AN EXPPLICIT VERSION OF SHIMURA'S RECIPROCITY LAW
FOR SIEGEL MODULAR FUNCTIONS

MARCO STRENG

Abstract. We give an explicit version of Shimura's reciprocity law for singular values of Siegel modular functions. We use this to construct the first examples of class invariants of quartic CM fields that are smaller than Igusa invariants. Our version also enabled a new proof of Shimura's reciprocity law by Tonghai Yang.

1. Introduction

The values of the modular function \( j \) in imaginary quadratic numbers \( \tau \) generate abelian extensions of imaginary quadratic fields \( K = \mathbb{Q}(\tau) \). These values \( j(\tau) \) enable explicit computation of the Hilbert class field of \( K \) and of elliptic curves over finite fields with a prescribed number of points (the "CM method") for primality testing and cryptography.

However, these algebraic numbers \( j(\tau) \) have very large height, which limits their usefulness in such applications. So we consider other modular functions \( f \) instead, whose values are again abelian over \( K \), hoping to find numbers of smaller height. If these values \( f(\tau) \) lie in the same field as \( j(\tau) \), then we call them class invariants, and they can take the place of \( j(\tau) \) in applications, which leads to great speed-ups [10].

The values \( f(\tau) \) are acted upon by ideals (and id` eles) of \( K \) via the Artin isomorphism. Shimura’s reciprocity law expresses this action in terms of an action on the modular functions \( f \) themselves, and an explicit version of this reciprocity law \([23, 54]\) allows one to search for class invariants in a systematic way.

There exists a higher-dimensional CM method, with applications in hyperelliptic curve cryptography and a more general analytic construction of class fields \([11, 53]\). A significant speedup will be obtained by replacing the Igusa invariants in this construction by smaller class invariants.

Shimura gave various higher-dimensional analogues of his reciprocity law \([41–45, 47]\). Our main result (Theorems 2.4, 2.5, and 2.9 below) is a new and explicit version, suitable for finding class invariants in the higher-dimensional setting.

We use our explicit formulation of Shimura’s reciprocity law to find the first examples of small class invariants of quartic CM fields (Section 7). Our formulation of Shimura’s reciprocity law also inspired a new proof of Shimura’s reciprocity law by Tonghai Yang \([65, \text{Section 4, see also Acknowledgements}]\). As a third application, Andreas Enge and the author \([18]\) use the explicit reciprocity law for generalizing Schertz’s work on class invariants \([10]\) to higher dimension.

1.1. Summary of results. Let \( \mathcal{F}_N \) be the field of Siegel modular functions of level \( N \) over \( \mathbb{Q}(\zeta_N) \) (c.f. (2.2)). Let \( f \in \mathcal{F}_N \) be such a function. Let \( \tau \in \mathbb{C}^{g \times g} \) be
a symmetric matrix with positive definite imaginary part (that is, a point in the Siegel upper half space $H_g$). If $\tau$ is a primitive CM point (Section 2.5), then $f(\tau)$ is an algebraic number and is in fact abelian over a field known as the reflex field $K_\tau$ (Section 2.6).

Now given $\sigma \in \text{Gal}(\overline{Q}/K_\tau)_{ab}$, there are various reasons why we would like to be able to compute $f(\tau^\sigma)$. For example, it allows us to decide whether $f(\tau)$ is in certain subfields of $\overline{Q}$ and to find its minimal polynomial over $K_\tau$. This minimal polynomial can be used to speed up explicit class field theory and explicit CM constructions of curves and Jacobians [17, 60].

Shimura’s reciprocity law [41–45, 47] expresses $f(\tau^\sigma)$ in the form $F(\tau)$ where $F$ is obtained from $f$ and $\sigma$. The function $F$ is obtained in terms of an action of an uncountable adelic group, which is not very helpful in computation. So in order to use such actions, one needs to approximate the adelic group elements by products of elements in particular subgroups. We did this, and the result is an explicit reciprocity law in terms of ideals and ray class groups, rather than idèle class groups.

Let $a$ be an ideal. Then Theorem 2.4 gives (in terms of $a$ and $\tau$) efficiently computable $U \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ and $\tau' \in H_g$ with

$$f(\tau)^a = f^U(\tau').$$

In turn, the action of $U$ on $\mathcal{F}_N$ can be computed in one of the various practical ways explained in Section 2.3. Moreover, we can make sure that $\tau'$ is in a fundamental region (Section 2.5.2), allowing for efficient numerical evaluation of $f^U(\tau')$.

We use this reciprocity law to prove (Theorem 2.5) a formula for the ideal group corresponding to the abelian extension

$$\mathcal{H}(N) = K^\tau(f(\tau) : f \in \mathcal{F}_N) \text{ of } K^\tau.$$

Computations with $f(\tau)$ become even more efficient when it is real instead of complex. Proposition 2.14 gives a sufficient condition for this to happen.

The author has implemented the actions in SageMath [55] (which uses PARI [61]) and made the program available online at [57].

1.2. Overview of content. Section 2 states the results and Sections 3–5 contain a proof. The action of $U$ in (1.1) becomes most explicit when expressing the function $f$ in terms of theta constants, see Section 6.

Section 7 gives a detailed example of how to obtain useful class invariants.

Finally, Section 8 gives applications to computational class field theory and to the construction of curves over finite fields. The final three sections (6–8) can be read independently of Sections 3–5.

2. Definitions and statement of the main results

2.1. The upper half space. Fix a positive integer $g$. The Siegel upper half space $H_g$ is the set of $g \times g$ symmetric complex matrices with positive definite imaginary part. It parametrizes $g$-dimensional principally polarized abelian varieties $A$ over $\mathbb{C}$ together with a symplectic basis $b_1, \ldots, b_{2g}$ of their first homology.

In more detail, every abelian variety over $\mathbb{C}$ is of the form $A = \mathbb{C}^g/\Lambda$ for a lattice $\Lambda$ of rank $2g$. A polarization is given by a Riemann form, i.e., an $\mathbb{R}$-bilinear form $E$ on $\mathbb{C}^g$ that restricts to an alternating bilinear form $\Lambda \times \Lambda \to \mathbb{Z}$ such that $(u, v) \mapsto E(u, v)$ is symmetric and positive definite. Given a $\mathbb{Z}$-basis of $\Lambda$, there is a $2g \times 2g$ matrix, which by abuse of notation we also denote by $E$, such that $E(u, v) = u^t E v$. We say that $E$ is principal if it has determinant 1. In that
case, there exists a symplectic basis, i.e., a basis such that \( E \) is given in terms of \((g \times g)\)-blocks as
\[
E = \Omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.
\]
To a point \( \tau \in \mathbf{H}_g \), we associate the principally polarized abelian variety with \( \Lambda = \tau \mathbb{Z}^g + \mathbb{Z}^g \) and symplectic basis \( \tau e_1, \ldots, \tau e_g, e_1, \ldots, e_g \), where \( e_i \) is the \( i \)-th standard basis element of \( \mathbb{Z}^g \). Conversely, given a principally polarized abelian variety and a symplectic basis, we can apply a \( \mathbf{C} \)-linear transformation of \( \mathbf{C}^g \) to write it in this form (see Chapter 8).

2.2. The algebraic groups. Given a commutative ring \( R \), let
\[
\text{GSp}_{2g}(R) = \{ A \in R^{2g \times 2g} : A^t \Omega A = \nu \Omega \text{ with } \nu \in R^\times \}.
\]
Note that \( \nu \) defines a homomorphism of algebraic groups \( \text{GSp}_{2g} \rightarrow \mathbf{G}_m \), and denote its kernel by \( \text{Sp}_{2g} \). For \( g = 1 \), we have simply \( \text{GSp}_2 = \text{GL}_2, \nu = \det, \text{Sp}_2 = \text{SL}_2 \).

The homomorphism \( \nu \) has a section \( i \), satisfying \( \nu \circ i = \text{id}_{\mathbf{G}_m} \), given by
\[
i(t) = \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix}.
\]
For any ring \( R \) for which this makes sense, we also define
\[
\text{GSp}_{2g}(R)^+ = \{ A \in \text{GSp}_{2g}(R) : \nu(A) > 0 \}.
\]
The group \( \text{GSp}_{2g}(R)^+ \) acts on \( \mathbf{H}_g \) by
\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1},
\]
where \( a, b, c, d \) are \((g \times g)\)-blocks. Changes of symplectic bases correspond to the action of \( \text{Sp}_{2g}(\mathbb{Z}) \subset \text{GSp}_{2g}(R)^+ \) on \( \mathbf{H}_g \) (see Lemma 4.7 below), leading to the well-known fact that \( \text{Sp}_{2g}(\mathbb{Z}) \backslash \mathbf{H}_g \) parametrizes the set of isomorphism classes of principally polarized abelian varieties of dimension \( g \).

The natural map \( \text{Sp}_{2g}(\mathbb{Z}) \rightarrow \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \) is surjective [39 Thm. VII.21]. Its kernel \( \Gamma_N \) is called the principal congruence subgroup of level \( N \).

2.3. Modular forms and group actions. A Siegel modular form of weight \( k \) and level \( N \) is a holomorphic function \( f : \mathbf{H}_g \rightarrow \mathbf{C} \) such that for all \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_N \), we have \( f(A\tau) = \det(c\tau + d)^k f(\tau) \), and which is “holomorphic at the cusps”. We will not define holomorphicity at the cusps, as it is automatically satisfied for \( g > 1 \) by the Koecher principle [31], and is a textbook condition for \( g = 1 \).

Every Siegel modular form \( f \) has a Fourier expansion or \( q \)-expansion
\[
f(\tau) = \sum_\xi a_\xi q^\xi, \quad a_\xi \in \mathbf{C}, \quad q^\xi := \exp(2\pi i \text{Tr}(\xi\tau)/N),
\]
where \( \xi \) runs over the symmetric matrices in \( \frac{1}{2}\mathbb{Z}^{g \times g} \) with integral diagonal entries. The numbers \( a_\xi \) are the coefficients of the \( q \)-expansion.

Let \( \mathcal{F}_N \) be the field
\[
\mathcal{F}_N = \left\{ \frac{g_1}{g_2} : \text{g}_1 \text{ are Siegel modular forms of equal weight and level } N, \text{ with } q \text{-expansion coefficients in } \mathbf{Q}(\xi_N), \text{ and } g_2 \neq 0 \right\}.
\]

\(^1\)Warning: our \( i \) differs from Shimura’s \( i \) in the sense that \( i(t) = i(t)^{-1} \). We made our choice in such a way that \( i \) is a section of \( \nu \), where \( \nu \) generalizes the determinant.
Proposition 2.1. There is a right action of $\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{F}_N$ given as follows. For $A \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$, let $t = \nu(A)$ and $B = i(t)^{-1}A$. Then

$$f^A = (f^{i(t)})^B,$$

where we have:

1. For $B \in \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$, let $\tilde{B} \in \text{Sp}_{2g}(\mathbb{Z})$ be such that $B = (\tilde{B} \mod N)$. Then $f^B(\tau) = f(\tilde{B}\tau)$ for all $f \in \mathcal{F}_N$.

2. For $t \in (\mathbb{Z}/N\mathbb{Z})^\times$, the matrix $i(t)$ acts by the natural Galois action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $q$-expansion coefficients, that is, if

$$f = \frac{\sum_{\xi,k} a(\xi,k)q^\xi}{\sum_{\xi,k} b(\xi,k)q^\xi} \in \mathcal{F}_N$$

with $a(\xi,k), b(\xi,k) \in \mathbb{Q}$, then

$$f^{i(t)} = \frac{\sum_{\xi,k} a(\xi,k)q^{kt\xi}}{\sum_{\xi,k} b(\xi,k)q^{kt\xi}}.$$

We give detailed references in Section 4.

Remark 2.2. As it is a group action, the action also satisfies $f^A = (f^{B'})^{i(t)}$ for $B' = A(i(t))^{-1} = i(t)Bi(t)^{-1}$.

2.4. Computing the group action. We highlight four ways in which, given $A \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$, $f \in \mathcal{F}_N$, and $\tau$, we could compute $f^A$ or $f^A(\tau)$.

1. From the definition. The most obvious is to use (1) and (2) directly.

First take $t = \nu(A)$, and write $A = i(t)B$ with $B = i(t)^{-1}A \in \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$. Next, compute a lift $\tilde{B} \in \text{Sp}_{2g}(\mathbb{Z})$ of $B$. This can be done by following the steps of the proof of [39] Thm. VII.21. Alternatively, one could compute a lift by expressing $B$ as a product of standard generators of $\text{Sp}_{2g}(\mathbb{Z})$ (in fact, in the case $g = 1$, this results in explicit formulas as in [22] Lemma 6).

Then we compute $f^{i(t)}$ and evaluate it at $\tilde{B}\tau$. The disadvantage of this method in practice is that while $\tau$ can often be engineered to be in a fundamental region where modular functions converge quickly, we have no control over $\tilde{B}\tau$.

For this reason, we will not take this approach, and we promote the methods 2–4 instead.

2. Using theta functions. The function $f \in \mathcal{F}_N$ has an expression as a rational function of of theta constants. If such an expression is known, then we can use a direct formula for the action of $\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ on $f$, which does not even require finding a lift to $\text{Sp}_{2g}(\mathbb{Z})$. We give this formula in Section 4 and use it in all our examples in Section 5.

3. By selecting $f$ in such a way that the action is easy. It is sometimes possible to choose $f$ that are fixed by the block-lower-triangular matrices in $\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ and to choose $\tau$ such that $A$ is block-lower-triangular, in which case we have $f^A = f$. Enge and the author take this approach in [18].

4. Using the moduli interpretation. In some cases, one could use the moduli interpretation of $f$. We do not follow this approach in the present article, but we do illustrate it with the following example.

Example 2.3. For $g = 1$ and $N = 2$, we have $\mathcal{F}_2 = \mathbb{Q}(\lambda)$, where $\lambda$ is the Legendre invariant given as follows. To an $\mathbb{R}$-basis $\omega_1, \omega_2$ of $\mathbb{C}$ with $\tau = \omega_1/\omega_2 \in \mathbb{H}_1$, we associate the lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, the elliptic curve $E(\mathbb{C}) = \mathbb{C}/\Lambda$, and the isomorphism $\phi : F^2 \rightarrow E[2] : v \mapsto \left(\frac{1}{2}(v \cdot (\omega_1, \omega_2)) \mod \Lambda\right)$. Let $e_1 = (1,0)$,
For a short Weierstrass model of $E$ with coordinates $x$ and $y$, let $x_1 = x(\phi(e_1))$. Then we define
\[ \lambda(\tau) = \frac{x_3 - x_1}{x_2 - x_1}. \]

The group $GSp_2(F_2) = SL_2(F_2)$ acts on $F^2_2$ by permutation of $e_1$, $e_2$ and $e_3$. In other words, we have the isomorphism $\sigma : GSp_2(\mathbb{Z}/2\mathbb{Z}) \to S_3$ given by $\sigma e_i = e_{\sigma(i)}$ for $i = 1, 2, 3$.

