extension; (iii) $\mathbf{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(r)$ is not a square in $\mathbb{Q}$.

We remark that there is much known on the index of $\mathbb{Z}[\sqrt{d},\sqrt{r}]$ in $\mathcal{O}_K$ (see [27] and the proof of Proposition 5 in [5], where the index is always 2 or 4, for example). Intuitively, at least, the better one approximates $\mathcal{O}_K$ by $\mathbb{Z}[\sqrt{d},\sqrt{r}]$ the better bounds one should get in Theorem 3.0.4 and its applications.

Let E_1, E_2 be supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Let $\mathfrak{a} = \mathrm{Hom}(E_2, E_1)$, $\mathfrak{a}^\vee := \mathrm{Hom}(E_1, E_2)$, $R_i = \mathrm{End}(E_i)$. Then $\mathrm{End}(E_1 \times E_2) = \left(\begin{smallmatrix} R_1 & \mathfrak{a} \\ \mathfrak{a}^\vee & R_2 \end{smallmatrix}\right)$. The product polarization induced by the divisor $E_1 \times \{0\} + \{0\} \times E_2$ on $E_1 \times E_2$ induces a Rosati involution denoted by $\vee$. This involution is given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^\vee = \left(\begin{smallmatrix} a^\vee & c^\vee \\ b^\vee & d^\vee \end{smallmatrix}\right)$, where $a^\vee, b^\vee$ etc. denotes the dual isogeny. The Rosati involution is a positive involution. The algebra $\mathrm{End}(E_i) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$, ramified precisely at the places $\{p, \infty\}$. It is thus non-canonically isomorphic to the quaternion algebra B of § 2.1. Under any such isomorphism, R_i is a maximal order of B and we have $a^\vee = \overline{a}, d^\vee = \overline{d}$, where $\bar{\cdot}$ is the canonical involution of B.

The embedding problem: *For a quartic CM field K, and a prime p, to find a ring embedding $\iota\colon \mathcal{O}_K \hookrightarrow \mathrm{End}(E_1 \times E_2)$ such that the Rosati involution coming from the product polarization induces complex conjugation on $\mathcal{O}_K$.*

As we shall see below, the problem is intimately related with bounding primes in the denominators of class invariants.

Theorem 3.0.4. — *Let $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$ be a primitive quartic CM field as above. If the embedding problem has a positive solution then $p \leqslant d^2(\mathrm{Tr}(r))^2$.*

Proof. — Assume such an embedding ι exists. Then $\iota(\mathcal{O}_{K^+})$ is fixed by the Rosati involution, thus $\sqrt{d} \mapsto M = \left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right)$, for some $a, e \in \mathbb{Z}$, $b \in \mathfrak{a}$, $b^\vee = c$. Moreover, $M^2 = \left(\begin{smallmatrix} d & 0 \\ 0 & d \end{smallmatrix}\right)$. This gives the following conditions on the entries of M.

$$a^2 + bb^\vee = d, \qquad b(a+e) = 0$$
$$b^\vee(a+e) = 0, \qquad b^\vee b + e^2 = d.$$

If $a \neq -e$ then $b = 0$ and hence d is a square - a contradiction. Thus, $a = -e$, and we can write the embedding as

$$\sqrt{d} \mapsto M = \begin{pmatrix} a & b \\ b^\vee & -a \end{pmatrix}, \quad a \in \mathbb{Z},\ b \in \mathfrak{a},\ a^2 + bb^\vee = d. \tag{3.1}$$

We may write

$$r = \alpha + \beta\sqrt{d}, \quad \alpha < 0, |\alpha| > |\beta\sqrt{d}|.$$

The condition of the Rosati involution inducing complex conjugation is equivalent to $\iota(\sqrt{r})^\vee = -\iota(\sqrt{r})$. So, if $\iota(\sqrt{r}) = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ then $\left(\begin{smallmatrix} x^\vee & z^\vee \\ y^\vee & w^\vee \end{smallmatrix}\right) = -\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$. This translates into the conditions $x = -x^\vee$, $w = -w^\vee$, $y = -z^\vee$, implying in particular that x and w have trace zero, which we write as $x \in R_1^0$ and $w \in R_2^0$. It follows that

$$\iota(\sqrt{r}) = \begin{pmatrix} x & y \\ -y^\vee & w \end{pmatrix}, \qquad x \in R_1^0,\ w \in R_2^0,\ y \in \mathfrak{a}. \tag{3.2}$$

A further condition is obtained from $\iota(\sqrt{r})^2 = r$, i.e.,

$$\begin{pmatrix} x & y \\ -y^\vee & w \end{pmatrix}^2 = \begin{pmatrix} \alpha+\beta a & \beta b \\ \beta b^\vee & \alpha-\beta a \end{pmatrix},$$

that is,

$$\begin{pmatrix} x^2 - yy^\vee & xy + yw \\ -y^\vee x - wy^\vee & w^2 - y^\vee y \end{pmatrix} = \begin{pmatrix} \alpha+\beta a & \beta b \\ \beta b^\vee & \alpha-\beta a \end{pmatrix}. \tag{3.3}$$

Since $yy^\vee = y^\vee y \in \mathbb{Z}$, this leads to the following necessary conditions

$$(\star) \qquad \begin{aligned} x^2 - yy^\vee &= \alpha + \beta a, & xy + yw &= \beta b \\ w^2 - yy^\vee &= \alpha - \beta a, & a^2 + bb^\vee &= d, \end{aligned}$$

where $x \in R_1^0,\ w \in R_2^0,\ b, y \in \mathfrak{a},\ \alpha, \beta, a \in \mathbb{Z}$.

Note that $y = 0$ implies that either $b = 0$ or $\beta = 0$. The case $b = 0$ gives that d is a square, hence is not possible; the case $\beta = 0$ is possible, but leads to K a bi-quadratic field, contrary to our assumption.

We use the notation $\mathbf{N}(s) = ss^\vee$, $\mathbf{N}(y) = yy^\vee$, *etc.* Note that for $s \in R_i$ this definition of the norm is the usual one and, in any case, under the interpretation of elements as endomorphisms $\mathbf{N}(s) = \deg(s)$ and so $\mathbf{N}(st) = \mathbf{N}(s) \cdot \mathbf{N}(t)$ when the product st makes sense. It follows from $(\star)$ that

$$(\star\star) \qquad \begin{aligned} \mathbf{N}(x) + \mathbf{N}(y) &= -(\alpha + \beta a) \\ \mathbf{N}(w) + \mathbf{N}(y) &= -(\alpha - \beta a). \end{aligned}$$

Let $\varphi\colon E_1 \to E_2$ be a non-zero isogeny of degree δ. For $f \in \mathrm{End}(E_1 \times E_2)$ the composition of rational isogenies

$$E_1 \times E_1 \xrightarrow{(1,\varphi)} E_1 \times E_2 \xrightarrow{f} E_1 \times E_2 \xrightarrow{(1,\delta^{-1}\varphi^\vee)} E_1 \times E_1,$$

gives a ring homomorphism $\mathrm{End}^0(E_1 \times E_2) \longrightarrow \mathrm{End}^0(E_1 \times E_1)$ that can be written in matrix form as

$$f = \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \mapsto \begin{pmatrix} f_{11} & f_{12}\varphi \\ \delta^{-1}\varphi^\vee f_{21} & \delta^{-1}\varphi^\vee f_{22}\varphi \end{pmatrix}.$$

Let ψ be the composition $K \longrightarrow \mathrm{End}^0(E_1 \times E_2) \longrightarrow \mathrm{End}^0(E_1 \times E_1)$. Then ψ is an embedding of rings with the property

$$\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} \psi(\mathcal{O}_K) \subset M_2(R_1). \tag{3.4}$$