Writing $\lambda_1 := 0$, $\lambda_2 := 1$, $\lambda_3 := \lambda \in J_2$, we claim that the action of Proposition 2.1 is
\[ \lambda^A = \frac{\lambda_{\rho(3)} - \lambda_{\rho(1)}}{\lambda_{\rho(2)} - \lambda_{\rho(1)}}, \quad \text{where} \quad \rho = \sigma(A'). \]

As special cases, we have
\[ \lambda(\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}) = \frac{0 - \lambda}{1 - \lambda} = \frac{\lambda}{\lambda - 1} \quad \text{and} \quad \lambda(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}) = \frac{\lambda - 1}{0 - 1} = 1 - \lambda. \]

To prove the claim, given $A$ and $\tau$, let $\tilde{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a lift of $A$ and consider $\left(\omega_1', \omega_2'\right) = (\omega_1, \omega_2)\tilde{A}^t$ and $\tau' = \omega_1'/\omega_2' = \tilde{A}\tau$, which leads to $\phi' = \phi \circ A'$. Choose the Weierstrass equation of $E = E'$ in such a way that $x_i = \lambda_i$. Then $x_i' = x(\phi'(e_i)) = x(\phi'(e_i)) = x(\phi(e_i))$, hence $\lambda^A(\tau) = \lambda(\tau')$ is indeed given by (2.3).

With Rosenhain invariants and the appropriate isomorphism $GSp_2(F_2) \cong S_6$, one would get the same kind of formulae for $q = N = 2$.

We hope that similar formulae can be obtained for other small values of $g$ and $N$ on a case-by-case basis.

2.5. Complex multiplication. A primitive CM point in $H_g$ is a point such that the endomorphism algebra $\text{End}(A) \otimes \mathbb{Q}$ of the corresponding principally polarised abelian variety $(A, E)$ is a number field $K$ of degree $2g$. We now explain what they look like and how to compute them.

2.5.1. Primitive CM points. All primitive CM points are of the following form. For details, see [33, §1.3, Thms. 1.4.1, 1.4.5]. Let $K$ be a CM field of degree $2g$, that is, a totally imaginary quadratic extension of a totally real number field of degree $g$. Let $\Phi = \{\phi_1, \ldots, \phi_g\}$ be a CM type, that is, a set of $g$ embeddings $K \to C$ such that no two are complex conjugate. By abuse of notation, write $\Phi(x) = (\phi_1(x), \ldots, \phi_g(x)) \in C^g$ for $x \in K$. Let $b$ be a lattice in $K$, that is, a non-zero fractional ideal of an order of $K$. Let $\xi \in K$ be such that for all $\phi \in \Phi$, the complex number $\phi(\xi)$ lies on the positive imaginary axis, and such that the bilinear form $E_\xi : K \times K \to \mathbb{Q} : (x, y) \mapsto \text{Tr}(\mathbf{7}g\xi)$ maps $b \times b$ to $\mathbb{Z}$. Take $A = C^g / \Phi(b)$ and let a polarization on $A$ be given by $E_\xi$ extended $\mathbb{R}$-linearly from $b$ to $C^g$. Finally, let $\mathcal{O} = \{x \in K : x\mathcal{B} \subset \mathcal{B}\}$ be the multiplier ring of $b$, and embed it into $\text{End}(A)$ by taking $x\Phi(u) = \Phi(xu)$ and extending this linearly. We find an embedding $K \to \text{End}(A) \otimes \mathbb{Q}$. Let $B$ be a symplectic basis of $b$ for the pairing $E_\xi$. Then we get a point
\[ \tau = (\Phi(b_{g+1}) \cdots \Phi(b_2))^{-1}(\Phi(b_1)) \cdots (\Phi(b_g)) \in H_g. \]

We denote this point also by $\tau(\Phi, b, \xi, B)$ or simply by $\tau(\Phi, B)$. It is a primitive CM point if and only if $A$ is simple, which happens if and only if $\Phi$ is primitive, that is, if and only if $\Phi_{|K'}$ is not a CM type for any CM subfield $K' \subset K$. Moreover, all primitive CM points are of this form.

We will make the reciprocity law explicit in terms of the quadruples $(\Phi, b, \xi, B)$. 

2.5.2. Computing the primitive CM points. Given $K$, we can find representatives $(\Phi, b, \xi)$ for all isomorphism classes of principally polarized abelian varieties with CM by $\mathcal{O}_K$ using van Wamelen’s algorithm [52, Algorithm 1]. For a version of this algorithm without duplicates, see [58, Algorithm 4.12].

A symplectic basis $B$ can be computed using classical methods that are available as E.symplectic_form() in SageMath [55] or the FrobeniusFormAlternating function in Magma [7]. See also [58, Algorithm 5.2].

Together, this gives a method for finding all CM points for $\mathcal{O}_K$, and we implemented this as CM_Field(...) . period_matrices() in [57], which returns CM points in the form of SageMath objects tau that include the data of $\Phi$, $b$, $\xi$, and the basis $B$ and can produce arbitrary-precision approximations of $\tau$.

In practical computations, one wants to take $B$ such that numerical formulas for modular forms converge quickly when evaluated in $\tau$. This can be done by first taking $B$ arbitrary and then applying an $\text{Sp}_{2g}(\mathbb{Z})$-reduction algorithm to $\tau$ to move it to a nice region such as a fundamental domain, and adjusting $B$ accordingly, see [14] and [30, Section 1.3]. The specific case $g = 1$ comes down to Gauss reduction of quadratic forms, and details for $g = 2$ are given in Dupont’s thesis [15]. We implemented this for $g \leq 2$ as tau.reduce() in [57]. For an implementation for $g = 3$, see Kılıçer [29].

2.6. The type norm. An important ingredient in the reciprocity law is the type norm map $N_{\Phi} : K \rightarrow C : x \mapsto \prod_{\psi \in \Phi^\tau} \psi(x)$ associated to a CM type $\Phi$. Its image generates the reflex field $K^r = \mathbb{Q}(N_{\Phi}(K)) \subset C$ of $\Phi$, and there is a reflex type norm map

$$N_{\Phi^r} : K^r \rightarrow K : x \mapsto \prod_{\psi \in \Phi^r} \psi(x),$$

where the product is taken over the reflex type $\Phi^r$, i.e., the set of embeddings $\psi : K^r \rightarrow \overline{K}$ such that there is a map $\phi : \overline{K} \rightarrow C$ with $\phi \circ \psi = \text{id}_{K^r}$ and $\phi|_K \in \Phi$.

The reflex type norm extends to ideals via ([50, Proposition 29 in §8.3])

$$N_{\Phi^r}(a)\mathcal{O}_L = \prod_{\psi \in \Phi^r} (\psi(a)\mathcal{O}_L)$$

for any number field $L \subset \overline{K}$ containing the images $\psi(K^r)$ for all $\psi \in \Phi^r$. We implemented this as Phir = Phi.reflex() and Phir.type_norm() in [57].

Given a positive integer $M$ and an order $A$ in a number field such that $A$ is maximal at all primes dividing $M$, let $I_A(M)$ be the group of fractional ideals of $A$ that can be written as $ab^{-1}$ with $a + MA = A = b + MA$. We use the shorthand

$$I(M) = I_{\mathcal{O}_K}(M)$$

and observe that $N_{\Phi^r}$ sends $I(M)$ to $I_{\mathcal{O}_K}(M)$.

In order for our results to apply to arbitrary orders $\mathcal{O} \subset K$, we give the following variant of $N_{\Phi^r}$. Let $F$ be the smallest positive integer such that $F\mathcal{O}_K$ is contained in $\mathcal{O}$. Then there is a natural isomorphism $I_{\mathcal{O}}(F) \rightarrow I_{\mathcal{O}_K}(F) : a \mapsto a\mathcal{O}_K$, and we define

$$N_{\Phi^r,\mathcal{O}} : I(F) \rightarrow I_{\mathcal{O}}(F) \quad \text{by} \quad N_{\Phi^r,\mathcal{O}}(a)\mathcal{O}_K = N_{\Phi^r}(a).$$

In particular, we have $N_{K^r,\mathcal{O}_K} = N_{K^r}$.

2.7. The first main theorem. Given a number field $K$, two bases $B = (b_1, \ldots, b_n)$ and $C = (c_1, \ldots, c_n)$ of $K$ over $\mathbb{Q}$ and an element $x \in K$, we denote by $[x]_B^C$ the $n \times n$ matrix over $\mathbb{Q}$ such that for each $j$ the $j$th row is $xc_j$ expressed in terms of $B$.

If we interpret $B$ and $C$ as column vectors in $K^n$, then we have

$$x C = [x]_B^C B.$$
We say that a matrix $M \in \mathbb{Q}^{d \times d}$ is invertible mod $N$ if the numerator of the determinant and the denominators of all coefficients are coprime to $N$. In that case, reduction modulo $N$ defines a matrix $(M \mod N) \in \text{GL}_d(\mathbb{Z}/N\mathbb{Z})$.

**Theorem 2.4** (General reciprocity law). Let $\tau = \tau(\Phi, b, \xi, B) \in H$, be a primitive CM point with CM field $K$, let $N$ be a positive integer and let $f \in \mathcal{F}_N$ be a function that does not have a pole at $\tau$. Let $F$ be the smallest positive integer such that $FO_K$ is contained in the multiplier ring $\mathcal{O}$ of $b$ ($F = 1$ if $\mathcal{O} = \mathcal{O}_K$). Then $f(\tau)$ lies in the ray class field of $K^\tau$ for the modulus $NF$.

For any fractional ideal $a \in I(NF)$, if $[a]$ is the class of $a$ in the ray class group mod $NF$, then $f(\tau)^[a]$ is given as follows.

Choose a symplectic basis $C$ of $\mathcal{N}_{\Phi, \mathcal{O}}(a)^{-1}b$ with respect to $E_{N(a)\xi}$ and let

$$\tau' = \tau(\Phi, \mathcal{N}_{\Phi, \mathcal{O}}(a)^{-1}b, N(a)\xi, C).$$

Then $M := [1]_B^C$ is in $\text{GSp}_{2g}(\mathbb{Q})^\tau$, with $\nu(M) = N(a)^{-1}$, and is invertible mod $N$. Moreover, we have $U := (M \mod N)^{-1} \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$, and

$$f(\tau)^[a] = f(U)(M\tau) = f(U)(\tau').$$

For the computation of suitable $B$ and $C$ (and hence $\tau'$, $M$ and $U$), see Section 2.5.2. We implemented the complete computation of $\tau'$, $M$ and $U$ in [57] as

$$\text{tau.Shimura_reciprocity}(a, N, \text{period_matrix=True}).$$

For the computation of $f(U)$, see Section 2.4. This makes $f(U)(\tau')$ an explicit expression for $f(\tau)^[a]$ that is suitable for computation.

### 2.8. The class fields generated by complex multiplication.

Fix a primitive CM point $\tau$ and let the notation be as above. The field

$$\mathcal{H}(N) = K^\tau(f(\tau) : f \in \mathcal{F}_N \text{ s.t. } f(\tau) \neq \infty) \subset \mathbb{C},$$

is an abelian extension of $K^\tau$, and we now describe the corresponding ideal group.

Let $F$ be the smallest positive integer satisfying $FO_K \subset \mathcal{O}$. For $x \in K$, we write $x \equiv 1 \mod \mathfrak{N}\mathcal{O}$ to mean $x = a/b$ where $a$ and $b \neq 0$ are elements of $\mathcal{O}$ that are invertible modulo $N\mathcal{O}$ and congruent to each other modulo $N\mathcal{O}$. For various equivalent definitions, see Definition 1.2. This is equivalent to standard definitions in the case $\mathcal{O} = \mathcal{O}_K$.

**Theorem 2.5.** The extension $\mathcal{H}(N)/K^\tau$ is abelian and of conductor dividing $NF$. Its Galois group is isomorphic via the Artin isomorphism to the quotient group $I(NF)/H_{\Phi, \mathcal{O}}(N)$, where $I(NF)$ is the group of fractional $\mathcal{O}_K$-ideals with numerator and denominator coprime to $NF$, and

$$H_{\Phi, \mathcal{O}}(N) = \left\{ a \in I(NF) : \exists \mu \in K \text{ with } \frac{N_{\Phi, \mathcal{O}}(a)}{\mu} \in \mathbb{Q}, \mu \equiv 1 \mod N\mathcal{O} \right\}.$$ 

**Remark 2.6.** A similar result for fields of definition of torsion points on normalized Kummer varieties appears as Main Theorem 3 in §17 of [31] (see also Main Theorem 2 in §16 of [19, 50]).

A similar result in adelic language for fields of moduli of abelian varieties with torsion structure appears as Corollary 5.16 of [18] and Corollary 18.9 of [49]. Our statement and proof are directly in the language of the fields $\mathcal{F}_N$ using the reciprocity laws. The proof is in Section 1.5.

Note that this theorem implies that $\mathcal{H}(N)$ depends only on $\mathcal{O}$ and $\Phi$, not on $\tau$.

**Definition 2.7.** For $a \in H_{\Phi, \mathcal{O}}(1)$, we write $\mu(a)$ to denote any element of $K^\times$ as in (2.6) with $N = 1$. 


Note that $\mu(a)$ is uniquely defined up to multiplication by roots of unity in $O$.

**Algorithm 2.8** (Computing $\mu(a)$ for the case $O = O_K$).

*Input:* $\Phi$ and a fractional ideal $a$ of $O_K$.

*Output:* The list of all elements $\mu \in K^\times$ such that $N_{\Phi}(a) = \mu O_K$ and $\mu \mathfrak{p} \in Q$.

*Algorithm:*

1. Compute the class group and unit group of $K$. Compute the maximal totally real subfield $K_0$ of $K$ and its unit group $O_{K_0}^\times$. Compute the quotient $O_{K_0}^\times/N_{K/K_0}(O_K^\times)$. This can be done using e.g. the algorithms of \cite{9}, or the software Magma \cite{7} or PARI \cite{61}. PARI \cite{61} can be used through SageMath \cite{55}.

2. Compute $N_{\Phi}(a)$ and test whether it is principal.
   - If it is, then let $\beta \in K^\times$ be a generator.
   - Otherwise return an empty list.

3. Let $u = \beta \mu/N(a) \in O_{K_0}^\times$, and test whether $u \in N_{K/K_0}(O_K^\times)$. If it is, then take $v \in O_K^\times$ such that $v \mathfrak{p} = u$.
   - Otherwise return an empty list.

4. Return $\{w \beta/v : w \in (O_K^\times)_{\text{tors}}\}$.

We implemented this as \texttt{a_to_mus(Phir, a)} in \cite{57}.

*Proof of Algorithm 2.8.* It is clear that every $\mu = w \beta/v$ in the output generates $N_{\Phi}(a)$ and satisfies $\mu \mathfrak{p} = N(a) \in Q$. Conversely, suppose that $N_{\Phi}(a) = \mu O_K$ and $\mu \mathfrak{p} \in Q$. Then $\mu \mathfrak{p} = N(a)$ and $N_{\Phi}(a)$ is principal, so $\beta$ exists.

Let $r = \beta/\mu \in O_K^\times$. Then $r \mathfrak{p} = \beta \mu/N(a) = u$, hence $v$ exists.