Choose $\varphi = y^\vee$. Taking $f = \left(\begin{smallmatrix} a & b \\ b^\vee & -a \end{smallmatrix}\right)$ (corresponding to $\sqrt{d}$), or $\left(\begin{smallmatrix} x & y \\ -y^\vee & w \end{smallmatrix}\right)$ (corresponding to $\sqrt{r}$), the embedding ψ is determined by

$$\psi(\sqrt{d}) = \begin{pmatrix} a & by^\vee \\ yb^\vee/\delta & -a \end{pmatrix}, \qquad \psi(\sqrt{r}) = \begin{pmatrix} x & \delta \\ -1 & ywy^\vee/\delta \end{pmatrix}. \tag{3.5}$$

We conclude that

$$S = \{by^\vee, yb^\vee, x, ywy^\vee\} \subset R_1.$$

Let

$$\begin{aligned} \delta_1 &= \min\{-(\alpha - \beta a), -(\alpha + \beta a)\} = |\alpha| - |\beta| \cdot |a|, \\ \delta_2 &= \max\{-(\alpha - \beta a), -(\alpha + \beta a)\} = |\alpha| + |\beta| \cdot |a|. \end{aligned}$$

It follows from (3.1) and ($\star\star$) that

$$\mathbf{N}(by^\vee) = \mathbf{N}(yb^\vee) \leqslant d\delta_1, \quad \mathbf{N}(x) \leqslant \delta_2.$$

Assume that $p > d^2(\mathrm{Tr}(r))^2 \geqslant \max\{4 \cdot d^2\delta_1^2, 4 \cdot \delta_2^2\}$. Then $\mathbf{N}(by^\vee)$, $\mathbf{N}(yb^\vee)$ and $\mathbf{N}(x)$ are all smaller than $\sqrt{p}/2$. By Corollary 2.1.3, the elements x, $y^\vee b$, $yb^\vee$ belong to some imaginary quadratic field K_1. The equation $xy + yw = \beta b$ appearing in ($\star$) gives the relation $xyy^\vee + ywy^\vee = \beta by^\vee$, which shows that $ywy^\vee \in K_1$. We conclude that ψ is an embedding $K \to M_2(K_1)$. This implies that $K_1 \hookrightarrow K$ (else consider the commutative subalgebra generated by K and K_1 in $M_2(K_1)$), contrary to our assumption. It follows that if there is a solution to the embedding problem ι then $p \leqslant d^2(\mathrm{Tr}(r))^2$. □

4. Bad reduction of CM curves

In this section we discuss the connection between solutions to the embedding problem and bad reduction of curves of genus two whose Jacobian has complex multiplication. We shall assume CM by the full ring of integers, but the arguments can easily be adapted to CM by an order, at least if avoiding primes dividing the conductor of the order.

4.1. Bad reduction solves the embedding problem

Fix a quartic primitive CM field K. Write $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, $r \in \mathcal{O}_{K^+}$, d a positive integer. Let $\mathscr{C}$ be a smooth projective genus 2 curve over a number field L. We say that $\mathscr{C}$ has CM (by $\mathcal{O}_K$) if $\mathrm{Jac}(\mathscr{C})$ has CM by $\mathcal{O}_K$. By passing to a finite extension of L we may assume that $\mathscr{C}$ has a stable model over $\mathcal{O}_L$ and that all the endomorphisms of $\mathrm{Jac}(\mathscr{C})$ are defined over L. Since K is primitive, $\mathrm{Jac}(\mathscr{C})$ is a simple abelian variety and so $\mathrm{End}^0(\mathrm{Jac}(\mathscr{C})) = K$. In particular, the natural polarization of $\mathrm{Jac}(\mathscr{C})$, associated to the theta divisor $\mathscr{C} \subset \mathrm{Jac}(\mathscr{C})$, preserves the field K and acts on it by complex conjugation.

It is well known that $\mathrm{Jac}(\mathscr{C})$ has everywhere good reduction. It follows that for every prime ideal $\mathfrak{p} \lhd \mathcal{O}_L$ either $\mathscr{C}$ has good reduction modulo $\mathfrak{p}$ or is geometrically isomorphic to two elliptic curves E_1, E_2 crossing transversely at their origins. In the latter case we have an isomorphism of principally polarized abelian varieties over $k(\mathfrak{p}) = \mathcal{O}_L/\mathfrak{p}$, $(\mathrm{Jac}(\mathscr{C}), \mathscr{C}) \cong (E_1 \times E_2, E_1 \times \{0\} + \{0\} \times E_2)$. Since $K \hookrightarrow \mathrm{End}(E_1 \times E_2) \otimes \mathbb{Q}$ we see that E_1 must be isogenous to E_2. Moreover, E_i cannot be ordinary; that implies that $K \hookrightarrow M_2(K_1)$ for some quadratic imaginary field K_1 and one concludes that $K_1 \hookrightarrow K$, contradicting the primitivity of K. We conclude

Lemma 4.1.1. — *Let $\mathscr{C}/L$ be a non-singular projective curve of genus 2 with CM by $\mathcal{O}_K$. Assume that $\mathscr{C}$ has a stable model over $\mathcal{O}_L$. If $\mathscr{C}$ has bad reduction modulo a prime $\mathfrak{p}|p$ of $\mathcal{O}_L$ then the embedding problem has a positive solution for the prime p.*

The following theorem now follows immediately using Theorem 3.0.4.

Theorem 4.1.2. — *Let $\mathscr{C}$ be a non-singular projective curve of genus 2 with CM by $\mathcal{O}_K$ and with a stable model over the ring of integers $\mathcal{O}_L$ of some number field L. Let $\mathfrak{p}|p$ be a prime ideal of $\mathcal{O}_L$. Assume that p is greater or equal to $d^2(\mathrm{Tr}(r))^2$ then $\mathscr{C}$ has good reduction modulo $\mathfrak{p}$.*

4.2. A solution to the embedding problem implies bad reduction

Theorem 4.2.1. — *Assume that the embedding problem of § 3 has a solution with respect to a primitive quartic CM field K. Then there is a smooth projective curve $\mathscr{C}$ of genus 2 over a number field L with CM by $\mathcal{O}_K$, whose endomorphisms and stable model are defined over $\mathcal{O}_L$, and a prime $\mathfrak{p}$ of $\mathcal{O}_L$ such that $\mathscr{C}$ has bad reduction modulo $\mathfrak{p}$.*

Our strategy for proving the theorem is the following. We consider a certain infinitesimal deformation functor $\mathbf{N}$ for abelian surfaces with CM by $\mathcal{O}_K$. We show that $\mathbf{N}$ is pro-representable by a $W(\overline{\mathbb{F}}_p)$-algebra R^{u}, and that a solution to the embedding problem can be viewed as an $\overline{\mathbb{F}}_p$-point x of $\mathrm{Spec}(R^{\mathrm{u}})$. We prove that R^{u} is isomorphic to the completed local ring of a point on a suitable Grassmann variety and deduce that $R^{\mathrm{u}} \otimes \mathbb{Q} \neq 0$. We conclude that x can be lifted to characteristic zero and finish using classical results in the theory of complex multiplication. Before beginning the proof proper, we need some preliminaries about Grassmann varieties.

4.3. Grassmann schemes

The following applies to any number field K with an involution $*$; we denote the fixed field of $*$ by K^+. Put $[K:\mathbb{Q}] = 2g$.

4.3.1. Consider the module $M_0 := \mathcal{O}_K \otimes_{\mathbb{Z}} W$, $W = W(\overline{\mathbb{F}}_p)$, equipped with an alternating perfect W-linear pairing $\langle \cdot, \cdot \rangle$ with values in W, such that for $s \in \mathcal{O}_K$ we have $\langle sr, r' \rangle = \langle r, s^* r' \rangle$. Note that this also holds for $s \in \mathcal{O}_K \otimes_{\mathbb{Z}} W$ if $*$ denotes the natural extension of the involution to this ring.

This defines a Grassmann problem: classify for W-algebras W' the isotropic, locally free, locally direct summands W'-submodules of $M_0 \otimes_W W'$ of rank g that are $\mathcal{O}_K$-invariant. This is representable by a projective scheme $\mathbf{G}' \to \mathrm{Spec}(W)$ (a closed subscheme of the usual (projective) Grassmann scheme). We claim that $\mathbf{G}'$ is topologically flat: namely, that every $\overline{\mathbb{F}}_p$-point of it lifts to characteristic zero. That means that for every submodule N_1 of $\mathcal{O}_K \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$, satisfying the conditions above, there is a flat W-algebra W' and such submodule N_0 of $\mathcal{O}_K \otimes_W W'$ that lifts N_1.

4.3.2. First note that for $k \supset W$ an algebraically closed field of characteristic zero, the k-points of $\mathbf{G}'$ are in bijection with "CM types". Indeed, we are to classify the isotropic, rank g, sub k-vector spaces of $\mathcal{O}_K \otimes_{\mathbb{Z}} k = \oplus_{\{\varphi\colon K \to k\}} k(\varphi)$, where $k(\varphi)$ is k on which $\mathcal{O}_K$ acts via φ. It is easy to see that the pairing decomposes as a direct sum of orthogonal pairings on the g subspaces $k(\varphi) \oplus k(\varphi \circ *)$ (use that for $r \in k(\varphi), r' \in k(\varphi')$ we have $\varphi(s)\langle r, r' \rangle = \langle sr, r' \rangle = \langle r, s^* r' \rangle = (\varphi' \circ *)(s)\langle r, r' \rangle$). On $k(\varphi) \oplus k(\varphi \circ *)$ the pairing is non-degenerate so every maximal isotropic subspace is a line and vice-versa. The condition of being an $\mathcal{O}_K$-submodule leaves us with precisely two submodules of $k(\varphi) \oplus k(\varphi \circ *)$, viz. $k(\varphi)$, $k(\varphi \circ *)$. Thus, the choice of an isotropic, $\mathcal{O}_K$-invariant k-subspace of dimension g of $\mathcal{O}_K \otimes_{\mathbb{Z}} k$ corresponds to choosing an element from each of the g pairs $\{\varphi, \varphi \circ *\}$.

4.3.3. We now prove topological flatness for $\mathbf{G}'$. We first make a series of reductions. Let $p = \prod \mathfrak{p}_i^{e_i}$ be the decomposition of p into prime in $\mathcal{O}_{K^+}$. We have $\mathcal{O}_{K^+} \otimes_{\mathbb{Z}} W = \oplus_{\mathfrak{p}|p} \mathcal{O}_{K^+_{\mathfrak{p}}} \otimes_{\mathbb{Z}_p} W$ (with corresponding idempotents $\{e_{\mathfrak{p}}\}$) and $\mathcal{O}_{K^+} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p = \oplus_{\mathfrak{p}|p} \mathcal{O}_{K^+}/\mathfrak{p}^{e_{\mathfrak{p}}} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$. The modules $M_0 = \mathcal{O}_K \otimes_{\mathbb{Z}} W$, $M_1 := \mathcal{O}_K \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$, which are, respectively, free $\mathcal{O}_{K^+} \otimes_{\mathbb{Z}} W$ and $\mathcal{O}_{K^+} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$ modules of rank 2, decompose accordingly as $\oplus_{\mathfrak{p}|p} M_0(\mathfrak{p}), \oplus_{\mathfrak{p}|p} M_1(\mathfrak{p})$. We claim that the submodules $\{M_0(\mathfrak{p}) : \mathfrak{p}|p\}$ (resp. $\{M_1(\mathfrak{p}) : \mathfrak{p}|p\}$) are orthogonal. Indeed, this follows from the fact that for the idempotents $\{e_{\mathfrak{p}}\}$ we have $\langle e_{\mathfrak{p}} r, e_{\mathfrak{p}'} r' \rangle = \langle e_{\mathfrak{p}}^2 r, e_{\mathfrak{p}'}^2 r' \rangle = \langle e_{\mathfrak{p}} r, e_{\mathfrak{p}} e_{\mathfrak{p}'}^2 r' \rangle = \delta_{\mathfrak{p},\mathfrak{p}'} \langle e_{\mathfrak{p}} r, e_{\mathfrak{p}'} r' \rangle$. We may thus assume without loss of generality that $p = \mathfrak{p}^e$ with residue degree f in $\mathcal{O}_{K^+}$ (note that the global nature of the rings $\mathcal{O}_K, \mathcal{O}_{K^+}$ plays no role). Let $W^+ = W(\mathbb{F}_{p^f})$ considered as the maximal unramified subextension of $\mathcal{O}_{K^+_{\mathfrak{p}}}$. A further reduction is possible: Since $\mathcal{O}_{K^+_{\mathfrak{p}}} \otimes_{\mathbb{Z}_p} W = \oplus_{\{W^+ \to W\}} \mathcal{O}_{K^+_{\mathfrak{p}}} \otimes_{W^+} W$, the same arguments as above (using idempotents etc.) allow us to assume with out loss of generality that $f = 1$. Thus, the problem reduces to the following:

4.3.4. One is given a p-adic ring of integers A, finite of rank e over W, and a free semi-simple A-algebra B of rank 2 with an involution $*$ whose fixed points are A. Also given is a perfect alternating pairing $\langle \cdot, \cdot \rangle \colon B \times B \to W$ such that for $s \in B$ we have $\langle sr, r' \rangle = \langle r, s^* r' \rangle$. One needs to show that every maximal isotropic $B \otimes_W \overline{\mathbb{F}}_p$ submodule of $B \otimes_W \overline{\mathbb{F}}_p$ lifts to characteristic zero in the sense previously described.

Note that B is either an integral domain that is a ramified extension of A or isomorphic as an A-algebra to $A \oplus A$ with the involution being the permutation of coordinates. The first case is immediate: We have $B \otimes_W \overline{\mathbb{F}}_p \cong \overline{\mathbb{F}}_p[t]/(t^{2e})$ and it has a unique submodule of rank e over $\overline{\mathbb{F}}_p$, viz. (t^e). Since the Grassmann scheme $\mathbf{G}'$ always has characteristic zero geometric points and is projective, a lift is provided by (any) characteristic zero point of $\mathbf{G}'$.

In the second case we have $B \otimes_W \overline{\mathbb{F}}_p \cong \overline{\mathbb{F}}_p[t]/(t^e) \oplus \overline{\mathbb{F}}_p[t]/(t^e)$. Every submodule of $B \otimes_W \overline{\mathbb{F}}_p$ of rank e over $\overline{\mathbb{F}}_p$ is a direct sum $(t^i) \oplus (t^{e-i})$. Such submodules are automatically isotropic. We claim that the submodule (t^i) of $\overline{\mathbb{F}}_p[t]/(t^e)$ can be lifted to characteristic zero, that such a lifting corresponds to a choice of $e - i$ embeddings $A \to \overline{\mathbb{Q}}_p$ over W and that each lifting is isotropic when considered as a submodule of $B \otimes_W W' = A \otimes_W W' \oplus A \otimes_W W'$, where W' is a "big enough" flat extension of W. Indeed, every geometric point of the appropriate Grassmann scheme, being proper over $\mathrm{Spec}(W)$, extends to an integral point (defined over a finite integral extension W'/W). Such a geometric point corresponds to a choice of $\binom{e}{i}$ embeddings $A \to \overline{\mathbb{Q}}_p$ over W and is isotropic (cf. § 4.3.2 – when we view $A \otimes W$ as a B-submodule of $B \otimes W$ via the first (or second) component, it is isotropic). Moreover, since the submodule (t^i) is uniquely determined by its rank, every such integral point indeed provides a lift of (t^i). It now easily follows that $(t^i) \oplus (t^{e-i})$ can be lifted in $\binom{e}{i}$ ways.