Let $w = v/r \in O_K^\times$. Then $w \mathfrak{p} = 1$, so $w$ is a root of unity. Therefore, $\mu = \beta/r = w \beta/v$ is listed by the algorithm. \hfill $\square$

Using Algorithm 2.8 and standard algorithms for computing ray class groups and computing quotients of groups, we can compute the group $H_{\Phi, O}(N)/P(NF)$ as a subset of the ray class group $\text{Cl}(NF) = I(NF)/P(NF)$ and in turn compute the group $\text{Gal}(H(N)/K^\times) = I(NF)/H_{\Phi, O}(N)$. For an efficient and detailed algorithm, see Asuncion \cite{12}.

### 2.9. Class invariants and a special case of the main theorem.

The reciprocity law (Theorem 2.4) gives the Galois action of $\text{Gal}(H(N))/K^\times$ on $f(\tau)$. In order to decide whether $f(\tau)$ is in the field $H(1)$ generated by the values of Igusa invariants at $\tau$, we need only the Galois action of the subgroup $\text{Gal}(H(N))/H(1)$. For that particular subgroup, we have a simpler version of the reciprocity law as follows.

From Theorem 2.5, we have $\text{Gal}(H(N)/H(1)) = (I(NF) \cap H_{\Phi, O}(1))/H_{\Phi, O}(N)$. For any fractional ideal $a \in I(NF) \cap H_{\Phi, O}(1)$, we get an element $\mu = \mu(a) \in K$ with $\mu \mathfrak{p} = N(a) \in Q$ and $N_{\Phi, O}(a) = \mu O$ (cf. Definition 2.7).

**Theorem 2.9.** Let $\tau = \tau(\Phi, b, \xi, B) \in H_2$ be a primitive CM point, let $N$ be a positive integer and let $f \in F_N$ be a function that does not have a pole at $\tau$.

For any $a \in I(NF) \cap H_{\Phi, O}(1)$, we have

$$f(\tau|a) = f(|\mu(a)|_B^B(\tau))$$

where $\mu \in K$ is such that $\mu \mathfrak{p} = N(a)$ and $N_{\Phi, O}(a) = \mu O$.

Observe that we have constructed a map

$$r : \frac{I(NF) \cap H_{\Phi, O}(1)}{H_{\Phi, O}(N)} \rightarrow \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})/[(O^\times)_{\text{tors}}]_B$$

with $a \mapsto [\mu(a)]_B^B$. 

---

8 MARCO STRENG
where \([\mathcal{O}^x]_{\mathcal{B}}^\text{tors} = \{ [u]_\mathcal{B}^\text{B} : u \in (\mathcal{O}^x)^\text{tors} \}\). The theorem then states

\[ f(\tau)^{[\alpha]} = f^{r(\alpha)}(\tau). \]

**Remark 2.10.** If \( \alpha \) is principal, then the reciprocity map becomes even more explicit:

\[(2.8) \quad r((\alpha)) = [N_{\Phi}(\alpha)]_\mathcal{B} \quad \text{for all} \quad \alpha \in K^r \quad \text{with} \quad (\alpha) \in I(NF). \]

We now get the following way to look for class invariants, that is, values \( f(\tau) \) with \( f \in \mathcal{F}_\infty \) and \( f(\tau) \in \mathcal{H}(1) \). Given \( \tau = \tau(\Phi,b,\xi,B) \), we compute the image \( r(X) \) for a set of generators \( X \) of the domain of \( r \). Then \( f(\tau) \) is a class invariant whenever \( f \) is fixed by \( r(X) \).

**Algorithm 2.11** (Computing the image of \( r \)).

**Input:** \( N, F, \Phi, b, \xi, B \).

**Output:** a complete set \( R \subset \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \) of representatives of the image \( r(X) \) of a set of generators \( X \) of the domain of \( r \).

**Algorithm:**

1. Compute \( G = (I(NF) \cap H_{\Phi,\mathcal{O}}(1))/P(NF) \subset \text{Cl}(NF) \).
2. Let \( X \) be a set of generators of \( G \).
3. For every element of \( X \), choose a representative \( \alpha \), take an arbitrary \( \mu \) in the output of Algorithm 2.8 and compute \([\mu]_\mathcal{B}^\text{B}\). Return the list of matrices \([\mu]_\mathcal{B}^\text{B}\) computed in this way.

We implemented this algorithm as \texttt{reciprocity_map_image(tau, N)} in \texttt{[57]}.

We give an example in Section 7.1.

2.10. Complex conjugation. Now assume that \( f(\tau) \) is a class invariant, that is, is in \( \mathcal{H}(1) \). The coefficients of its minimal polynomial \( H_f \) over \( K^r \) are elements of \( K^r \). If these coefficients are in the maximal totally real subfield \( K_0^r \subset K^r \), then they are easier to compute and take up even less space. We now give a sufﬁcient criterion for these coefficients to be in \( K_0^r \).

Let \( \mathcal{M} := \mathbb{Q}(f(\tau) : f \in \mathcal{F}_1, f(\tau) \neq \infty) \) be the field of moduli of the principally polarized abelian variety corresponding to \( \tau \), and let \( \mathcal{M}_0 = MK_0^r \subset MK^r = \mathcal{H}(1) \).

We give two results. Lemma 2.12 says that often \( \mathcal{M}_0 \) is strictly smaller than \( \mathcal{H}(1) \). And if this is the case, then Proposition 2.14 gives a criterion for the minimal polynomial of \( f(\tau) \) over \( K^r \) to have coefficients in \( K_0^r \).

**Lemma 2.12.** Suppose \( \tau \) corresponds to a pair \( (b,\xi) \).

1. The degree of \( \mathcal{H}(1)/\mathcal{M}_0 \) equals 2 if and only if there is an ideal \( \alpha \in I(F) \) and an element \( \mu \in K^r \) such that \( N_{\Phi,\mathcal{O}}(\alpha) = \mu b \) and \( \mu \mathcal{O} \subset \mathbb{Q} \).
2. If \( g \leq 2 \), \( b \) is coprime to \( F\mathcal{O} \), and \( \Phi \) is a primitive CM type, then the conditions in part (1) are satisfied and we can take
   \[(a) \quad g = 1, \quad \alpha = N_{\Phi}(b \mathcal{O}_K^{-1} \mathcal{O}_K) \quad \text{and} \quad \mu = 1; \quad \text{or} \]
   \[(b) \quad g = 2, \quad \alpha = N_{\Phi}(b \mathcal{O}_K) \quad \text{and} \quad \mu = \mathcal{N}(b). \]
3. If \( b = \mathcal{O} \), then the conditions in part (1) are satisfied and we can take \( \alpha = \mathcal{O}_K \), and \( \mu = 1 \).

**Remark 2.13.** The conditions in part (1) are equivalent to condition (5.1) of Enge-Streng [18]. Proposition 5.3 of [18] gives some cases in which they hold for \( g = 3 \) and \( g = 6 \).

**Proposition 2.14.** Given \( \tau = \tau(\Phi,B) \) and \( f \in \mathcal{F}_N \), assume \( \text{deg} \mathcal{H}(1)/\mathcal{M}_0 = 2 \) and \( f(\tau) \in \mathcal{H}(1) \).

Let \( (\alpha,\mu) \) be as in Lemma 2.12(1) and assume that \( \alpha \) is coprime to \( N \). Write \( B = (b_1,\ldots,b_g,b_{g+1},\ldots,b_{2g}) \) and consider the \( \mathbb{Q} \)-basis \( Q = (\mu^{-1}b_1,\ldots,\mu^{-1}b_g,\mu^{-1}b_{g+1},\ldots,\mu^{-1}b_{2g}) \) of \( K \).
Then \([1]_{12}^2\) is invertible modulo \(N\) with inverse \(V \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})\). Moreover, the following are equivalent:

1. \(f(\tau) \in M_0\),
2. \(f^V(\tau) = f(\tau)\).

If these conditions are satisfied, then the minimal polynomial of \(f(\tau)\) over \(K^\tau\) has coefficients in \(K^\tau\).

The assumption that \(a\) be coprime to \(N\) is without loss of generality.

**Example 2.15.** Suppose \(g = 1\) and \(b = \mathbb{Z}[\sqrt{D}]\). Then we can take \(b_1 = \sqrt{D}\) and \(b_2 = 1\), and by Lemma 2.12 also \(\mu = 1\), so \(c_1 = -b_1\) and \(c_2 = b_2\), hence \(M\) is the diagonal \(2 \times 2\) matrix \([\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\]) and so is \(V\). As the matrix \(-I \in \text{SL}_2(\mathbb{Z})\) acts trivially on every \(\tau \in \mathbb{H}_1\), we find that \(V\) acts exactly as \(i(\mathbb{Z} \bmod{N})\) does, which is as complex conjugation of the coefficients of \(f\). The condition 2.14(2) then translates to \(f\) having only real coefficients in its \(q\)-expansion.

We will prove Lemma 2.12 and Proposition 2.14 in Section 5. These results show that, if we restrict to \(f\) that satisfy \(f^V = f\), then the minimal polynomial of \(f(\tau)\) over \(K^\tau\) is defined over \(K^\tau\). We implemented the computation of the matrix \(V\) in \(\text{tau.complex_conjugation_symplectic_matrix}(\mathbb{N})\).

### 3. The adèlic version

In Section 4 we give a proof of the results stated in Sections 2.3–2.9 (including the reciprocity law). For this, we use Shimura’s own formulation of his reciprocity law, which we state in Section 3. In Section 5 we prove the results about complex conjugation stated in Section 2.10.

The reader who is not interested in the proof, or would like to see the applications first, is advised to skip ahead and read Sections 6 (Theta constants), 7 (Examples) and 8 (Applications), first. They are independent of Sections 3–5.

Shimura developed his reciprocity laws for various types of multivariate modular functions, modular forms, and theta functions in a series of articles \([41–45, 47]\). See also the textbook \([49, 26.10]\). Rather than reproving the reciprocity law in our setting, we will quote a streamlined version stated by Shimura in the language of idèles and rework it (in Section 4) into a version with ideals and a more explicit group action. This means that our proof will not be the most direct proof, as the adèlic statement mashes all levels \(N\) together, and we take them apart again; and Shimura’s original series of articles starts with theta functions, while we give them as a special case afterwards (Section 4). However, our approach does allow us to give both the computationally practical statement and the elegant adèlic statement, explain how they are related, and keep the proofs short at the same time.

The reader who would rather see a direct proof of our explicit version of the reciprocity law should see Yang \([65]\). Yang, inspired by our explicit statements, gives a direct proof of our explicit version of Shimura’s reciprocity law (Theorem 4.1 of \([65]\) is our Theorem 2.4) and uses that to prove the adèlic statement.

We start by citing Shimura’s adèlic action of \(\text{GSp}_{2g}\), and linking it to the actions of Proposition 2.1.

Let \(A\) be the ring of adèles of \(\mathbb{Q}\) and call an element of its unit group positive if its \(\mathbb{R}\)-component is positive. Let \(\hat{\mathbb{Z}} = \lim_{\leftarrow} \mathbb{Z}/N\mathbb{Z}\) be the ring of finite integral adèles, so \(A = (\hat{\mathbb{Z}} \otimes \mathbb{Q}) \times \mathbb{R}\). Let \(\mathcal{F}_\infty = \cup_N \mathcal{F}_N\).

**Proposition 3.1.** There is a unique right action of \(\text{GSp}_{2g}(\mathbb{A})^+\) on \(\mathcal{F}_\infty\) satisfying

1. for \(x \in A^\times\) and \(f \in \mathcal{F}_\infty\), we define \(f^x\) as the function obtained from \(f\) by acting with \(x^{-1}\) on the \(q\)-expansion coefficients,
2. for \(A \in \text{GSp}_{2g}(\mathbb{Q})^+, f \in \mathcal{F}_\infty, \tau \in H_g\), we have \(f^A(\tau) = f(A\tau)\).
(3) for any $N$, the group $T = \{ A \in \text{GSp}_{2g}(\hat{\mathbb{Z}}) : A \equiv 1 \mod N \} \times \text{GSp}_{2g}(\mathbb{R})^+$ acts trivially on the subfield $\mathcal{F}_N$, where we write $A \equiv 1 \mod N$ if and only if for all $p \mid N$ we have $A_p \in 1 + N\mathbb{Z}_p^{2g}$.

Proof. Existence is a special case of [33] Thm. 5(vi,vi,ii)]. Uniqueness follows from the proof of [33] Proposition 1.3. □

Remark 3.2. Our reference for existence in Proposition 3.1 though directly applicable to our situation, may not be satisfactory to some readers, as the paper does not contain the full proof. Therefore, just like [33], we give some pointers for the proof. The action is constructed in [31] Section 2.7 for a field $k_S(V_\tau)$. The field $k_S(V_\tau)$ is defined without $q$-expansions, hence that reference only contains a weak version of (1), but (2) is [31] (2.7.2) and (3) follows immediately from [31] (2.5.3). Our stronger version of (1), as well as the link between $\mathcal{F}_N$ and $k_S(V_\tau)$, is given in [34]. Both that reference and [33] §6 claim that the proof is exactly the same as in the Hilbert modular case, which is [33].

The following corollary proves exactly Proposition 2.1.

Corollary 3.3. The action of Proposition 3.1 has the following property:

(4) For any positive integer $N$, any $f \in \mathcal{F}_N$, and any

$$A = (A_\tau, A_\infty) \in \text{GSp}_{2g}(\hat{\mathbb{Z}}) \times \text{GSp}_{2g}(\mathbb{R})^+ \subset \text{GSp}_{2g}(\mathbb{A})^+,$$

we have $f^A \in \mathcal{F}_N$, and $f^A$ depends only on $(A_\tau \mod N) \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$.

Moreover, the induced action of $\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{F}_N$ is exactly as in Proposition 2.1.

Proof. The inclusion $f^A \in \mathcal{F}_N$ follows from the construction of the action (see [31] (2.5.3)) and [33]. That $f^A$ depends only on $(A_\tau \mod N)$ is Proposition 3.1(3).

It follows that the action induces an action of $\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{F}_N$. To prove that this action is as in Proposition 2.1, it remains only to compute this action for $B \in \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ and for $B = i(t)$ with $t \in (\mathbb{Z}/N\mathbb{Z})^\times$.

In the case $B \in \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$, we lift $B$ to $A' \in \text{Sp}_{2g}(\mathbb{Z})$ (possible by [39] Theorem VII.21), and we get $f^B = f^{A'}$ by Proposition 2.1(3). As we have

$$\text{Sp}_{2g}(\mathbb{Z}) = \text{GSp}_{2g}(\mathbb{Q})^+ \cap (\text{GSp}_{2g}(\mathbb{Z} \times \text{GSp}_{2g}(\mathbb{R})^+),$$

can then apply Proposition 3.1(2) to get that $f^B$ is as in Proposition 2.1.