4.4. Proof of Theorem 4.2.1

By an *abelian scheme with CM* we mean in this section a triple $(A/S, \lambda, \iota)$, consisting of a principally polarized abelian scheme over S with an embedding of rings $\iota\colon \mathcal{O}_K \to \mathrm{End}_S(A)$ such that the Rosati involution defined by λ induces complex conjugation on $\mathcal{O}_K$. We denote complex conjugation on K by $*$ and let K^+ be the totally real subfield of K. As before, $W = W(\overline{\mathbb{F}}_p)$. The following lifting lemma, that holds for any CM field K and whose proof is given in §§ 4.4.1–4.4.4, is the key point. [1]

Lemma 4.4.1. — *Let (A, λ, ι) be an abelian variety with CM over $\overline{\mathbb{F}}_p$ then (A, λ, ι) can be lifted to characteristic zero.*

4.4.1. Let S be a local artinian ring with residue field $\overline{\mathbb{F}}_p$. Let (A', λ', ι') be an abelian scheme over S with CM. We claim that $\mathbb{H}^1_{\mathrm{dR}}(A'/S)$ is a free $\mathcal{O}_K \otimes_{\mathbb{Z}} S$-module of rank 1. Since $\mathbb{H}^1_{\mathrm{dR}}(A'/S)$ is a free S-module of rank $2g$, to verify that it is a free $\mathcal{O}_K \otimes_{\mathbb{Z}} S$-module it is enough to prove that modulo the maximal ideal of S (cf. [2, Rmq. 2.8]), namely, to prove that $\mathbb{H}^1_{\mathrm{dR}}(A' \otimes_S \overline{\mathbb{F}}_p/\overline{\mathbb{F}}_p)$ is a free $\mathcal{O}_K \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$-module. This is [22, Lem. 1.3]. In fact, loc. cit. gives that $H^1_{\mathrm{crys}}(A' \otimes_S \overline{\mathbb{F}}_p/W)$ is a free $\mathcal{O}_K \otimes_{\mathbb{Z}} W$-module.

4.4.2. The polarization λ induces a perfect alternating pairing $\langle \cdot, \cdot \rangle$ on the free $\mathcal{O}_K \otimes_{\mathbb{Z}} W$-module $H^1_{\mathrm{crys}}(A/W)$, which we identify with $M_0 := \mathcal{O}_K \otimes_{\mathbb{Z}} W$. This pairing induces complex conjugation on $\mathcal{O}_K$ and reduces modulo p to the pairing induced by λ on $\mathbb{H}^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)$. Moreover, there exists a finite flat extension Λ of W such the Hodge filtration

$$0 \to H^0(A, \Omega^1_{A/\overline{\mathbb{F}}_p}) \to \mathbb{H}^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)$$

can be lifted to $M_0 \otimes_W \Lambda$. This follows from the discussion in § 4.3. In fact, the results of that section show that such a lift is uniquely determined by

[1] After this paper was submitted for publication, we were informed by Chia-Fu Yu that this lemma was obtained by him independently. See his paper in *J. Pure Appl. Algebra* 187 (2004), no. 1-3, 305–319.

its generic point, a subspace of $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_p = \oplus_{\{\varphi\colon K \to \overline{\mathbb{Q}}_p\}} \overline{\mathbb{Q}}_p(\varphi)$, consisting of a choice of one subspace out of each pair $\overline{\mathbb{Q}}_p(\varphi) \oplus \overline{\mathbb{Q}}_p(\varphi \circ *)$.

Recall that a CM type Φ of K is a subset of $\mathrm{Hom}(K,\mathbb{C})$ (or of $\mathrm{Hom}(K,\overline{\mathbb{Q}}_p)$) that is disjoint from its complex conjugate, equivalently, a subset that induces $\mathrm{Hom}(K^+, \mathbb{C})$ (or $\mathrm{Hom}(K^+, \overline{\mathbb{Q}}_p)$). A choice of lift of the Hodge filtration provides us with CM type Φ. Let K^* be the reflex field defined by Φ. We see that, in fact, a lift of the Hodge filtration is defined over Λ, where Λ is the compositum of W with the valuation ring of the p-adic reflex field associated to Φ.

4.4.3. Let $V = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{C}$ - a complex vector space on which $\mathcal{O}_K$ acts. Choose a $\mathbb{Z}$-basis $e_1, \dots, e_{2g}$ for $\mathcal{O}_K$ and consider $f_\Phi(\underline{x}) = \det(\sum e_i x_i, \mathrm{Lie}(A))$. This a polynomial in $x_1, \dots, x_{2g}$ with coefficients in $\mathcal{O}_{K^*}$ that depends only on Φ and determines it.

Let $\mathbf{M}\colon \underline{\mathrm{Sch}}_{\mathcal{O}_{K^*}} \to \underline{\mathrm{Sets}}$ be the functor from the category of schemes over $\mathcal{O}_{K^*}$ to the category of sets such that $\mathbf{M}(S)$ is the isomorphism classes of triples $(A/S, \lambda, \iota\colon \mathcal{O}_K \hookrightarrow \mathrm{End}_S(A))$, where $(A/S, \lambda)$ is a principally polarized abelian scheme with CM and $\det(\sum e_i x_i, \underline{\mathrm{Lie}}(A)^*) = f_\Phi(\underline{x})$. That is, the triple $(A/S, \lambda, \iota\colon \mathcal{O}_K \hookrightarrow \mathrm{End}_S(A))$ satisfies the Kottwitz condition [15, § 5] uniquely determined by Φ (with the slight variation of working with $\underline{\mathrm{Lie}}(A)^*$ instead of $\underline{\mathrm{Lie}}(A)$).

For the given point $x = (A, \lambda, \iota) \in \mathbf{M}(\overline{\mathbb{F}}_p)$ we consider the local deformation problem induced by $\mathbf{M}$. This is the functor $\mathbf{N}$ from the category $\mathbf{C}_\Lambda$ of local artinian Λ-algebras with residue field $\overline{\mathbb{F}}_p$ to the category $\underline{\mathrm{Sets}}$ associating to a ring R in $\mathbf{C}_\Lambda$ those elements of $\mathbf{M}(R)$ specializing to x. We remark that the Kottwitz condition is closed under specialization. It is thus fairly standard that $\mathbf{N}$ is pro-represented by a complete noetherian Λ-algebra R^{u}; cf. [20, § 2] and [3, § 4].

4.4.4. Let $\mathbf{G} \to \mathrm{Spec}(\Lambda)$ be the Grassmann variety parameterizing for a scheme $S \to \mathrm{Spec}(\Lambda)$ the set of $\mathcal{O}_K$-invariant, isotropic, locally free, locally direct summands $\mathcal{O}_S$-submodules of rank g of $M_0 \otimes_\Lambda \mathcal{O}_S$ (with the pairing coming from x as above) and satisfying Kottwitz condition f_Φ for a CM type Φ. (In fact, one can deduce that $\mathbf{G} \cong \mathrm{Spec}(\Lambda)$ but we don't need it here.) Let x be the point of $\mathbf{G}$ corresponding to $H^0(A, \Omega^1_{A/\overline{\mathbb{F}}_p}) \to \mathbb{H}^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)$.

Given the results of § 4.4.1, the theory of local models furnishes an isomorphism $\mathcal{O}^\wedge_{\mathbf{G},x} \cong R^u$; cf. [2, § 3], [3, Thm. 4.4.1] – the arguments easily extend to allow a Kottwitz condition. We conclude therefore that there is a triple (A, λ, ι) lifting x defined over the p-adic field $K_1 = \Lambda \otimes \mathbb{Q}$. This concludes the proof of the lemma.