In the case $B = i(t)$ with $t \in (\mathbb{Z}/N\mathbb{Z})^\times$, we lift $t$ to $x \in \hat{\mathbb{Z}}^\times$ and apply Proposition 3.1(1), which gives $f^B = f^x = f^{-1} = f^1$, so that again $f^B$ is as in Proposition 2.1. Here, the switch from $x^{-1}$ to $x$ is explained by the usual map from the idèle class group to the ray class group: starting from $x \in \hat{\mathbb{Z}}^\times$, we take $c \in \mathbb{Q}^\times \cap \mathbb{Z}$ with $t = (c \mod N)$ to get $cx \in \hat{\mathbb{Q}}^\times$ that is 1 modulo $N$ and in the same idèle class. Then $cx$ in turn maps to the class of the fractional ideal $(c)$ in the ray class group, which acts as $t$ on $\mathbb{Q}(\zeta_N)$.

Let $\tau = \tau(\Phi, B) \in H_j$ be a primitive CM point for the CM field $K$.

The type norm $N_{\phi}$ and the map $\epsilon : a \mapsto [a]_B$, induce adelic maps $N_{\phi^*} : K^\times_A \to K^\times_A$, and $\epsilon : K^\times_A \to \text{GL}_{2g}(\mathbb{A})$, and the composite map sends $K^\times_A$ to $\text{GSp}_{2g}(\mathbb{A})^+$. Shimura gives the following reciprocity law, stated in a very sleek manner using the action of Proposition 3.1.

Theorem 3.4 (Shimura). Let $\tau$ and the notation be as above. Then for every $f \in \mathcal{F}_\infty$ such that $f(\tau)$ is finite and every $x \in K^\times_A$, we have

$$f(\tau) \in K^\times_{ab} \quad \text{and} \quad f(\tau)^x = f(\epsilon(N_{\phi^*}(x))^{-1}(\tau).$$
Proof. This is equation (3.43) of [47, p. 57] up to two minor modifications.

First of all, that reference assumes that the abelian variety \( A = \mathbb{C}^g / (\tau \mathbb{Z}^n + \delta \mathbb{Z}^n) \) for an integer \( \delta \geq 3 \) has CM, but that variety has CM by \( K \) if and only if ours has.

Secondly, the matrix \( \epsilon(a) \) is defined differently in [47], namely for \( a \in K \) by the (less computationally convenient) identity of complex matrices

\[
\rho(a)(\tau, 1g \times g) = (\tau, 1g \times g) \epsilon(a)^t
\]

where \( \rho(a) \in \mathbb{C}^{g \times g} \) is the matrix of \( a \in K = \text{End}(A) \otimes \mathbb{Q} \) with respect to the standard basis of \( \mathbb{C}^g \). We now check that our matrix \( \epsilon(a) = [a]_B^B \) also satisfies (3.1).

We have \( aB = [a]_B^B B \), which by taking the transpose and applying \( \Phi \) leads to

\[
\text{diag}(\Phi(a))(\Phi(b_1), \ldots, \Phi(b_2)) = (\Phi(b_1), \ldots, \Phi(b_2))([a]_B^B)^t.
\]

The change of basis \((\Phi(b_{g+1}), \ldots, \Phi(b_2))^{-1}\) yields (3.1) for \( \epsilon(a) = [a]_B^B \). \( \Box \)

Remark 3.5. Recent work of Hertogh [25,26] provides a computer implementation of adèles and idèles. It would be interesting to see whether this allows one to use Theorem 3.3 directly in a practical way on a computer, and whether this can be made to work as well in practice as our main theorems.

4. Proof of the explicit reciprocity law

In this section, we prove our explicit version of Shimura’s reciprocity law, using Shimura’s adélic version (Theorem 3.4).

The bridge between adélic and ideal theoretic class field theory is the surjection

\[
K_{\Lambda}^{\times} / K_{\Lambda}^{\times} \to \text{Cl}(NF) = I(NF)/P(NF)
\]

that maps the class of an idèle \( x \equiv 1 \mod \Lambda \) of \( NF \) to the class of the ideal \( a \) with \( \text{ord}_p(a) = \text{ord}_p(x_p) \).

Given \( f \in \mathcal{F}_N \) and an idèle \( x \in K_{\Lambda}^{\times} \), let \([a] \) be the image of \( x \) under the map (3.1). By Theorem 3.3 we have \( f(\tau)^a = f(\tau)^x = f^{(N_{\Lambda}^\times(x))^{-1}}(\tau) \), and our goal is to express this in terms of \( a \). To do so, we write \( \epsilon(N_{\Lambda}^\times(x))^{-1} = SU M \) with \( M \in \text{GSp}_{2g}(\mathbb{Q})^+ \), \( U \in \text{GSp}_{2g}(\mathbb{Z}) \), \( S \in \text{Stab}_f \), and both \( M \) and \( (U \mod N) \) explicit in terms of \( a \). Then we can conclude \( f^\delta(\tau) = f(U^\mod N)(M) \), by Theorem 3.3.

Remark 4.1. The strong approximation theorem for \( \text{GSp}_{2g}(A) \) in fact tells us that such a decomposition always exists, even with \( U \in i(\mathbb{Z}^\times) \) (47 Lemma 1.1)). However, as in the genus-one case [24], we will be satisfied with having only \( U \in \text{GSp}_{2g}(\mathbb{Z}) \). In fact, by allowing \( U \in \text{GSp}_{2g}(\mathbb{Z}) \), we can make sure that \( M \tau \) is in a fundamental domain for \( \text{Sp}_{2g}(\mathbb{Z}) \), which improves the speed of convergence in practical computations.

4.1. Coprimality and congruence for fractions. To help in translating adélic statements to more concrete statements, we first state some equivalent definitions of “mod\(^\times\)” that we will use. This is not new, but statements that apply to non-maximal orders are rare in the literature, so we give a detailed statement and proof.

Let \( \mathcal{O} \) be an order in \( K \) and let \( F \in \mathbb{Z} \) be the smallest positive integer such that \( \mathcal{O} \supset F \mathcal{O}_K \). For any prime number \( p \in \mathbb{Z} \), let

\[
\mathcal{O}(p) = \{ a/b \in K : a \in \mathcal{O}, b \in \mathbb{Z} \setminus p \mathbb{Z} \}.
\]

In this section, for \( a \in \mathcal{O} \), we use the notation \( \overline{a} = (a \mod NF \mathcal{O}) \in (\mathcal{O}/NF \mathcal{O})^\times \).

Definition 4.2. Let \( N \) be a positive integer. We say that an element \( x \in K_{\Lambda}^{\times} \) is coprime to \( NF \) with respect to \( \mathcal{O} \) if one of the following equivalent conditions holds (equivalence is proven below):

(1) \( x = a/b \) for some \( a, b \in \mathcal{O} \) with \( \overline{a}, \overline{b} \in (\mathcal{O}/NF \mathcal{O})^\times \) and \( b \neq 0 \),
(2) \( x = a/b \) for some \( a \in \mathcal{O} \) and \( b \in \mathbb{Z} \setminus \{0\} \) with \( \bar{a} \in (\mathcal{O}/N\mathcal{O})^\times \) and \( b - 1 \in NF\mathbb{Z} \).

(3) for all prime numbers \( p \mid NF \), we have \( x \in \mathcal{O}_{(p)}^\times \).

(4) \( x\mathcal{O} = ab^{-1} \) for non-zero \( \mathcal{O} \)-ideals \( a \) and \( b \) that are coprime to \( NF \) in the sense that \( a + N\mathcal{O} = b + N\mathcal{O} = \mathcal{O} \).

We write \( x \equiv 1 \mod^\times\mathcal{O} \) to mean that one of the following equivalent conditions holds (equivalence is proven below):

(1') as in (1) above, with additionally \( a - b \in N\mathcal{O} \),

(2') as in (2) above, with additionally \( a - 1 \in N\mathcal{O} \),

(3') as in (3) above, with additionally \( x - 1 \in N\mathcal{O}_{(p)} \) for all prime numbers \( p \mid N \).

In terms of \( p \)-adic numbers, both \( \mathcal{O} \otimes \mathbb{Z}_p \) and \( K \) are subrings of \( \mathcal{O} \otimes \mathbb{Q}_p \), and their intersection is exactly \( \mathcal{O}_{(p)} \). In particular, the conditions (3) and (3') can equivalently be written with \( \mathcal{O} \otimes \mathbb{Z}_p \) instead of \( \mathcal{O}_{(p)} \).

**Proof of equivalence in Definition 4.2.** We start with the equivalence of (1)–(4).

(2) \( \Rightarrow \) (1) is obvious.

(1) \( \Rightarrow \) (2). Let \( N(b) = \#(\mathcal{O}/b\mathcal{O}) \). We start by showing that \( NF \) is coprime to \( N(b) \) and that \( N(b) \) is an \( \mathcal{O} \)-multiple of \( b \).

We have \( 1 \in b\mathcal{O} + N\mathcal{O} \), so \( NF \) is a unit modulo \( b\mathcal{O} \), hence multiplication by \( NF \) is invertible on the additive group \((\mathcal{O}/b\mathcal{O})\) of order \( N(b) \), so \( NF \) is coprime to \( N(b) \). Note that \( N(b) \) annihilates the group \( \mathcal{O}/b\mathcal{O} \), hence \( N(b) \in b\mathcal{O} \), so \( N(b) \) is a multiple of \( b \).

Let \( c \in \mathbb{Z} \) be such that \( b' := cN(b) \equiv 1 \mod NF \). We get \( x = a'/b' \) with \( a' = acN(b)/b \in \mathcal{O} \) and \( a'/b' \in (\mathcal{O}/N\mathcal{O})^\times \).

(1) \( \Rightarrow \) (3). Suppose that \( x \) satisfies (1). Then \( x^{-1} \) also satisfies (1). By “(1) \( \Rightarrow \) (2)”, we then get that both \( x \) and \( x^{-1} \) satisfy (2). By the definition of \( \mathcal{O}_{(p)} \), we then get \( x, x^{-1} \in \mathcal{O}_{(p)} \), hence \( x \in \mathcal{O}_{(p)}^\times \).

(3) \( \Rightarrow \) (4). If \( NF = 1 \), then this is trivial, so suppose \( NF > 1 \).

For every prime \( p \mid NF \), write \( x = a_p/b_p \) and \( x^{-1} = c_p/d_p \) with \( a_p, c_p \in \mathcal{O} \) and \( b_p, d_p \in \mathbb{Z} \setminus p\mathbb{Z} \). Let \( b = \sum a_p b_p \mathcal{O} \subset \mathcal{O} \), \( d = \sum c_p d_p \mathcal{O} \subset \mathcal{O} \), \( a = bx = \sum c_p b_p \mathcal{O} \subset \mathcal{O} \), and \( c = bx^{-1} = \sum d_p c_p \mathcal{O} \subset \mathcal{O} \). We get \( ac = bd \). The ideals \( b \) and \( d \) are coprime to all prime numbers \( p \mid NF \) because of \( b_p \in b \) and \( d_p \in d \). It follows that \( ac = bd \) is coprime to \( N\mathcal{O} \). In particular, both \( a \) and \( b \) are coprime to \( N\mathcal{O} \), hence \( b \) is invertible and we have \( x\mathcal{O} = ab^{-1} \).

(4) \( \Rightarrow \) (1). Suppose \( x = ab^{-1} \) with \( a \) and \( b \) non-zero ideals of \( \mathcal{O} \) coprime to \( N\mathcal{O} \). Then \( a \) and \( b \) are both invertible and we have \( xb = a \). We have \( b + N\mathcal{O} = \mathcal{O} \), hence there exists an \( a \in b \) with \( b \equiv 1 \mod(NF\mathcal{O}) \). Take a non-zero such \( b \). Let \( a = bx \). Then \( a\mathcal{O} = (bb^{-1})a \) is coprime to \( N\mathcal{O} \). This proves (1).

We have now proved that (1)–(4) are equivalent. It remains to prove that (1')–(3') are equivalent. Note that each (n') implies (n), so we may and will assume that (1)–(4) hold. Write \( x = a/b \) as in (1) and \( x = a'/b' \) as in (2). We have \( ab' = a'b \), hence \( b'(a-b) = b(a'-b') \). As \( b \) and \( b' \) are invertible in \( \mathcal{O}/N\mathcal{O} \), we get (1') \( \iff b'(a-b) \in N\mathcal{O} \iff b(a'-b') \in N\mathcal{O} \iff b(a'-b') \in N\mathcal{O} \iff (2') \).

Next, we have \( b'(x-1) = (a'-1) = (b'-1) \) and for all \( p \mid N \) we have \( b' \in \mathcal{O}_{(p)}^\times \) and \( b' - 1 \in NFZ \subset N\mathcal{O}_{(p)} \). In particular, we have (3') if and only if for all \( p \mid N \) we have \( a' - 1 \in N\mathcal{O}_{(p)} \). We also have \( a' - 1 \in \mathcal{O} \) and \( \cap_{p \mid N} N\mathcal{O}_{(p)} \cap \mathcal{O} = N\mathcal{O} \), so (3')\( \iff (2') \).

**4.2. The conductor.** We now prove the first statement in Theorem 2.3 that \( f(r) \) lies in the ray class field for the modulus \( NF \). In other words, we prove that the
extension $\mathcal{H}(N) = K^\times(f(\tau) : f \in \mathcal{F}_N)$ of $K^\times$, which is abelian by Theorem 4.4 has conductor dividing $NF$.

As in Section 2, let $\mathfrak{b}$ be a fractional $\mathcal{O}$-ideal with $\text{End}(\mathfrak{b}) = \mathcal{O}$ and let $F$ be the smallest positive integer such that $FO_K \subset \mathcal{O}$. Let $B$ be a $\mathbb{Z}$-basis of $\mathfrak{b}$.

**Lemma 4.3.** For $a \in K^\times$, we have $a \in \mathcal{O}$ if and only if $[a]_B^B \in \mathbb{Z}^{2g \times 2g}$.

**Proof.** We have $a \in \mathcal{O}$ if and only if $ab \subset \mathfrak{b}$, which is equivalent to $[a]_B^B \in \mathbb{Z}^{2g \times 2g}$. □

**Lemma 4.4.** For $a \in K$, we have $a \equiv 1 \mod \mathcal{O}$ if and only if the following two conditions hold:

1. we have $[a]_B^B \in \text{GL}_{2g}(\mathbb{Z}_p)$ for all $p \mid NF$, and
2. the coefficient-wise reduction modulo $N$ of $[a]_B^B$ is the identity matrix.

**Proof.** Lemma 4.3 and its proof stay valid when considered locally at a prime number $p$, that is, replacing $\mathcal{O}$ by $\mathcal{O}_p$ and $\mathbb{Z}$ by $\mathbb{Z}_p$ for a prime $p$. By Definition 4.3, we have $a \equiv 1 \mod \mathcal{O}$ if and only if $(a-1)/N \in \mathcal{O}_p$ for all $p \mid N$ and $a \in \mathcal{O}_p$ for all $p|N$. The result follows if we apply Lemma 4.3 to $(a-1)/N$ locally at all primes dividing $N$ and to $a$ and $a^{-1}$ at all primes dividing $NF$. □

**Proposition 4.5.** The conductor of $\mathcal{H}(N)$ divides $NF$.

**Proposition 4.5.** The conductor of $\mathcal{H}(N)$ divides $NF$.

**Proof.** What we need to prove is equivalent to the statement that the kernel

$$W_{NF} = \{ xK^\times \in K^\times_K / K^\times : x \equiv 1 \mod \mathcal{O}, \forall \nu \ord_\nu(x) = 0 \}$$

of $\mathfrak{a}$ acts trivially on all $f \in \mathcal{F}_N$. So take $x$ with these properties and let $y = \{[N_{\nu,\nu'}(x)]_B^B\}_i^{-1}$. Then Theorem 4.4 tells us $f(\tau)^y = f^y(\tau)$.

We have $N_{\nu,\nu'}(x) \equiv 1 \mod \mathcal{O}$, hence $N_{\nu,\nu'}(x) \equiv 1 \mod \mathcal{O}$. Then by Lemma 4.3 and another local application of Lemma 4.3 (this time to $p \mid N$), we find that $y$ is in the group $T = \{ A \in \text{GSp}_{2g}(\mathbb{Z}) : A \equiv 1 \mod N \} \times \text{GSp}_{2g}(\mathbb{R})^+$, which acts trivially on $f$ by Proposition 4.3. So we get $f^y = f$, hence $f(\tau)^y = f^y(\tau) = f(\tau)$. □

### 4.3. Changes of symplectic bases.

The next statement in Theorem 2.4 is that the matrix $M = [1]_B^B$ is in the group $\text{GSp}_{2g}(\mathbb{Q})^+$. Lemma 4.7 proves this claim.

**Lemma 4.6.** For a field $F$ and matrix $M \in \text{GL}_{2g}(F)$, the following are equivalent:

1. there exists $y \in F^\times$ such that $yM\Omega M^t = \Omega$,
2. $M \in \text{GSp}_{2g}(F)$.

If this is the case, then $\nu(M) = y^{-1}$.

**Proof.** Statement (2) means $M^t\Omega M = \nu(M)\Omega$ for some $\nu(M) \in F^\times$. By taking inverses and observing $\Omega^{-1} = -\Omega$, we see that this is equivalent to $M^{-1}\Omega(M^t)^{-1} = \nu(M)^{-1}\Omega$. Multiplying on the left by $M$ and on the right by $M^t$ shows that this is equivalent to (1), with $y = \nu(M)^{-1}$. □

**Lemma 4.7.** Given $\tau = (\Phi, b, \xi, B)$ and $M \in \text{GL}_{2g}(\mathbb{Q})$, let $\mathfrak{c}$ be the subgroup of $K$ generated by $C = MB$ and let $E = E_{\mathfrak{c}}$. Then the following are equivalent:

1. there exists $y \in \mathbb{Q}^\times$ such that $yE$ is a principal polarization for $\mathfrak{c}$ and $C$ is a symplectic basis of $\mathfrak{c}$ for $yE$,
2. $M \in \text{GSp}_{2g}(\mathbb{Q})^+$.

Moreover, if this is the case, then we have

1. $\nu(M) = y^{-1}$, and
2. $\tau(\Phi, \mathfrak{c}, y\xi, C) = M\tau$. 

Proof. Since \( C \) is a basis of \( \epsilon \), statement (1) is statement (1) of Lemma 4.6 together with positive-definiteness of \((u,v) \mapsto yE(iu,v)\). This positive-definiteness is equivalent to \( y > 0 \), hence Lemma 4.6 gives equivalence of (1) and (2), as well as (a).

Let \( \tau' = \tau(\Phi, \epsilon, y, \xi, C) \). It remains to show \( \tau' = M\tau \). Write \( M = (a,b,c,d) \) for \( g \times g \) blocks \( a,b,c,d \). Write \( B = (b_1, \ldots, b_2g) \), and take the \( g \times 2g \) matrix \( B = (b_1 B_2) = (\Phi(b_1) \mid \ldots \mid \Phi(b_2g)) \), and similarly define \( C \) using \( C \). We have \( C = MB \), hence \( C = BM' = (B_1c^i + B_2b'|B_1c^j + B_2b^j) \). This gives \( \tau' = (B_1c^j + B_2b^j)^{-1}(B_1c^i + B_2b^i) \). As \( \tau \) and \( \tau' \) are symmetric, we get \( \tau = B_1^{-1}B_2^{-1}(B_1c^i + B_2b^i) \) and \( \tau' = (aB_1 + bB_2)(cB_1 + dB_2)^{-1} = (\tau + b)(\tau + c)^{-1} \).

4.4. Decomposing \( \epsilon(N_{\Phi}(x)) \) modulo the stabilizer. Let us recall the situation of the theorem we are proving (Theorem 2.4): we have a fractional \( \mathcal{O}_{K'} \)-ideal \( \mathfrak{a} \) coprime to \( NF \), a symplectic basis \( B = (b_1, \ldots, b_g) \) of \( \mathfrak{b} \) with respect to \( \mathcal{E}_{\xi} \), and a symplectic basis \( C = (c_1, \ldots, c_g) = BM' \) of \( N_{\Phi, \mathcal{O}(a)}^{-1}\mathfrak{b} \) with respect to \( E_{N(a)\xi} \). Here \( M = [1]_{\mathfrak{b}} \).

In order to compute the action of the ray class \([a]\) of \( \mathfrak{a} \) modulo \( NF \), we choose an idèle \( x \) whose class maps to \([a]\). To be precise, we choose \( x \in K_{\mathfrak{a}}^\times \) such that

1. for every prime ideal \( p \mid NF \) we have \( x_p = 1 \),
2. for all other prime ideals \( p \) we have \( \text{ord}_p(x_p) = \text{ord}_p(a) \).

Then by Lemma 4.3 we have

\[
(4.2) \quad \epsilon(N_{\Phi}(x)) \equiv 1_{2g} \mod \mathcal{E}_{\xi} \quad \text{NF},
\]

with \( \epsilon : a \mapsto [a]_{\mathfrak{p}}^B \) as defined above Theorem 3.3.

Lemma 4.8. The matrix \( A := \epsilon(N_{\Phi}(x))^{-1}M^{-1} \) lies in \( \text{GSp}_{2g}(\mathbb{Z}) \times \text{GSp}_{2g}(\mathbb{R})^+ \).

Proof. Note \( \nu \circ \epsilon \circ N_{\Phi} = N_{K'/\mathbb{Q}} \), and the fact that \( K' \) has no real embeddings implies \( N_{K'/\mathbb{Q}}(K'^\times \otimes \mathbb{R}) \subset \mathbb{R}_{>0}^\times \), so \( \epsilon(N_{\Phi}(x))_{\infty} \in \text{GSp}_{2g}(\mathbb{R})^+ \). We also have \( M \in \text{GSp}_{2g}(\mathbb{Q})^+ \) by Lemma 4.7, hence \( A_{\infty} \in \text{GSp}_{2g}(\mathbb{R})^+ \). It now suffices to prove for every prime number \( p \) that \( A_p \) is in \( \text{GSp}_{2g}(\mathbb{Z}_p) \). For any number field \( L \) and \( x \in L^\times \), write \( x_p \in L \otimes \mathbb{Z}_p \) for the part corresponding to primes over \( p \).

We have the following identity of \( \mathbb{Z}_p \)-submodules of \( K^\times \otimes \mathbb{Z}_p \) of rank \( 2g \):

\[
(N_{\Phi}(a)^{-1}b) \otimes \mathbb{Z}_p = N_{\Phi}(x)^{-1}_p(b \otimes \mathbb{Z}_p)
\]

(\[\text{indeed, for } p \mid FN, \text{ both sides are equal to } b \otimes \mathbb{Z}_p, \text{ while for } p \notmid F, \text{ the order is locally maximal and the identity follows from } \text{ord}_p(a) = \text{ord}_p(x) \]. We have already chosen a basis \( C = (c_1, \ldots, c_{2g}) \) of the left hand side. We take the \( \mathbb{Z}_p \)-basis \( C' = (N_{\Phi}(x)_p^{-1}b_1, \ldots, N_{\Phi}(x)_p^{-1}b_{2g}) \) of the right hand side and notice that \( A_p \) transforms one basis to the other in the sense that \( C' = N_{\Phi}(x)_p^{-1}B = \epsilon(N_{\Phi}(x)_p^{-1}B = A_p C \).

In particular, we have \( A_p \in \text{GL}_{2g}(\mathbb{Z}_p) \). As the basis on the left is symplectic for \( (N(a)\xi) \) and the one on the right is symmetric for \( (N(x)\xi) \), we apply Lemma 4.6 and find \( A_p \in \text{GSp}_{2g}(\mathbb{Q}_p) \). As we already had \( A_p \in \text{GL}_{2g}(\mathbb{Z}_p) \), we conclude \( A_p \in \text{GSp}_{2g}(\mathbb{Z}_p) \).

Proof of Theorem 2.4. The fact that \( f(\tau) \) is in the ray class field modulo \( NF \) is Proposition 4.5. We have \( M \in \text{GSp}_{2g}(\mathbb{Q})^+ \), \( \nu(M) = N(a)^{-1} \), and \( \tau' = M\tau \) by Lemma 4.7.

It remains to prove that \( M \) is invertible modulo \( N \) and that \( U = (M \mod N)^{-1} \) is in \( \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \) and satisfies \( f(\tau)^{[a]} = f(U)(\tau) \).

We have \( \epsilon(N_{\Phi}(x))^{-1} = A \) with \( A \in \text{GSp}_{2g}(\mathbb{Z}) \times \text{GSp}_{2g}(\mathbb{R})^+ \) by Lemma 4.8. This and (1.2) imply that \( M \) is invertible modulo \( N \) and that the inverse \( U \) is \( (A \mod N) \). The adèlic reciprocity law (Theorem 3.3) tells us \( f(\tau)^{[a]} = f(\tau)^x = \).
which satisfies which scales the polarization by element of we find µγ to change the basis isomorphism hMτ is integral, that is, we have H trivially on M. We have now proven all results from Sections 2.1–2.9.

Next, we prove Theorem 2.5, which states Gal(H(N)/K) = I(NF)/HΦ,0(N).

Proof of Theorem 2.5. Note that Theorem 2.4 and Lemma 4.4 already imply that HΦ,0(N) acts trivially on H(N). It remains to prove that if a ∈ I(NF) acts trivially on H(N), then a ∈ HΦ,0(N). Here without loss of generality the ideal a is integral, that is, we have a ⊂ OKn. So let a ∈ I(NF) be an integral ideal with f(τ)a = f(τ) for all f ∈ FN. Let U and M be as in Theorem 2.4, so that for all f ∈ FN, we get f(τ) = f(τ) = fU(Mτ) with U ∈ GSp2g(Z/NZ) and M ∈ GSp2g(Q)+ such that U = (M mod NF)−1. We claim that without loss of generality, we have U = 1, M ≡ 1 mod N and Mτ = τ.

Proof of the claim: By taking f = ζN, we find ζN(U) = ζN, hence U ∈ Sp2g(Z/NZ). Then lift U to Sp2g(Z), and use the lift to change the chosen basis c1, . . . , cg of Theorem 2.4. We find that without loss of generality, we have U = 1, which implies M ≡ 1 mod N. We now have f(τ) = f(Mτ) for all f ∈ FN, and by [21, (2.5.1)], this implies τ ∈ ΛN Mτ, i.e., τ = γMτ for some γ ∈ ΛN. We use γ to change the basis c1, . . . , cg again, and conclude also Mτ = τ. This proves the claim.

Let c = NΦ,0(a)−1b with basis C = MB, leading by Lemma 1.7(b) to the period matrix Mτ. We have Mτ = τ, hence there is a polarization-preserving isomorphism h : C/Φ(c) → C/Φ(b) := A sending the ith element of C to the ith element of B. The identity map on C induces an isogeny the other way around, which scales the polarization by N(a). Their composite is some µ ∈ End(A) = O, which satisfies µ−1b = c and µ−1 = N(a) ∈ Q. This last identity shows that µ is coprime to F, so if we look at the (invertible) coprime-to-F part of µ−1b = c, then we find µO = NΦ,0(a).

We have c(µ) = M. Lemma 4.3 therefore shows µ ≡ 1 mod N O.

We have now proven all results from Sections 2.1–2.9.

5. Complex conjugation

Next, we prove the results in Section 2.10.

Proof of Lemma 2.13. Recall M0 = K0(f(τ) : f ∈ Fl), and consider the extension H(1) = M0 Kτ/M0. Part (1) of Lemma 2.12 states that this extension has degree 2 if and only if there exist a ∈ I(F) and µ ∈ K× such that NΦ,0(a)b = µb and µ−1 ∈ Q.

We start by proving the ‘only if’ part, so suppose that H(1)/M0 has degree 2. The non-trivial automorphism 7 of this extension restricts to complex conjugation on K, so γ : x → 7(x) is an element of Gal(H(1)/K). Suppose that 7 is obtained from (b, ξ), and let A be the corresponding principally polarized abelian variety.

As γ and complex conjugation are equal on M0, we get that γ(A) and A are isomorphic.

By [33, Proposition 3.5.5], the abelian variety A corresponds to (b, ξ). At the same time, the automorphism γ corresponds via the Artin map to the class of an
ideal \(a\) of \(K\). The isomorphism between \(\gamma(A)\) and \(\overline{A}\) then gives an element \(\mu \in K^\times\) such that we have \(N_{\Phi}(a\overline{b}) = \mu b\) and \(N(a) = \mu\). This proves the ‘only if’ of (1).

Conversely, if \(a\) exists, by scaling \(a\) (and scaling \(\mu\) accordingly), we can assume \(a\) to be coprime to \(NF\). Then take the corresponding \(\gamma \in \text{Gal}(H(1)/K')\) and let \(\gamma_0: x \to \gamma(x)\), which is in \(\text{Gal}(H(1)/M_0)\) and is non-trivial as it restricts to complex conjugation on \(K'\). This prove the ‘if’ part.

For part (2), in case \(g = 1\) and \(b\) is coprime to \(FO\), we simply take \(a = N_{\Phi}(b\overline{b})\) and \(\mu = 1\) as \(N_{\Phi}\) is an isomorphism with inverse \(N_{\Phi}\).

If \(g = 2\) and \(b\) is coprime to \(FO\), take \(a = N_{\Phi}(bO_K)\) and \(\mu = N(b)\). We have \(N_{\Phi}N_{\Phi}(bO_K) = N(b)b^{-1}O_K\) (see [46, (3.3)] or [28, (3.2)]), which implies part (2).

Finally, if \(b = O\), then \(\overline{b} = O = O\), so \(a = 1\) and \(\mu = 1\) suffice.

\[\phi_{\text{explicit}} \quad \text{SHIMURA RECIPROCITY FOR SIEGEL MODULAR FUNCTIONS} \quad 17\]

**Proof of Proposition 2.14** Assume that \(H(1)/M_0\) is an extension of degree 2, so there exist \(a, \mu\) and \(\gamma_0\) as in the proof of Lemma 2.12 and without loss of generality we have \(a \in I(NF)\).

Let \(f \in F_N\) be such that \(f(\tau)\) is a class invariant. Now \(f(\tau)\) is in \(M_0\) if and only if \(\gamma_0(\tau) = f(\tau)\) holds, that is, if and only if we have \(\tau[\overline{a}] = f(\tau)\).