4.4.5. Let K be a primitive quartic CM field. A solution of the embedding problem for p provides us with a triple $(A/\overline{\mathbb{F}}_p, \lambda, \iota) = (E_1 \times E_2/\overline{\mathbb{F}}_p, \lambda = \lambda_1 \times \lambda_2, \iota \colon \mathcal{O}_K \to \mathrm{End}_{\overline{\mathbb{F}}_p}(E_1 \times E_2))$. By Lemma 4.4.1, we may lift $(A/\overline{\mathbb{F}}_p, \lambda, \iota)$ to a triple $(A_0, \lambda_0, \iota_0)$ defined over the ring of integers of some p-adic field K_1 and so, by Lefschetz principle, defined over $\mathbb{C}$. By the theory of complex multiplication $(A_0, \lambda_0, \iota_0)$ is defined over some number field K_2. Since the CM field K is primitive, A_0 is simple and principally polarized. By a theorem of Weil [31] the polarization is defined by a non singular projective genus 2 curve $\mathscr{C}$ and it follows that $A_0 \cong \mathrm{Jac}(\mathscr{C})$ as polarized abelian varieties. Furthermore, $\mathscr{C}$ is defined over a number field K_3 (that is at most a quadratic extension of K_2). By passing to a finite extension L of K_3, we get a stable model.

4.4.6. It remains to explain why $\mathscr{C}$ has bad reduction modulo $\mathfrak{p}$. Let $\mathscr{C}_\mathfrak{p}$ denote the reduction. The polarization on $\mathrm{Jac}(\mathscr{C})$ is defined by the theta divisor $\mathcal{O}_{\mathrm{Jac}(\mathscr{C})}(\mathscr{C})$ and the polarization on $\mathrm{Jac}(\mathscr{C}_\mathfrak{p})$ is the reduction of that of $\mathrm{Jac}(\mathscr{C})$ and hence defined by $\mathcal{O}_{\mathrm{Jac}(\mathscr{C}_\mathfrak{p})}(\mathscr{C}_\mathfrak{p})$. Note that, thus far, the embedding of $\mathscr{C}$ or $\mathscr{C}_\mathfrak{p}$ into the Jacobian is only determined up to translation. On the other hand, the polarization on $\mathrm{Jac}(\mathscr{C}_\mathfrak{p})$ is also given by the reducible divisor $E_1 \times \{0\} + \{0\} \times E_2$. The fact that this implies that $\mathscr{C}_\mathfrak{p}$ is isomorphic to the two elliptic curves E_1, E_2 crossing transversely follows from a theorem Weil [31], but we provide a self contained argument.

Let X/k be an abelian variety over an algebraically closed field k and let K, L be two ample divisors of degree one on X, which are algebraically equivalent. Then, after a suitable translation of L we have $K = L$. Indeed, for a divisor D on X let $\phi_D = \phi_{\mathcal{O}_X(D)}$ denote the associated homomorphism $X \to \mathrm{Pic}^0(X)$, $x \mapsto T_x^*\mathcal{O}_X(D) \otimes \mathcal{O}_X(D)^{-1} = \mathcal{O}_X(T_x^*D - D)$. By assumption, $\phi_{K-L} = 0$. This implies that $\mathcal{O}_X(K - L) \in \mathrm{Pic}^0(\mathrm{X})$, cf. [19, § 8]. Since L is ample, ϕ_L is surjective and so $\mathcal{O}_X(K - L) \cong \mathcal{O}_X(T_x^*L - L)$ for a suitable $x \in X$. It follows that $\mathcal{O}_X(K - T_x^*L)$ is the trivial sheaf. Without loss of generality we may assume that $L = T_x^*L$, and so there exists a rational function f on X such that $(f) = K - L$. But such a function belongs to $\mathcal{O}_X(L)$. By the Riemann-Roch theorem for abelian varieties $\dim H^0(X, \mathcal{O}_X(nL)) = n^g(L^g)/g! = n^g$, since L is ample of degree one [19, § 16]. But then $H^0(X, \mathcal{O}_X(L)) = k$ and it follows that $K = L$.

5. Applications

5.1. A general principle

The following lemma is folklore and easy to prove:

Lemma 5.1.1. — *Let $\pi\colon S \to R$ be a proper scheme over a Dedekind domain R with quotient field H. Let $\mathscr{L} \to S$ be a line bundle on S and $f, g\colon S \to \mathscr{L}$ sections. Let $x \in S(H')$ be a point, where H' is a finite field extension of H. Let $u = (f/g)(x) \in H'$. Let $\mathfrak{p}$ be a prime of R', the integral closure of R in H'. Let $\bar{x}$ be the R'-point corresponding to x. Then $\mathrm{val}_{\mathfrak{p}}(u) < 0$ implies that $\bar{x}$ intersects the divisor of g in the fiber of S over $\mathfrak{p}$.*

Corollary 5.1.2. — *Let $\mathscr{A}_2 \to \mathrm{Spec}(\mathbb{Z})$ be the moduli space of principally polarized abelian surfaces and let*

$$\Theta(\tau) = \frac{1}{2^{12}} \prod_{\substack{(\epsilon,\epsilon')\\ \text{even char.}}} \left(\Theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}(0,\tau)\right)^2. \tag{5.1}$$

Let f be a Siegel modular form with q-expansion $\sum_\nu a(\nu) q^{2\pi i \mathrm{Tr}(\,^t\nu\tau)}$, where ν runs over $g \times g$ semi-integral, semi-definite symmetric matrices. Assume that all the Fourier coefficients $a(\nu) \in \mathcal{O}_L$, the ring of integers of a number field L, and that the weight of f is of the form $10k$, k a positive integer.

Let τ be a point on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$ corresponding to a smooth genus 2 curve $\mathscr{C}$ with CM by the full ring of integers of a primitive CM field K and CM type Φ. Then $(f/\Theta^k)(\tau)$ is an algebraic number lying in the compositum $H_{K^*}L$ of L and the Hilbert class field of the reflex field K^* of (K,Φ). If a prime $\mathfrak{p}$ divides the denominator of $(f/\Theta^k)(\tau)$ then $\mathscr{C}$ has bad reduction modulo $\mathfrak{p}$.

Proof. — The argument is essentially that of [24, § 4.4]: Igusa [13] proved that Θ is a modular form on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$ (see [13, Thm. 3], Θ is denoted there $-2^2\chi_{10}$). It is well known to have weight 10 and a computation shows that its Fourier coefficients are integers and have g.c.d. 1. The q-expansion principle [6, Ch. V, Prop. 1.8] shows that f and Θ^k are sections of a suitable line bundle of the moduli scheme $\mathscr{A}_2 \otimes_{\mathbb{Z}} \mathcal{O}_L$. The value $(f/\Theta^k)(\tau)$ lies in $H_{K^*}L$ by the theory of complex multiplication.

It is classical that the divisor of Θ over $\mathbb{C}$, say D_{gen}, is the locus of the reducible polarized abelian surfaces – those that are a product of elliptic curves with the product polarization. The Zariski closure $D_{\mathrm{gen}}^{\mathrm{cl}}$ of D_{gen} in $\mathscr{A}_2$ is contained in the divisor D_{arith} of Θ, viewed as a section of a line bundle over $\mathscr{A}_2$, and therefore $D_{\mathrm{gen}}^{\mathrm{cl}} = D_{\mathrm{arith}}$, because by the q-expansion principle D_{arith} has no "vertical components". Since $D_{\mathrm{gen}}^{\mathrm{cl}}$ also parameterizes reducible polarized abelian surfaces, it follows that D_{arith} parameterizes reducible polarized abelian surfaces. (Furthermore, it is easy to see by lifting that every reducible polarized abelian surface is parameterized by D_{arith}.) The Corollary thus follows from Lemma 5.1.1. □

Corollary 5.1.3. — *$(f/\Theta^k)(\tau)$ is an S-integer, where S is the set of primes of lying over rational primes p less than $d^2(\mathrm{Tr}(r))^2$ and such that p decomposes in a certain fashion in a normal closure of K as imposed by superspecial reduction* [8, Thms. 1, 2] *(for example, if K is a cyclic Galois extension then p is either ramified or decomposes as $\mathfrak{p}_1\mathfrak{p}_2$ in K).*