The action of complex conjugation is easy to describe. For \(h \in F_N\), note that \(h^{-1}(\mod N)\) is \(h\) with its Fourier coefficients replaced by their complex conjugates. Since complex conjugation is continuous on \(C\), we get

\[h(\tau) = h(\overline{\tau}) \mod N(\overline{\tau}).\]

Let us look at the action of \([a]\) via the reciprocity law (Theorem 2.4). Let \(b_1, \ldots, b_g\) be a symplectic basis of \(b\) that gives rise to \(\tau\) and consider the symplectic basis

\[C = (\mu^{-1}b_1, \ldots, \mu^{-1}b_g, -\mu^{-1}b_{g+1}, \ldots, -\mu^{-1}b_{2g})\]

of \(\mu^{-1}C = N_{\Phi}(\overline{a})^{-1}b\) with respect to \(\mu\overline{b}\overline{\xi} = N(a)\overline{\xi}\), which gives rise to the period matrix \(\overline{C}\). By Theorem 2.4 we have \([1]_{C}^{C} \in \text{GSp}_{2g}(\mathbb{Q})^+, U := ([1]_{B}^{C} \mod N)^{-1} \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})\), and \(f[\overline{a}] = fU(-\overline{\tau})\).

The basis \(C\) differs from \(Q\) by multiplying the final \(g\) entries by \(-1\), so we have \([1]_{Q}^{C} = i(-1)\). In particular, we have \([1]_{Q}^{Q} = i(-1)[1]_{C}^{C}\), hence \(V = Ui(-1) \mod N\).

Applying 2.10 to \(h = fU\), we conclude \([f(\tau)]^\phi = fV(\tau)\), so indeed we have \(f(\tau) \in M_0\) if and only if \(fV(\tau) = f(\tau)\).

Finally, suppose that we have \(\alpha = f(\tau) \in M_0\). Let \(P \in K'[X]\) be the minimal polynomial of \(\alpha\) over \(K'\). Then \(\overline{P} = \gamma_0(P)\) is the minimal polynomial of \(\gamma_0(\alpha)\) over \(K'\). In the case \(\alpha \in M_0\), we have \(\gamma_0(\alpha) = \alpha\), hence \(\overline{P} = P\), so \(P\) has coefficients in \(K_0^\phi\).

\[6. \quad \text{THETA CONSTANTS}\]

For \(c_1, c_2 \in \mathbb{Q}^2\), the theta constant with characteristic \(c_1, c_2\) is the map \(\theta[c_1, c_2] : H_g \to C\) given by

\[\theta[c_1, c_2](\tau) = \sum_{v \in \mathbb{Z}^g} \exp(\pi i (v + c_1)^\tau(v + c_1) + 2\pi i (v + c_1)^\tau).\]

We often restrict to theta constants with \(c_i \in [0, 1]^g\), because we have

\[\theta[c_1 + n_1, c_2 + n_2] = \exp(2\pi i c_1^\tau n_2)\theta[c_1, c_2] \quad \text{for} \quad n_1, n_2 \in \mathbb{Z}^g.\]

Theta constants have a very explicit action, as the following result shows. The result itself is not surprising, but the author is unaware of an equally explicit version in the literature: directly working for \(\text{GSp}_{2g}\) instead of only \(\text{Sp}_{2g}\) and working with arbitrary coefficient-wise lifts instead of having to lift to \(\text{Sp}_{2g}(\mathbb{Z})\).
Proposition 6.1. Given $D \in 2\mathbb{Z}$ and $c_1, c_2, c'_1, c'_2 \in D^{-1}\mathbb{Z}$, we have

$$\frac{\theta[c_1, c_2]}{\theta[c'_1, c'_2]} \in \mathcal{F}_{2D^2}.$$ 

Moreover, the action of $A \in \text{GSp}_{2g}(\mathbb{Z}/2D^2\mathbb{Z})$ is as follows. Take lifts

$$B = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in \mathbb{Z}^{2g \times 2g} \quad \text{and} \quad t_\text{inv} \in \mathbb{Z}$$

of $A$ and $\nu(A)^{-1}$. Define

$$\left(\begin{array}{c} d_1 \\ d_2 \end{array}\right) = B^t \left(\begin{array}{c} c_1 - \frac{1}{2} t_\text{inv} \text{diag}(cd^t) \\ c_2 - \frac{1}{2} t_\text{inv} \text{diag}(ab^t) \end{array}\right)$$

and define $d'_1, d'_2, r'$ analogously. Then we have

$$(6.3) \quad \left(\frac{\theta[c_1, c_2]}{\theta[c'_1, c'_2]}\right)^A = \exp(2\pi i (r - r')) \frac{\theta[d_1, d_2]}{\theta[d'_1, d'_2]}.$$ 

Remark 6.2. It is known that the field generated by all quotients as in Proposition 6.1 (for all $D$) equals the field $\mathcal{F}_N$ (see for example [49, 27.15]).

To prove Proposition 6.1 we use the following lemma giving the action of $\text{Sp}_{2g}(\mathbb{Z})$.

Lemma 6.3. Given $B \in \text{Sp}_{2g}(\mathbb{Z})$, there is a holomorphic $\rho = \rho_B : H_g \to \mathbb{C}^\times$ such that for all $c_1, c_2 \in \mathbb{Q}$, we have

$$\theta[c_1, c_2](B\tau) = \rho(\tau) \exp(2\pi i r) \theta[d_1, d_2](\tau),$$

where $d_1, d_2, r$ are as in the formulas of Proposition 6.1 with $t = 1$.

Proof. This follows with some algebraic manipulation when substituting our $d$ for the $c$ in Formula 8.6.1 of [6] (see [6, Lemma 8.4.1(b)] for the definition of $M[d]$).

Remark 6.4. The interested reader could see [6, Exercise 8.11(9)] for more information about $\rho_B$.

Proof of Proposition 6.1. Let $N = 2D^2$. We start by showing that the right hand side of (6.3) is independent of the choices of lifts.

Note that a change of lift changes $B^t$ at most by adding elements of $2D^2\mathbb{Z}$ to the entries. Similarly, it changes $c_i = \frac{1}{2} t_\text{inv} \text{diag}(\cdots) \in D^{-1}\mathbb{Z}$ at most by adding elements of $2D^2\mathbb{Z}$. In particular, it changes $d_1, d_2, d'_1, d'_2$ at most by adding elements of $2D^2\mathbb{Z}$. In turn, this means that $r$ changes at most by adding an element of $\mathbb{Z}$. Neither change has effect on the right hand side of (6.3) by (6.2).

Now that we know that (6.3) is independent of the chosen lifts, we prove it for $A \in \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ by taking a lift in $B \in \text{Sp}_{2g}(\mathbb{Z})$, taking $t_\text{inv} = 1$, and applying Lemma 6.3 to the numerator and denominator, where the factors $\rho(\tau)$ cancel.

Next, we show that $f = \theta[c_1, c_2]/\theta[c'_1, c'_2]$ is indeed in $\mathcal{F}_N$. First multiply the numerator and denominator of $f$ by $\theta[0, 0]^7$. Then we use Lemma 6.3 with $\rho_B(\tau)^8 = (\det cr + d)^4$. We have already done all the computations required for checking that these modular forms are invariant under $\Gamma_N$. As the Fourier coefficients are in $\mathbb{Q}(\zeta_N)$ by the definition [6], we find $f \in \mathcal{F}_N$.

Finally, any element $A \in \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ can be written as $A = A^0 i(t)$, with $t = \nu(A) \in \mathbb{Z}/N\mathbb{Z}$, and $A^0 \in \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$. Choose lifts $B \in \mathbb{Z}^{2g \times 2g}$ of $A^0$ and $\bar{t} \in \mathbb{Z}$ of $t$. Starting from (6.3) for $A^0$, we compare what happens when we either multiply $A^0$ by $i(t)$ from the right, or act on the right hand side of (6.3) by $i(t)$. 

\[18\text{ MARCO STRENG}\]
The latter replaces $\zeta_N$ by $\zeta_N^2$, which is equivalent (by the definition (6.1)) to changing $r$ into $tr$ and $(d_1, d_2)$ into $(d_1, \bar{d}_2)$.

Writing $B = (a, b, c, d)$, we get $A = (a, b\bar{c}, c, d) \mod N$. It is straightforward to check that multiplying $b$ and $d$ by $\bar{t}$ and changing $t_{\text{inv}} = 1$ into $t_{\text{inv}}$ changes $(d_1, d_2)$ into $(d_1, \bar{d}_2)$ modulo $D^2\mathbb{Z}$. In turn, this changes $r$ into $tr$ modulo $\mathbb{Z}$. By (6.2), this gives the same result as just changing $r$ into $tr$ and $(d_1, d_2)$ into $(d_1, \bar{d}_2)$.

Given a rational function $f \in \mathcal{F}_N$ that is expressed in terms of theta constants with characteristics in $D^{-1}\mathbb{Z}^{2g}$ with $N | 2D^2$, we can now evaluate the action of $A \in \text{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ on $f$. We do not need to lift $A$ to $\text{Sp}_{2g}(\mathbb{Z})$, only to $\text{GSp}_{2g}(\mathbb{Z}/2D^2\mathbb{Z})$, which is a relatively simple matter of linear algebra over $\mathbb{F}_p$ for primes $p | 2D$. And in fact, we choose even to avoid that by applying the reciprocity theorem (Theorem 2.4) directly with $2D^2$ in place of $N$ (and using $f \in \mathcal{F}_N \subset \mathcal{F}_{2D^2}$).

If $f$ is a quotient of homogeneous polynomials of equal degree in the theta constants, then we can simply apply the formulas in Proposition 6.1 directly to the individual theta constants and do not have to write $f$ as a rational function of quotients of the form $\theta[c_1, c_2]/\theta[c_1', c_2']$. For example, note that we have

\[
(6.4) \quad f = \frac{\theta[\frac{1}{2}, 0, 0, \frac{1}{2}]}{\theta[\frac{1}{2}, 0, 0, 0]} = \frac{\theta[\frac{1}{2}, 0, 0, 1]}{\theta[1, c_1, c_2]} + \frac{\theta[0, 0, 0, 0]}{\theta[0, 0, 0, 1]}
\]

and the copies of $\exp(-2\pi ir)\theta[d'_1, d'_2]^{-1}$ in the numerator and denominator cancel in the end anyway.

We implemented the formulas of Proposition 6.1 in [57] as $f^A$ where $f$ as in (6.4) can be constructed using

\[
f = \text{ThetaModForm}([[1/2, 0, 0, 1/2]]) / (\text{ThetaModForm}([[1/2, 1/2, 0, 0]])) + \text{ThetaModForm}([[0, 0, 0, 0]]).
\]

7. Finding class invariants and minimal polynomials

In this section, we demonstrate how to use the main results for finding class invariants. We give additional results and algorithms as we need them.

Given an order $\mathcal{O}$ in a CM field $K$ of degree $2g$ and a primitive CM type $\Phi$ of $K$, a class invariant is a value $f(\tau)$ with $f \in \mathcal{F}_{X}$, $\tau$ a primitive CM point with CM by $\mathcal{O}$ of type $\Phi$, and $f(\tau) \in \mathcal{H}(1)$. For example, if $K$ is quadratic and $\mathcal{O} = \mathbb{Z} + \tau\mathbb{Z}$, then $j(\tau)$ is a class invariant, and its minimal polynomial over $K$ is called the Hilbert class polynomial $H_\mathcal{O} \in \mathbb{Z}[X]$. Weber [63] gave class invariants of imaginary quadratic orders with minimal polynomial that have much smaller coefficients than $H_\mathcal{O}$ and from which $j(\tau)$ can be recovered. For CM fields of degree $2g$, we compare the height of our our class invariants with the height of values of known generators of $\mathcal{F}_1$, such as $j$ for $g = 1$ and absolute Igusa invariants [27] for $g = 2$.

Given $f \in \mathcal{F}_N$, we check the inclusion $K^i(f(\tau)) \subset \mathcal{H}(1)$ (equivalently $f(\tau) \in \mathcal{H}(1)$) using Theorem 2.9. If $f$ is sufficiently general, then the inclusion of fields $K^i(f(\tau)) \subset \mathcal{H}(1)$ is an equality, which can be verified numerically using Theorem 2.4. The latter theorem also allows us to numerically determine the minimal polynomial of $f(\tau)$ over $K^i$.

7.1. Finding a class invariant. In this example, consider quotients $f$ of products of theta constants with $c_1, c_2 \in \{0, \frac{1}{2}\}^2$, that is, $g = 2$, $D = 2$, $N = 8$. We also include this example at the beginning of the file article.sage at [57], so it could be followed step by step on a computer. The theta constants for which $4c_1c_2$ is odd are identically zero, and we are left with 10 so-called even theta constants, which happen to have Fourier coefficients in $\mathbb{Z}$. Following [15], we use the notation...
\(\theta[(a, b), (c, d)] =: \theta_{16b + 8a + 4d + 2c}\) for \(a, b, c, d \in \{0, \frac{1}{2}\}\), so the even theta constants are \(\theta_k\) for \(k \in \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}\).

We take the quartic CM field \(K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/(X^4 + 27X^2 + 52)\) from Example III.3.2. Its real quadratic subfield is \(K_0 = \mathbb{Q}(\sqrt{52}).\) Take the CM type \(\Phi = \{\phi : K \to \mathbb{C} \mid \phi(\alpha) \in i\mathbb{R}_{>0}\}\) and let \(w = \sqrt{15} \in \mathbb{R}_{>0}.\) The real quadratic subfield of the reflex field \(K^1\) is \(\mathbb{Q}(w)\).

We start by finding a period matrix \(\tau = \tau(\Phi, b, \xi, B)\) as in Section 2.5.2. In our case, this yields \(b = \mathcal{O}, \xi = 2(224411531\alpha^3 + 46779315\alpha)\)^{-1}, and a symplectic basis

\[
B = \left[ \begin{array}{c}
(653\alpha^3 + 3414\alpha^2 + 1363\alpha + 7126, 401\alpha^3 + 2360\alpha^2 + 837\alpha + 4926, \\
- 653\alpha^3 + 1306\alpha^3 - 1363\alpha + 2726, 2108\alpha^2 + 4400) \end{array} \right].
\]

Next, we compute generators of the image of the map

\[
r : \frac{I(N) \cap H_{\Phi, \mathcal{O}}(1)}{H_{\Phi, \mathcal{O}}(N)} \to \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})/[(\mathcal{O}^\times)^{\text{tors}}]_B
\]

from (2.2) in Section 2.3 using the command \text{reciprocity_map_image(tau, 8)} of 27, that is, using Algorithm 2.11. This yields a list \(R\) of 6 matrices in \text{GSp}_{2g}(\mathbb{Z}/8\mathbb{Z}).

A function \(f \in \mathcal{F}_8\) yields a class invariant if it is fixed by all elements of \(R\). Let us look at the action on quotients of theta constants of Proposition 6.1 more closely, starting with 8th powers so that the factor \(\exp(2\pi i(r - r'))\) vanishes. This action can be viewed as an action on the numerator and denominator separately. So this is an action of \(\text{GSp}_{2g}(\mathbb{Z}/8\mathbb{Z})\) on the set of 8th powers of the ten even theta constants. Under the action of the subgroup generated by \(R\), we compute that this set is partitioned into 4 orbits: \(\{\theta_0^8, \theta_1^8, \theta_6^8\}, \{\theta_2^8, \theta_3^8, \theta_9^8\}, \{\theta_8^8, \theta_3^8, \theta_15^8\}, \{\theta_12^8\}\).

Let us restrict our search for class invariants to those functions \(f\) that are products of powers of the theta constants. To ensure that the image of \(r\) fixes \(f^8\) up to units, we use whole orbits, that is, write

\[
f = c(\theta_0\theta_1\theta_5)^j(\theta_2\theta_3\theta_4)^k(\theta_8\theta_9\theta_{15})^l\theta_{12}^m
\]

with \(c \in \mathbb{Q}^{\mathbb{Q}}\) and integers \(j, k, l, m\) that satisfy \(3j + 3k + 3l + m = 0\).

There are various values of \((j, k, l, m)\) that one could try, but we prefer the minimal polynomial of \(f(\tau)\) over \(K^1\) to have coefficients in \(K_0^1\), so we also look at the action of \(V\) from Proposition 2.13. It turns out that this action swaps the first two orbits, so we take \(j = k\). In fact, we like to use small products of theta constants, so we leave out these six theta constants, that is, we take \(j = k = 0\). We then get \(3l = -m\), so with \(n = -l\) we get

\[
f = cf_0^n\quad\text{where}\quad f_0 = \frac{\theta_{12}^3}{\theta_8\theta_9\theta_{15}}.
\]

Note that if 8 divides \(n\) and \(c \in \mathbb{Q}\), then we have \(f(\tau) \in \mathcal{H}(1)\), but to let \(f(\tau)\) have small height, we want to try smaller values of \(n\).

Explicitly computing the action of \(R\) and \(V\) on \(f_0\) and \(\zeta_8\), and trying out every \(c \in \mu_8\) for \(n = 1, 2, \ldots,\) we find that \(n = 2, c = \zeta_8^3\) gives a function that is invariant under \(R\) and \(V\), so that we have \(f(\tau) \in \mathcal{M}_0\).

The steps above illustrate a general algorithm, which is also what we followed when creating the examples mentioned in Section 7.3 below.

It is however sometimes too restrictive to only consider roots of unity \(c\), as demonstrated by Sotákova 52 (even in the case \(g = 1\)). In Section 7.4 we give the higher-dimensional version of Sotákova’s ideas for finding the optimal \(n\) and \(c\). For this particular function \(f\) it still yields \(n = 2\) as the smallest valid exponent.
7.2. Computing the minimal polynomial. So now we have our class invariant \( f(\tau) \in \mathcal{H}(1) \) and we would like to compute its minimal polynomial over \( K' \). We have \( \text{Gal}(\mathcal{H}(1)/K') = I(1)/H_{\mathcal{O}(1)} \) (Theorem 2.5). In general, this group could be computed using the methods of [19, Section 4.2]. In this particular case, the class number of \( K' \) is odd and the class group of its real quadratic subfield is trivial, hence (see [56, Example 1.10.4]) the Galois group is simply the class group of \( K' \).

For each of the 7 ideal classes of \( K' \), we compute \( U \) and \( \tau' \) as in Theorem 2.4. We make sure that the basis \( C \) is such that \( \tau' \) is reduced for the action of \( \text{Sp}_{2g}(\mathbb{Z}) \) (see the end of Section 2.5.2) so that the theta constants can be numerically evaluated most efficiently.

Then we compute \( f^U \) as in Section 6 and evaluate it numerically at \( \tau' \) to get a root of the minimal polynomial of \( f(\tau) \) over \( K' \). This yields an approximation of

\[
H_f = \prod_{i=1}^{7} (X - f(U_i(\tau'_i))) \in K'_0[X],
\]

and we recognize its coefficients as elements of \( K'_0 \subset \mathbb{C} \) with the LLL-algorithm as in [35, Section 7]. The entire calculation is in the file article.sage of [57]. We find that numerically with high precision, we have

\[
101^2 H_1 = 66928761X^7 + (21911488848w - 76603728240)X^6 + (-20331835674284w + 733099844294784)X^5 + (-2807221228773580980w + 1012518088965439488)X^4 + (-2349120383562514432w + 846987458815623744)X^3 + (-7859120312174770816w + 28336461342131104256)X^2 + (25091734141632512w - 904696010264018944)X - 364471595827200w + 13127826580439040904198594009X^7 + (155205162116358647755w + 559600170220988887110)X^6 + (152407687697460195175920750535594152550w + 549513732768094562589706361181928594009X^5 + (2201909958003052373027262384843538048317834513875w + 7939998794735431484153019089320973153011210882125)X^4 + (104775262927931828916458740891367594710449395570625w + 3775644104882208328657293464297520693800908715736875)X^3 + (9073992148004948551367529911060411111644713247380607234375w + 32716516813059111926889031427237753094763461200379169938284375)X^2 + (15014166049656519860048580229712441133906502590506987454062500w + 541334555036719078560594444586939893083538154105365978411062500)X + (320854170291151322128777010521751800513120977055409053777776328984375w + 1156856162931200673807932114342428501257906676832654599917987279296875).
\]

As the first polynomial is so much smaller, we needed a much lower precision to reconstruct it from a numerical approximation. As our invariant \( f \) is built up from the same theta constants as the absolute Igusa invariants (see [58, Section 8]), it takes the same time to evaluate it to any given precision, so saving precision in this way means saving time.

7.3. More examples. We searched for class invariants with \( D = g = 2 \) for a few more fields. For each of the fields we tried, the results were similar to Section 7.1.
an easily found product of powers of the ten even theta constants yielded a class invariant, which reduced the precision required for finding the class polynomials. We made such examples available online in article.sage at [57].

We mention one of them in particular. Andreas Enge and Emmanuel Thomé, when demonstrating their implementation of a method for computing class polynomials [10], presented at the GeoCrypt 2011 conference a computation of the Igusa class polynomials of the maximal order $\mathcal{O}_K$ of the field $K = \mathbb{Q}[X]/(X^4 + 310X^2 + 1764)$ of class number 3948.

Following the steps of Section 7.1 we found that the functions
\[ t = \frac{\theta_2\theta_8}{\theta_4\theta_{12}} \in \mathcal{F}_8, \quad u = \left( \frac{\theta_2\theta_8}{\theta_6\theta_{12}} \right)^2 \in \mathcal{F}_2, \quad v = \left( \frac{\theta_2\theta_2}{\theta_4\theta_6} \right)^2 \in \mathcal{F}_2 \]
are class invariants with CM by $\mathcal{O}_K$.

These invariants have the additional advantage that $(t^2, u, v)$ are Rosenhain invariants, meaning that the abelian variety corresponding to $\tau$ is the Jacobian of
\[ C : y^2 = x(x - 1)(x - t(\tau)^2)(x - u(\tau))(x - v(\tau)). \]
In particular, they are especially useful for constructing curves as in Section 8.2.

We believe for two reasons that these class invariants have much smaller height than the Igusa invariants. First, this is what happened in our other examples with quotients of small products of theta functions, and second it is claimed in [13] that Rosenhain invariants typically have much smaller height than Igusa invariants. As a result we expect that these invariants would have significantly sped up the computation for the example of Enge and Thomé.

7.4. More general constants. In Section 7.1 we described a general procedure for finding class invariants of the form $c \prod \theta_{[c_i]}^{e_i}(\tau)$ with roots of unity $c$. Sotáková in her MSc thesis [52] showed how to do the same with arbitrary elements $c \in \mathbb{Q}(\zeta_N)^\times$ that are not necessarily roots of unity. Her ideas come down to the use of the inflation-restriction sequence from group cohomology and Hilbert’s theorem 90, and amount to the following result.

Proposition 7.1 (cf. [52] Section 5.4.3). Given a subgroup $G \subset \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$, let $\mathcal{F}_N^G$ be the fixed subfield.

Let $H \subset G$ and $C \subset (\mathbb{Z}/N\mathbb{Z})^\times$ be the kernel and image of $\nu : G \to (\mathbb{Z}/N\mathbb{Z})^\times$. Then we have
\[[7.1] \{ f \in \mathcal{F}_N^G : \exists c \in \mathbb{Q}(\zeta_N)^\times \text{ cf } \in \mathcal{F}_N^G \} = \left\{ f \in \mathcal{F}_N^G : \forall A \in G \text{ and } f^A/f \in \mathbb{Q}(\zeta_N)^\times \right\}. \]

Moreover, for every element $f$ of the right hand side we can find $c$ with $cf \in \mathcal{F}_N^G$ as follows:

1. let $\phi : C = \nu(G) \to \mathbb{Q}(\zeta_N)^\times$ be $\nu(A) \mapsto f^A/f$,
2. take any $g \in \mathbb{Q}(\zeta_N)$ such that $c := \sum_{k \in C} \phi(k)g^\sigma(k) \neq 0$,

where $\zeta_N^\sigma(k) = \zeta_N^k$.

Remark 7.2. Two typical groups $G$ we take are as follows. Let $\tau$ be a CM period matrix and let $G^r$ be the preimage $\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ of the image of $r$ as in (2.27).

We can take $G = G^r$, and then $f \in \mathcal{F}_N^G$ implies $f(\tau) \in \mathcal{H}(1)$ by Theorem 2.9.
Alternatively, we take \( G = \langle G', V \rangle \) to be the subgroup of \( \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \) generated by \( G' \) and the complex conjugation matrix \( V \) of Proposition 7.14. In that case \( f \in \mathcal{F}_N^G \) implies \( f(\tau) \in M_0 \), so that the minimal polynomial of \( f(\tau) \) over \( K^r \) has coefficients in \( K_0^r \).

**Remark 7.3.** In practical computations, we consider a free abelian subgroup \( F \subset \mathcal{F}_N^G/\mathcal{Q}(\zeta_N)^r \) generated by finitely many theta constants and stable under the action of \( \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \). Then the conditions on the right hand side of (7.1) come down to linear equations in the \( \mathbb{Z} \)-module \( F \), and hence finding the intersection of \( F \) with the right hand side of \((7.1)\) comes down to linear algebra over \( \mathbb{Z} \).

**Proof.** The left hand side of \((7.1)\) is contained in the right because its elements \( f \) satisfy \( f^A = (cf)^A/c^A = cf/cf^A = (c/c^A)f \) for all \( A \in G \) with \( c/c^A = c \) if \( A \in H \).

For the reverse inclusion, it suffices to show that the procedure of steps (1) and (2) is correct. Note that the map \( \phi \) is well-defined precisely when \( f \) is in the right hand side of \((7.1)\). This map \( \phi \) is a 1-cocycle for the group \( C \subset (\mathbb{Z}/N\mathbb{Z})^r = \text{Gal}(\mathcal{Q}(\zeta_N)/\mathcal{Q}) \) and the \( C \)-module \( \mathcal{Q}(\zeta_N)^r \), that is, we have \( \phi(kf) = \phi(k)^{\nu(\ell)}\phi(\ell) \). Such a cocycle is a coboundary by Hilbert’s theorem 90 \((H^1(\text{Gal}(E/F), E^r)) = 0 \) with \( E = \mathcal{Q}(\zeta_N) \) and \( F = E^C \). In fact, the proof of Hilbert’s theorem 90 comes down to \( c \) being non-zero for some \( y \) together with the direct verification of the identity \( c^{\nu(\ell)} = \phi(\ell)^{-1}c \). This gives \((cf)^A = \phi(\nu(A))^{-1}c\phi(\nu(A))f = cf \), hence \( cf \in \mathcal{F}_N^G \).

As examples where this procedure finds small class invariants where \( c \) is not a root of unity, see [52, Sections 6.2 and 6.3].

8. Applications

8.1. Class fields. Hilbert class fields of number fields can be computed using Kummer theory [7][10], but that requires extending the base field with auxiliary roots of unity, which make such computations too costly for larger examples. Complex multiplication yields a more efficient way to compute the Hilbert class field if the base field is imaginary quadratic [12][61] or quartic CM [2]. Class invariants yield a further speed-up by lowering the required precision.

8.2. Curves of genus two with prescribed Frobenius. In this section we show how class invariants give a practical improvement to the CM method for constructing curves of genus two. We start with a sketch of the CM method without class invariants \((8.2.1)\). Then we recall how class invariants are used in genus one \((8.2.2)\). Finally we explain how class invariants give an improvement in genus two \((8.2.3)\).

8.2.1. The CM method. We would like to construct a \( g \)-dimensional abelian variety over a finite field with a prescribed characteristic polynomial \( f \) of the Frobenius endomorphism \( \pi \). Indeed, when choosing \( f \) appropriately, this yields an abelian variety with a prescribed number of points, or with good cryptographic properties \([11][20][53]\).

The idea of the CM method is to take an abelian variety \( \tilde{A} \) in characteristic zero with a nice endomorphism ring \( \mathcal{O} \), and reduce it modulo a prime. The endomorphism ring of the reduction \( A \) will contain both \( \pi \) and \( \mathcal{O} \). A ‘lack of space’ in \( \text{End}(\tilde{A}) \) then relates \( \pi \) to \( \mathcal{O} \), giving us the control that we need.

In more detail, assuming for simplicity that \( f \) is an irreducible Weil polynomial of degree \( 2g \), this works as follows. The field \( K = \mathcal{Q}[X]/(f) \) is a CM field of degree \( 2g \), the constant coefficient \( f(0) = p^{m_0} \) is a prime power, and the root \( \pi_0 = (X \mod f) \) is a Weil \( p^m \)-number, that is, satisfies \( \pi_0^{p^m} = p^m \). Let \( \tilde{A} \) be an abelian variety over a number field \( k \) with \( \text{End}(\tilde{A}_k) \cong \mathcal{O}_K \) of CM type \( \Phi \). Assume \( k \supset K^r \), or
equivalently, that the endomorphisms of \( \tilde{A} \) over \( \overline{\mathbb{F}} \) are defined over \( k \). Let \( \mathfrak{p} \) be a prime of \( k \). Suppose that \( \tilde{A} \) has good reduction at \( \mathfrak{p} \) and let \( A \) be the reduction. Let \( \pi \in \text{End}(A) \) be the Frobenius endomorphism of \( A \). Reduction modulo \( \mathfrak{p} \) gives an embedding \( \mathcal{O}_K = \text{End}(\tilde{A}) \subseteq \text{End}(A) \) and we have the following result.

**Theorem 8.1** (Shimura-Taniyama formula [50] Thm.1 in §13). The endomorphism \( \pi \) is an element of the ring \( \mathcal{O}_K \subseteq \text{End}(A) \) and generates the ideal \( N_{\mathfrak{p}}(N_{k/K}(\mathfrak{p})) \) of \( \mathcal{O}_K \).

This, together with the fact \( \pi \mathfrak{p} = \#(\mathcal{O}_k/\mathfrak{p})^g \) determines \( \pi \) up to roots of unity. In fact, by taking \( k \) to be minimal, we get \( \pi = \pi_0 \) up to roots of unity, that is, up to twists of \( A \).

This CM method can be made to be practical for at least \( g = 1 \) [3, 5, 50, 15, 53, 65], and \( g = 2 \) [4, 32, 34, 64], as well as for a certain class of curves with \( g = 5 \) [51].