5.2. Class invariants

Igusa [11, p. 620] defined invariants $A(u), B(u), C(u), D(u)$ of a sextic $u_0X^6+u_1X^5+\cdots+u_6$, with roots $\alpha_1, \dots, \alpha_6$, as certain symmetric functions of the roots. For example, $D(u) = u_0^{10}\prod_{i<j}(\alpha_i - \alpha_j)^2$ is the discriminant. Igusa also proved that if k is a field of characteristic different from 2, the complement of $D = 0$ in Proj $k[A, B, C, D]$, where A, B, C, D are of weights $2, 4, 6, 10$ respectively, is the coarse moduli space for hyperelliptic curves of genus 2. Moreover, the ring of rational functions is generated by the "absolute invariants" $B/A^2, C/A^3, D/A^5$ (see [12, p. 177], [11, p. 638]). One can choose other generators of course, and for our purposes it makes sense to choose generators with denominator a power of D. Choose then as in [30, p. 313] the generators

$$i_1 = A^5/D, \quad i_2 = A^3B/D, \quad i_3 = A^2C/D.$$

One should note though that these invariants are not known a-priori to be valid in characteristic 2, since Weierstrass points "do not reduce well" modulo 2. The invariants i_n can be expressed in terms of Siegel modular forms thus:

$$i_1 = 2\cdot 3^5\chi_{10}^{-6}\chi_{12}^{5}, \quad i_2 = 2^{-3}\cdot 3^3\psi_4\chi_{10}^{-4}\chi_{12}^{3},$$
$$i_3 = 2^{-5}\cdot 3\psi_6\chi_{10}^{-3}\chi_{12}^{2} + 2^2\cdot 3\psi_4\chi_{10}^{-4}\chi_{12}^{3}.$$

See [12, pp. 189, 195] for the definitions; ψ_i are Eisenstein series of weight i, $-2^2\chi_{10}$ is our Θ.

Another interesting approach to the definition of invariants is the following: Let $I_2 = h_{12}/h_{10}$, $I_4 = h_4$, $I_6 = h_{16}/h_{10}$, $I_{10} = h_{10}$ be the modular forms of weight $2, 4, 6, 10$, respectively, as in [17]. The appeal of this construction is that each h_n is a simple polynomial expression in Riemann theta functions with integral even characteristics $\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]$; for example, $h_4 = \sum_{10}(\Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](0,\tau))^8$, $h_{10} = 2^{12}\Theta$. It is not hard to prove that the g.c.d. of the Fourier coefficients of $\Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](0,\tau)$, for $\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]$ an integral even characteristic, is 1 if $\epsilon \in \mathbb{Z}^2$ (that happens for 4 even characteristics) and 2 if $\epsilon \notin \mathbb{Z}^2$ (that happens for 6 even characteristics). Using that and writing $I_n = */\Theta$, one finds that the numerator of I_n has an integral Fourier expansion. One then lets

$$\mathfrak{j}_1 := I_2^5/2^{-12}I_{10}, \quad \mathfrak{j}_2 := I_2^3I_4/2^{-12}I_{10}, \quad \mathfrak{j}_3 := I_2^2I_6/2^{-12}I_{10}.$$

These are modular functions of the form f/Θ^k, such that the numerator has integral Fourier coefficients. Slightly modifying the definition of [17] (there one uses $j_i := 2^{-12}\mathfrak{j}_i$), we put

$$H_i(X) = \prod_\tau (X - \mathfrak{j}_i(\tau)), \quad i = 1, 2, 3, \tag{5.2}$$

where the product is taken over all $\tau \in \mathrm{Sp}(4,\mathbb{Z})\backslash\mathfrak{H}_2$ such that the associated abelian variety has CM by $\mathcal{O}_K$ (thus all polarizations and CM types appear). We remark that $j_1 = i_1, j_2 = i_2$; this can be verified using the formulas given in [14, p. 848].

The polynomials appearing in Equation (5.2) have rational coefficients that are symmetric functions in modular invariants, viz. the values of the functions $\mathfrak{j}_i$ associated to CM points. As such, it is natural to ask for the prime factorization of these coefficients. For example, the results of [9] give the factorization of the discriminant of the Hilbert class polynomial in the case of imaginary quadratic fields and so provide a bound on the primes which can appear. In [17], it was conjectured that primes dividing the denominators of the coefficients of $H_i(X)$ are bounded by the discriminant of K (note that the only difference between the current definition and loc. cit. is powers of 2). We deduce from the preceding results the following:

COROLLARY 5.2.1. — *The coefficients of the rational polynomials $H_i(X)$ are S-integers where S is the set of primes smaller than $d^2(\mathrm{Tr}(r))^2$ and satisfying a certain decomposition property in a normal closure of K as imposed by superspecial reduction* [8, Thms. 1, 2].

Remark 5.2.2. — Theorem 4.2.1 gives a partial converse to this corollary.

Remark 5.2.3. — We would like to explain the connection between our results and the conjectures of [17] and [1]. In [17], the primes appearing in the denominators of the coefficients of the class polynomials H_i were conjectured to be bounded by the discriminant of K. When K is written in the form $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, with $d > 0$ a fundamental discriminant and $r = a + b\sqrt{d}$ a totally negative element of $\mathbb{Z}[\sqrt{d}]$, the discriminant of K is roughly $d^2(a^2 - b^2d)$ (it certainly divides $2^8d^2(a^2 - b^2d)$). In fact, it was suggested there, based on numerical evidence, that the correct bound on the primes may be a small multiple of $N_{K^+/\mathbb{Q}}d_{K/K^+}$, which is roughly $d_0 = a^2 - b^2d$. Our bound, on the other hand, is $4d^2a^2$, which is larger than $d^2(a^2 - b^2d)$. One therefore expects that our bound can be improved. This is also suggested by the method of our proof, which replaces algebraic identities by metric inequalities.

It is also of much interest to compare the above with the work of Bruinier and Yang [1], which also suggests that our bound can be improved. Their paper considers a CM field K with absolute discriminant p^2q and $K^+ = \mathbb{Q}(\sqrt{p})$, where p, q are primes congruent to 1 modulo 4. To fix ideas, assume that K^+ has strict class number one. Then one finds that $K = \mathbb{Q}(\sqrt{p})(\sqrt{a + b\sqrt{p}})$, where $a + b\sqrt{p}$ is a totally negative element whose norm is q. Conjecture (1.10) of loc. cit. can be applied to the divisor of the pull-back of Θ under the modular map from the Hilbert to the Siegel upper half space, see loc. cit. Remark 9.3. This allows one to conclude after some simple calculations that their conjecture implies that primes in the denominators are bounded by $pq/64$. We should stress though, that we have not attempted to optimize our calculations and possibly a better bound can be drawn from their work.

5.3. Units

Let K be a primitive quartic CM field as before. In [24], de Shalit and the first named author constructed class invariants $u(\Phi; \mathfrak{a})$, $u(\Phi; \mathfrak{a}, \mathfrak{b})$, associated to certain ideals of K and a CM type Φ. The construction essentially involves the evaluation of Θ at various CM points associated to K. Though the construction is general, we recall it here only under very special conditions. For the general case, refer to loc. cit.

Example 5.3.1. — Assume that K is a cyclic CM field with odd class number h_K and that $h_{K^+} = 1$. Let Φ be a CM type of K and assume that the different ideal $\mathcal{D}_{K/\mathbb{Q}} = (\delta)$ with $\overline{\delta} = -\delta$ and $\mathrm{Im}(\varphi(\delta)) > 0$ for $\varphi \in \Phi$.

Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ and choose $a \in K^+, a \gg 0$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (a)$. The form $\langle f, g\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\overline{f}g/a\delta)$ induces a principal polarization on $\mathbb{C}^2/\Phi(\mathfrak{a})$. Write the lattice $\Phi(\mathfrak{a})$ as spanned by the symplectic basis formed by the columns of $(\omega_1\ \omega_2)$ and consider $\Delta(\Phi(\mathfrak{a})) := \det(\omega_2)^{-10}\Theta(\omega_2^{-1}\omega_1)$. It depends only on $\Phi, \mathfrak{a}$ and not on a. One then lets

$$u(\Phi;\mathfrak{a}) = \frac{\Delta(\Phi(\mathfrak{a}^{-1}))}{\Delta(\Phi(\mathcal{O}_K))}, \qquad u(\Phi;\mathfrak{a},\mathfrak{b}) = \frac{u(\Phi;\mathfrak{a}\mathfrak{b})}{u(\Phi;\mathfrak{a})u(\Phi;\mathfrak{b})}. \tag{5.3}$$

See [24, § 1.3] for remarkable properties of these invariants. In particular, if h_K is a prime different from 5 the group generated by the $u(\Phi;\mathfrak{a},\mathfrak{b})$ in $H_K^\times$ has rank $h_K - 1$. The following corollary holds in general.

Corollary 5.3.2. — *The invariants $u(\Phi;\mathfrak{a},\mathfrak{b})$ are S-units for S the set of primes of H_{K^*} that lie over rational primes p smaller than $d^2(\mathrm{Tr}(\delta^2))^2$ such that p decomposes in a certain fashion in a normal closure of K as imposed by superspecial reduction* [8, Thms. 1,2].

6. Appendix: Numerical data

6.1. Class polynomials

Let $K = \mathbb{Q}[x]/(x^4 + 50x^2 + 93)$ be the non-normal quartic CM field of class number 4 generated by $i\sqrt{25 + 2\sqrt{133}}$ over its totally real subfield $K_0 = \mathbb{Q}(\sqrt{133})$. The field discriminant of K is $d_K = 3 \cdot 31 \cdot 133^2$ and the norm of the relative discriminant is 93. The reflex field of K is the quartic CM field $K^* = \mathbb{Q}[x]/(x^4 + 100x^2 + 2128)$, and it also has class number 4. The Igusa class polynomials for K have degree 8, and the first one, $H_1(X)$, has denominators which factor as:

$$7^{48} \cdot 11^{72} \cdot 19^{24} \cdot 23^{12} \cdot 29^{12} \cdot 83^{12} \cdot 89^{12} \cdot 167^{12}.$$

Note that for the first Igusa invariant, χ_{10} appears to the sixth power in the denominator, which agrees with the fact that all powers are a multiple of 6. To give an idea of the size, the numerator of the constant term factors as:

$$2^{224} \cdot 3^{20} \cdot 23^{15} \cdot (53 \cdot 1508303 \cdot 54586453 \cdot 38280141661140007 \\ \cdot 1375394310638387387)^5.$$

The other two class polynomials are not given here, as they have the same primes in their denominators. The polynomials were computed using PARI with 1000 digits of precision in about 8 hours each on an Intel Pentium 4, 2.2GHZ, 512MB memory.

The algorithm used to compute the Igusa class polynomials is given in [30], [32], and [17]. Roughly speaking, the algorithm works by listing ideal classes in $\mathcal{O}_K$ and computing for each ideal class and CM type the period matrices associated to the corresponding abelian variety with its principal polarization(s) (as in [26, Section 4.2 and p. 62]). The Siegel modular functions are then evaluated, to some amount of precision, at each of the period matrices, and the minimal polynomial of the Igusa invariants is formed. To recognize the coefficients of the minimal polynomial as rational numbers, the continued fraction algorithm is used.

If enough precision is used in the computation, then the algorithm succeeds, but a bound on the size of the denominators is needed to determine the amount of precision necessary. For primes satisfying mild ramification conditions, the first named author has obtained bounds on the powers of the primes appearing in the denominators of the Igusa class polynomials and the class invariants of § 5.3. This will be published elsewhere. Together with the bound given here on the primes, this provides a bound on the denominators. In practice, the resulting triple of Igusa class polynomials are checked by taking triples of roots modulo a prime ℓ which splits completely in K (and into principal ideals in K^*, the reflex field of K), generating the genus 2 curve over $\mathbb{F}_\ell$ with those invariants using Mestre's algorithm, and checking that a point on the Jacobian is killed by one of the group orders predicted for the Jacobian of a curve over $\mathbb{F}_\ell$ with CM by K.

6.2. Curves with bad reduction

To illustrate the theory we give an example of a CM field K and two genus 2 curves over $\mathbb{Q}$ with CM by K. We list their invariants, and verify that they have bad reduction at the primes in the denominators of the invariants. In [30], van Wamelen gives a complete list of all isomorphism classes of genus 2 CM curves defined over the rationals along with their Igusa invariants. For example, for the cyclic CM field $K = \mathbb{Q}(i\sqrt{13 - 3\sqrt{13}})$ of class number 2, there are two non-isomorphic genus 2 curves defined over $\mathbb{Q}$.

The curve with invariants equal to

$$\begin{aligned}
i_1 &= \frac{2\cdot 11^5\cdot 53^5\cdot 6719^5\cdot 30113^5}{3^7\cdot 23^{12}\cdot 131^{12}},\\
i_2 &= \frac{2\cdot 5\cdot 11^3\cdot 53^3\cdot 6719^3\cdot 7229\cdot 30113^3}{3^3\cdot 23^8\cdot 131^8},\\
i_3 &= \frac{2\cdot 11^2\cdot 19\cdot 53^2\cdot 6719^2\cdot 30113^2\cdot 237589628623651}{3^4\cdot 23^8\cdot 131^8},
\end{aligned}$$

has an affine model

$$\begin{aligned}
y^2 = -70399443x^6 + 36128207x^5 + 262678342x^4 - 48855486x^3\\
- 112312588x^2 + 36312676x.
\end{aligned}$$

The reduction of a genus 2 curve at a prime can be calculated using [18, Thm. 1, p. 204]. For these examples we actually calculated the reduction using the genus 2 reduction program written by Liu. The output of the program shows that at the primes $p = 2, 3, 23, 131$, the curve has potential stable reduction equal to the union of two supersingular elliptic curves E_1 and E_2 intersecting transversally at one point.

The second curve has invariants equal to

$$\begin{aligned}
i_1 &= \frac{2\cdot 7^{10}\cdot 11^5\cdot 21059^5}{3^7\cdot 23^{12}},\\
i_2 &= \frac{2\cdot 5\cdot 7^7\cdot 11^3\cdot 8387\cdot 21059^3}{3^3\cdot 23^8},\\
i_3 &= \frac{2\cdot 7^6\cdot 11^2\cdot 21059^2\cdot 71347\cdot 739363}{3^4\cdot 23^8},
\end{aligned}$$

and has an affine model

$$y^2 = -243x^6 + 2223x^5 - 1566x^4 - 19012x^3 + 903x^2 + 19041x - 5882.$$

In this case, the output of the genus 2 reduction program shows that at the primes $p = 2, 3, 23$, the curve has potential stable reduction equal to the union of two supersingular elliptic curves E_1 and E_2 intersecting transversally at one point.

The reader may have noticed that 2 does not appear in the denominator of the invariants. This is not due to the invariants i_n being divisible by 2. It is an artifact of cancellation between "values of the numerator and the denominator" and explains in which sense Theorem 4.2.1 may fail to provide a converse to Corollary 5.1.2. In fact, bad reduction of CM curves modulo primes over 2 turns out to be prevalent. According to [10], there is no smooth superspecial curve in characteristic 2. On the other hand, using complex multiplication, one can prove (e.g. for cyclic CM fields K and primes decomposing as $(p) = \mathfrak{p}_1\mathfrak{p}_2$ or $(p) = \mathfrak{p}_1^2$) superspecial reduction of principally polarized abelian surfaces with CM by K (cf. [8]). This implies for $p = 2$ bad reduction of the corresponding curve.