In all practical situations, one does not write down defining equations for the characteristic-zero abelian variety \( \tilde{A} \), but only evaluates certain modular functions at \( \tilde{A} \). For example, for \( g = 1 \), we take the \( j \)-invariant and for \( g = 2 \), we take a triple of absolute Igusa invariants \( i_1, i_2, i_3 \).

In the case \( g = 1 \), the elliptic curve \( A \) can be reconstructed from \( j(A) = (j(\tilde{A}) \mod \mathfrak{p}) \) by a textbook formula. In the case \( g = 2 \), for generic values of the Igusa invariants modulo \( \mathfrak{p} \), one can reconstruct \( \tilde{A} \) as the Jacobian of a hyperelliptic curve using Mestre’s algorithm [37]. Similar constructions are used for \( g = 3 \) and \( g = 5 \).

In the CM method for \( g = 1 \), the value \( j(\tau) \) is represented by its minimal polynomial, the Hilbert class polynomial. We reduce \( j(\tau) \) modulo a prime by reducing the Hilbert class polynomial modulo \( p \) and taking a root of that in \( \overline{\mathbb{F}}_p \).

In the case \( g \geq 2 \), we take a minimal polynomial \( H_{i_1} \) of the first invariant \( i_1(\tilde{A}) \) over \( K' \), and we represent \( i_2, \ldots, i_d \) by polynomials

\[
\hat{H}_{i_1, i_n} = \sum_{\gamma} i_n(\tilde{A})^\gamma \prod_{\sigma}(X - i_n(\tilde{A})^\sigma) \in K'_0[X],
\]

where sum and product range over \( \text{Gal}(H(1)/K') \) (see [21]). Reducing \( H_{i_1} \) modulo a prime \( p_0 \) of \( K_0' \) and taking any root is equivalent to reducing \( i_1(\tilde{A}) \) modulo a prime over \( p_0 \). We can then find \( i_2(A), \ldots, i_d(A) \) by computing

\[
i_n(A) = \frac{\hat{H}_{i_1, i_n}(i_1(A))}{H_{i_1}'(i_1(A))}
\]

if \( p \) is sufficiently large.

This is how the CM method works, and now we would like to use class invariants for efficiency.

### 8.2.2. Class invariants for genus one.

We now summarise the (standard) way in which class invariants are used in the CM method in the case \( g = 1 \). Let \( f \in \mathcal{F}_N \) be a non-constant function and let \( \Phi_{f,j}(X, Y) \in \mathbb{Q}[X, Y] \) be such that \( \Phi_{f,j}(j, Y) \in \mathbb{Q}(j)[Y] \) is a (not necessarily monic) minimal polynomial of \( f \) over \( \mathcal{F}_1 = \mathbb{Q}(j) \). Then we have \( \Phi_{f,j}(j(\tau), f(\tau)) = 0 \). So given \( f(\tau) \), we can find \( j(\tau) \) by solving for \( X \) in \( \Phi_{f,j}(X, f(\tau)) = 0 \).

For the CM method, we compute the polynomial \( \Phi_{f,j} \) and the minimal polynomial \( H_f \) of a class invariant \( f(\tau) \). Here \( \Phi_{f,j} \) can be reused as it depends only on \( f \), and \( H_f \) is much smaller than the Hilbert class polynomial \( H_j \), hence needs less precision. We compute \( f(\tau) \) modulo a prime over \( \mathfrak{p} \) by taking a root \( f_0 \) of \( H_f \) modulo \( p \). Then we solve for \( X \) in \( \Phi_{f,j}(X, f_0) = 0 \) to get \( j(A) \).
8.2.3. **Class invariants in general.** For general $g$, we give three methods for using class invariants.

**Using modular polynomials as in $g = 1$.** For $g \geq 2$, modular polynomials are much harder to compute \cite{8,24,36,38}, and the higher-dimensional analogue of solving $\Phi_{f,j}(X, f_0) = 0$ involves Gröbner bases. But for some choices of invariants this may be doable.

**A modular interpretation of the class invariants.** Some class invariants themselves give rise to models of curves or abelian varieties in a direct way, without the need of invariants from $F_1$. For example, the modular functions $t, u, v \in F_8$ of Section 7.3 give rise to the curve $y^2 = x(x-1)(x-t^2)(x-u)(x-v)$ without the intermediate step of Igusa invariants.

**Numerically expressing invariants in terms of the class invariant.** Suppose that $i_1, \ldots, i_d$ are the invariants we need in order to construct our curve or abelian variety. We numerically compute $H_f$ and

$$\hat{H}_{f,i_n} = \sum_{\gamma} i_n(\tilde{A})^\gamma \prod_{\sigma}(X - f(\tilde{A})^\sigma) \in K^r[X].$$

These polynomials are in $K^r_0[X]$ if the conditions of Proposition 2.14 are satisfied. We find $f_0$ as a root of $H_d$ modulo $p$, and compute $i_n(A)$ for $n$ from it by the formula

$$i_n(A) = \frac{\hat{H}_{f,i_n}(f_0)}{H'_f(f_0)}.$$

We do need to compute $d + 1$ polynomials instead of $d$, compared to when only using $i_1, \ldots, i_d$, but as the size is dominated by the first invariant, which is now $f$ instead of $i_1$, the total size of the polynomials still goes down.

For the example from Sections 7.1–7.2, we computed the polynomials $H_f$ and $\hat{H}_{f,i_n}$ and made them available online (close to line 200 of the file article.sage of \cite{7}). These four polynomials together take up 15% less space than the three polynomials $H_i$ and $\hat{H}_{i,i_n}$. More importantly, the largest coefficient (which determines the precision at which theta constants need to be evaluated, the dominant step in the computation) is 40% smaller.

**References**

1. Jared Asuncion. Computing the Hilbert class fields of quartic CM fields using complex multiplication. preprint, \url{arXiv:2104.15363}, 2021.
2. Jared Asuncion. Complex multiplication constructions of abelian extensions of quartic fields. PhD thesis, Université de Bordeaux and Universiteit Leiden, 2022. \url{https://hdl.handle.net/1887/3304503}
3. A. Oliver L. Atkin and François Morain. Elliptic curves and primality proving. Math. Comp., 61(203):29–68, 1993. \url{http://www.inria.fr/rrrt/rr-1256.html}
4. Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. LMS J. Comput. Math., 19(suppl. A):283–300, 2016.
5. Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In Algorithmic Number Theory – ANTS-VIII (Banff, 2008), LNCS 5011, pages 282–295. Springer, 2008.
6. Christina Birchendhake and Herbert Lange. Complex abelian varieties, volume 302 of Grundlehren der mathematischen Wissenschaften. Springer, second edition, 2004.
7. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
8. Reinier Bröker and Kristin Lauter. Modular polynomials for genus 2. LMS Journal of Computation and Mathematics, 12:326–339, 2009.
9. Henri Cohen. A Course in Computational Algebraic Number Theory, volume 138 of Graduate Texts in Mathematics. Springer, 1993.
[10] Henri Cohen. Advanced topics in computational number theory, volume 193 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2000.

[11] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. Handbook of elliptic and hyperelliptic curve cryptography. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[12] Henri Cohen and Peter Stevenhagen. Computational class field theory. In J. Buhler and P. Stevenhagen, editors, Surveys in Algorithmic Number Theory, volume 44 of MSRI Publications, pages 497–534. Cambridge University Press, 2008.

[13] Craig Costello, Alyson Deines-Schutz, Kristin Lauter, and Tonghai Yang. Constructing abelian surfaces for cryptography via Rosenhain invariants. LMS J. Comput. Math., 17(suppl. A):157–180, 2014.

[14] Bernard Deconinck, Matthias Heil, Alexander Bobenko, Mark van Hoeij, and Marcus Schmies. Computing Riemann theta functions. Math. Comp., 73(247):1417–1442, 2004.

[15] Régis Dupont. Moyenne arithmético-géométrique, suites de Borchardt et applications. PhD thesis, École Polytechnique, 2006. http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf.

[16] Andreas Enge. CM. software available at http://www.multiprecision.org/cm/.

[17] Andreas Enge and François Morain. Fast decomposition of polynomials with known Galois group. In Applied algebra, algebraic algorithms and error-correcting codes (Toulouse), LNCS 2643, pages 254–264. Springer, 2003.

[18] Andreas Enge and Marco Streng. Schertz style class invariants for genus two, 2016. preprint, arXiv:1610.04505.

[19] Andreas Enge and Emmanuel Thomé. Computing class field polynomials for abelian surfaces. Exp. Math., 23(2):129–145, 2014.

[20] David Freeman, Peter Stevenhagen, and Marco Streng. Abelian varieties with prescribed embedding degree. In A. J. van der Poorten and A. Stein, editors, ANTS, volume 5011 of Lecture Notes in Computer Science, pages 60–73. Springer, 2008.

[21] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In Advances in Cryptology – ASIACRYPT 2006, LNCS 4284, pages 114–129. Springer, 2006.

[22] Alice Gee. Class invariants by Shimura’s reciprocity law. J. Théor. Nombres Bordeaux, 11(1):45–72, 1999. Les XXèmes Journées Arithmétiques (Limoges, 1997).

[23] Alice Gee and Peter Stevenhagen. Generating class fields using Shimura reciprocity. In Algorithmic number theory (Portland, OR, 1998), volume 1423 of Lecture Notes in Comput. Sci., pages 441–453. Springer, Berlin, 1998.

[24] David Gruenewald. Explicit Algorithms for Humbert Surfaces. PhD thesis, University of Sidney, 2009. (3,3) modular polynomial at http://www.maths.usyd.edu.au/u/davidg/thesis.html.

[25] Mathé Hertogh. Computing with adèles and idèles. MSc thesis, Universiteit Leiden, https://hdl.handle.net/1887/3249353. 2021.

[26] Mathé Hertogh. Computing with adèles and idèles. SageMath code, https://github.com/mathehertogh/adeles. 2021.

[27] Jun-Ichi Igusa. Arithmetic variety of moduli for genus 2. Annals of Mathematics, 72(3):612–649, 1960.

[28] Pınar Kılıçer and Marco Streng. The CM class number one problem for curves of genus 2. Res. Number Theory, 9(1):Paper No. 15, 29, 2023.

[29] Pınar Kılıçer. Reduction of period matrices in genus 3. https://bitbucket.org/pkilicer/period-matrices-for-genus-3-cm-curves/.

[30] Pınar Kılıçer, Hugo Labrande, Reynald Lerca, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over Q with complex multiplication. Acta Arith., 185(2):127–156, 2018.

[31] Max Koecher. Zur Theorie der Modulformen n-ten Grades. I. Math. Z., 59:399–416, 1954.

[32] Kenji Koike and Annegret Weng. Construction of CM Picard curves. Mathematics of Computation, 74:499–518, 2004.

[33] Serge Lang. Complex Multiplication, volume 255 of Grundlehren der mathematischen Wissenschaften. Springer, 1983.

[34] Joan-C. Lario and Anna Somoza. An inverse Jacobian algorithm for Picard curves (with an appendix by Christelle Vincent). Res. Number Theory, 7(2):32, 2021. arXiv:1611.07202.

[35] Hendrik W. Lenstra, Jr. Lattices. In J. Buhler and P. Stevenhagen, editors, Surveys in Algorithmic Number Theory, volume 44 of MSRI Publications, pages 127 – 181. Cambridge, 2008.

[36] Chloe Martindale. Hilbert modular polynomials. J. Number Theory, 213:464–498, 2020.
[37] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry* (Castiglioncello, 1990), volume 94 of Progr. Math., pages 313–334. Birkhäuser, 1991.

[38] Enea Milio and Damien Robert. Modular polynomials on Hilbert surfaces. *J. Number Theory*, 216:403–459, 2020. https://hal.archives-ouvertes.fr/hal-01520262v2

[39] Morris Newman. *Integral matrices*. Academic Press, 1972. Pure and Applied Mathematics, Vol. 45.

[40] Reinhard Schertz. Weber’s class invariants revisited. *Journal de Théorie des Nombres de Bordeaux*, 14(1):325–345, 2002.

[41] Goro Shimura. On canonical models of bounded symmetric domains I. *Ann of Math*, 91:144–222, 1970.

[42] Goro Shimura. On canonical models of bounded symmetric domains II. *Ann of Math*, 92:528–549, 1970.

[43] Goro Shimura. On some arithmetic properties of modular forms of one and several variables. *Ann. of Math. (2)*, 102(3):491–515, 1975.

[44] Goro Shimura. On the Fourier coefficients of modular forms of several variables. *Göttingen Nachr. Akad. Wiss.*, pages 261–268, 1975.

[45] Goro Shimura. Theta functions with complex multiplication. *Duke Mathematical Journal*, (4):673–696, 1976.

[46] Goro Shimura. On abelian varieties with complex multiplication. *Proc. London Math. Soc. (3)*, 34(1):85–86, 1977.

[47] Goro Shimura. On certain reciprocity-laws for theta functions and modular forms. *Acta Math.*, 141(1-2):35–71, 1978.

[48] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1994.

[49] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998. Sections 1–16 essentially appeared before in [50].

[50] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. 1961.

[51] Anna Somoza. PhD thesis, Universitat Politècnica de Catalunya and Universiteit Leiden, 2019. Inverse Jacobian and related topics for certain superelliptic curves.

[52] Jana Sotáková. Eta quotients of class fields of imaginary quadratic fields. MSc thesis, Universiteit Leiden and Universität Regensburg, https://hdl.handle.net/1887/3597051, 2017.

[53] Anne-Monika Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994. http://www.iem.uni-due.de/zahlentheorie/AES-KG2.pdf

[54] Harold M. Stark. L-functions at s = 1. IV. First derivatives at s = 0. *Adv. in Math.*, 35(4):197–235, 1980.

[55] William A. Stein et al. *Sage Mathematics Software (Version 8.6)*. The Sage Development Team, 2019. http://www.sagemath.org

[56] Marco Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universität Leiden, 2010. http://hdl.handle.net/1887/15572

[57] Marco Streng. *Recip, 2011–2023*. REpository of Complex multiplication SageMath code, formerly package for using Shimura’s RECIProcity law, version TODO https://bitbucket.org/mstreng/recip/

[58] Marco Streng. Computing Igusa class polynomials. *Math. Comp.*, 83:275–309, 2014. arXiv:0903.3766

[59] Andrew V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Math. Comp.*, 80(275):501–538, 2011.

[60] Andrew V. Sutherland. Accelerating the CM method. *LMS J. Comput. Math.*, 15:172–204, 2012.

[61] The PARI Group, Bordeaux. *PARI/GP, version 2.11.1*, 2018. available from http://pari.math.u-bordeaux.fr/

[62] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999.

[63] Heinrich Weber. *Algebraische Zahlen*, volume 3 of *Lehrbuch der Algebra*. Friedrich Vieweg, 1908.

[64] Annekret Weng. Hyperelliptic CM-curves of genus 3. *Journal of the Ramanujan Mathematical Society*, 16(4):339–372, 2001.

[65] Tonghai Yang. Rational structure of X(N) over Q and explicit Galois action on CM points. *Chin. Ann. Math. Ser. B*, 37(6):821–832, 2016.