6.3. Class invariants

In his McGill M.Sc. thesis, Daniel Vallieres calculated for the first time numerical examples of the class invariants appearing in § 5.3. With his kind permission, we provide an example here; many more appear in [28]. As one may expect, such invariants are rarely units. For an explanation of this phenomena see [7]. The same remarks concerning the validity of the calculations made in § 6.1 apply here. The field K we consider is $\mathbb{Q}(\sqrt{-15+6\sqrt{5}})$. Its discriminant is $2^4 \cdot 3^2 \cdot 5^3$. This field has class group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and we denote by $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideals representing its non-zero elements. For a suitable choice of these ideals and a CM type Φ, the data is given in the following table. All minimal polynomials split in $K^+ = \mathbb{Q}(\sqrt{5})$. The prime 31 splits in K^+ as $(31) = \mathfrak{p}_{31,1}\mathfrak{p}_{31,2}$.

invariant	minimal polynomial	factorization of $u(\Phi;\mathfrak{x},\mathfrak{y})$ in $\mathbb{Q}(\sqrt{5})$
$u(\Phi;\mathfrak{a},\mathfrak{a})$	$t^2 - \frac{10155047}{923521}\cdot t + \frac{1}{923521}$	$\mathfrak{p}_{31,1}^{-4}$
$u(\Phi;\mathfrak{a},\mathfrak{b})$	$t - \frac{1}{961}$	$\mathfrak{p}_{31,1}^{-2}\mathfrak{p}_{31,2}^{-2}$
$u(\Phi;\mathfrak{a},\mathfrak{c})$	$t^2 - \frac{10155047}{961}\cdot t + 1$	$\mathfrak{p}_{31,1}^{-2}\mathfrak{p}_{31,2}^{2}$
$u(\Phi;\mathfrak{b},\mathfrak{b})$	$t^2 - \frac{20809922}{923521}\cdot t + \frac{1}{923521}$	$\mathfrak{p}_{31,2}^{-4}$
$u(\Phi;\mathfrak{b},\mathfrak{c})$	$t^2 - \frac{20809922}{961}\cdot t + 1$	$\mathfrak{p}_{31,1}^{2}\mathfrak{p}_{31,2}^{-2}$
$u(\Phi;\mathfrak{c},\mathfrak{c})$	$t^2 - 228826127\cdot t + 1$	1 (unit)

We remark that already in [28] one finds invariants with 7 primes in their decomposition, and based on [7] the number of primes is expected to be arbitrarily large when the discriminants of K and K^+ grow. Also, as previously mentioned, in general the invariants $u(\Phi;\mathfrak{a},\mathfrak{b})$ generate nontrivial ray class fields of K.

Acknowledgments. — We would like to thank Ehud de Shalit and Payman Kassaei for valuable discussions. The first named author's research was partially supported by NSERC; he would like to thank Microsoft Research for its hospitality during a visit where this project took shape. The second named author thanks Tonghai Yang for many stimulating discussions and McGill University for its hospitality.

BIBLIOGRAPHY

[1] J. H. Bruinier & T. Yang, "CM-values of Hilbert modular functions", *Invent. Math.* **163** (2006), no. 2, p. 229-288.

[2] P. Deligne & G. Pappas, "Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant", *Compositio Math.* **90** (1994), no. 1, p. 59-79.

[3] T. Dokchitser, *Deformations of p-divisible groups and p-descent on elliptic curves*, Memoir, Utrecht, 2000.

[4] D. R. Dorman, "Singular moduli, modular polynomials, and the index of the closure of $\mathbf{Z}[j(\tau)]$ in $\mathbf{Q}(j(\tau))$", *Math. Ann.* **283** (1989), no. 2, p. 177-191.

[5] A. K. Eisenträger & K. E. Lauter, "A CRT algorithm for constructing genus 2 curves over finite fields", to appear in Proceedings of Arithmetic, Geometry and Coding Theory (AGCT 2005).

[6] G. Faltings & C.-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990, With an appendix by David Mumford.

[7] E. Z. Goren & K. E. Lauter, "Evil primes and superspecial moduli", *International Mathematics Research Notices* **2006** (2006), p. 1-19, Article ID 53864.

[8] E. Z. Goren, "On certain reduction problems concerning abelian surfaces", *Manuscripta Math.* **94** (1997), no. 1, p. 33-43.

[9] B. H. Gross & D. B. Zagier, "On singular moduli", *J. Reine Angew. Math.* **355** (1985), p. 191-220.

[10] T. Ibukiyama, T. Katsura & F. Oort, "Supersingular curves of genus two and class numbers", *Compositio Math.* **57** (1986), no. 2, p. 127-152.

[11] J.-i. Igusa, "Arithmetic variety of moduli for genus two", *Ann. of Math. (2)* **72** (1960), p. 612-649.

[12] ———, "On Siegel modular forms of genus two, I", *Amer. J. Math.* **84** (1962), p. 175-200.

[13] ———, "On Siegel modular forms of genus two, II", *Amer. J. Math.* **86** (1964), p. 392-412.

[14] ———, "Modular forms and projective invariants", *Amer. J. Math.* **89** (1967), p. 817-855.

[15] R. E. Kottwitz, "Points on some Shimura varieties over finite fields", *J. Amer. Math. Soc.* **5** (1992), no. 2, p. 373-444.

[16] S. Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften, vol. 255, Springer-Verlag, New York, 1983.

[17] K. E. Lauter, "Primes in the denominators of Igusa class polynomials", Preprint, Available from `http://www.arxiv.org/abs/math.NT/0301240`, 2003.

[18] Q. Liu, "Courbes stables de genre 2 et leur schéma de modules", *Math. Ann.* **295** (1993), no. 2, p. 201-222.

[19] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[20] F. Oort, "Finite group schemes, local moduli for abelian varieties, and lifting problems", *Compositio Math.* **23** (1971), p. 265-296.

[21] A. Pizer, "An algorithm for computing modular forms on $\Gamma_0(N)$", *J. Algebra* **64** (1980), no. 2, p. 340-390.

[22] M. Rapoport, "Compactifications de l'espace de modules de Hilbert-Blumenthal", *Compositio Math.* **36** (1978), no. 3, p. 255-335.

[23] F. Rodriguez-Villegas, "Explicit models of genus 2 curves with split CM", in *Algorithmic number theory (Leiden, 2000)*, Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, p. 505-513.

[24] E. de Shalit & E. Z. Goren, "On special values of theta functions of genus two", *Ann. Inst. Fourier (Grenoble)* **47** (1997), no. 3, p. 775-799.

[25] G. Shimura & Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[26] A.-M. Spallek, "Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen", PhD Thesis, Universität Gesamthochschule Essen, 1994.

[27] B. K. Spearman & K. S. Williams, "Relative integral bases for quartic fields over quadratic subfields", *Acta Math. Hungar.* **70** (1996), no. 3, p. 185-192.

[28] D. Vallières, *Class Invariants*, Memoir, McGill, October 2005, Available from `http://www.math.mcgill.ca/goren/Students/students.html`.

[29] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.

[30] P. van Wamelen, "Examples of genus two CM curves defined over the rationals", *Math. Comp.* **68** (1999), no. 225, p. 307-320.

[31] A. Weil, "Zum Beweis des Torellischen Satzes", *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.* **1957** (1957), p. 33-53.

[32] A. Weng, "Constructing hyperelliptic curves of genus 2 suitable for cryptography", *Math. Comp.* **72** (2003), no. 241, p. 435-458 (electronic).

Manuscrit reçu le 20 juin 2005,
révisé le 1^{er} mai 2006,
accepté le 22 août 2006.

Eyal Z. GOREN
McGill University
Department of Mathematics and Statistics
805 Sherbrooke St. W.
Montreal H3A 2K6, QC (Canada)
goren@math.mcgill.ca

Kristin E. LAUTER
Microsoft Research
One Microsoft Way
Redmond, WA 98052 (USA)
klauter@microsoft.com