MATHEMATICS OF COMPUTATION
Volume 83, Number 287, May 2014, Pages 1477–1488
S 0025-5718(2013)02769-X
Article electronically published on September 4, 2013

# CONSTRUCTING CLASS INVARIANTS

ARISTIDES KONTOGEORGIS

Abstract. Shimura reciprocity law allows us to verify that a modular function gives rise to a class invariant. Here we present a new method based on Shimura reciprocity that allows us not only to verify but to find new class invariants from a modular function of level $N$.

## 1. Introduction

It is well known that the ring class field of imaginary quadratic orders can be generated by evaluating the $j$-invariant at certain algebraic integers. There are many modular functions that can be used for the generation of the ring class field. In a series of articles [5], [7], [6], [19] A. Gee and P. Stevenhagen developed a method based on Shimura reciprocity law, in order to check whether a modular function gives rise to a class invariant. A necessary condition for this is the invariance of the modular function under the action of the group $G_N = (\mathcal{O}/N\mathcal{O})^*/\mathcal{O}^*$, where $\mathcal{O}$ is an order of a quadratic imaginary field.

So far it seems that all known class invariants were found out of luck or by extremely ingenious people like Ramanujan. The aim of this article is to provide a more systematic method for finding class invariants. In order for our method to work we need a finite dimensional vector space $V$ consisting of modular functions of level $N$ and an action of the group $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ on $V$. We can take as $V$ the space of generalized Weber functions defined in eq. (4.2) in section 4.1. We will use a combination of techniques from classical invariant theory [15] and Galois descent [2].

The structure of this article is as follows: In section 2 we give a very quick description of the technique based on Shimura reciprocity law for checking whether a modular function is a class invariant. The interested reader should consider the more detailed explanations found in [5], [7], [6], [19]. In section 3 we explain our main observation. The action of $G_N$ is given in terms of matrices but the function $\rho$ sending elements of the group $G_N$ to matrices is not a linear representation but a cocycle. Then we break the computation into two parts. The first part considers a subgroup $H$ of $G_N$ such that $\rho$ when restricted to $H$ is a linear representation. Classical invariant theory provides us with a set of $H$-invariant elements. The second part makes the observation that the quotient $G_N/H$ is isomorphic to the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, where $\zeta_N$ is a primitive $N$-th root of unity. Then

Received by the editor June 7, 2012 and, in revised form, October 30, 2012 and November 14, 2012.

2010 *Mathematics Subject Classification.* Primary 11R29, 11R37, 11Y40; Secondary 11R34.

This research has been co-financed by the European Union (European Social Fund - ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) - Research Funding Program: THALES: Reinforcement of the interdisciplinary and/or inter-institutional research and innovation.

Hilbert's 90th theorem ensures us that we can find a set of $G_N$ invariants. In section 4 we use our technique in the case of generalized Weber functions. We selected these modular functions since a lot of work has been done on them and also the action of $\mathrm{SL}(2,\mathbb{Z})$ on them is well understood. For a given prime number $N$ and a discriminant $D$ we are able to construct a whole $\mathbb{Q}$-vector space consisting of class invariants. A lot of examples are given and the magma code [1] used to compute them is freely available upon request.

## 2. Shimura reciprocity law

Let $\Gamma(N)$ be the kernel of the map $\mathrm{SL}(2,\mathbb{Z}) \mapsto \mathrm{SL}\left(2,\mathbb{Z}/N\mathbb{Z}\right)$. The group $\mathrm{SL}(2,\mathbb{Z})$ acts on the upper half plane $\mathbb{H}$ in terms of linear fractional transformations and is known to be generated by the elements $S : z \mapsto -\frac{1}{z}$ and $T : z \mapsto z+1$.

It is known that the quotient Riemann surface $\Gamma(N)\backslash\mathbb{H}^*$ can be defined over the field $\mathbb{Q}(\zeta_N)$, where $\zeta_N$ is a primitive $N$-th root of unity. We consider the function field $F_N$ of the corresponding curve defined over $\mathbb{Q}(\zeta_N)$. The function field $F_N$ is acted on by

$$\Gamma(N)/\{\pm 1\} \cong \mathrm{Gal}(F_N/F_1(\zeta_N)).$$

For an element $d \in \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^*$ we consider the automorphism $\sigma_d : \zeta_N \mapsto \zeta_N^d$. Since the Fourier coefficients of a function $h \in F_N$ are known to be in $\mathbb{Q}(\zeta_N)$, we consider the action of $\sigma_d$ on $F_N$ by applying $\sigma_d$ on the Fourier coefficients of $h$. In this way we define an arithmetic action of

$$\mathrm{Gal}(F_1(\zeta_N)/F_1) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^*,$$

on $F_N$. We have an action of the group $\mathrm{GL}\left(2,\frac{\mathbb{Z}}{N\mathbb{Z}}\right)$ on $F_N$ that fits in the following short exact sequence:

$$1 \rightarrow \mathrm{SL}\left(2,\frac{\mathbb{Z}}{N\mathbb{Z}}\right) \rightarrow \mathrm{GL}\left(2,\frac{\mathbb{Z}}{N\mathbb{Z}}\right) \xrightarrow{\det} \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^* \rightarrow 1.$$

A. Gee and P. Stevehagen [5], [7], [6], [19] proved the following theorem which was based on the work of Shimura [17]:

**Theorem 1.** *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic number field $K$ of discriminant $d < -4$. Suppose that a modular function $h \in F_N$ does not have a pole at $\theta$ and $\mathbb{Q}(j) \subset \mathbb{Q}(h)$. Denote by $x^2+Bx+C$ the minimum polynomial of $\theta$ over $\mathbb{Q}$. Then there is a subgroup $W_{N,\theta} \subset \mathrm{GL}\left(2,\frac{\mathbb{Z}}{N\mathbb{Z}}\right)$ with elements of the form:*

$$W_{N,\theta} = \left\{ \begin{pmatrix} t-Bs & -Cs \\ s & t \end{pmatrix} \in \mathrm{GL}\left(2,\frac{\mathbb{Z}}{N\mathbb{Z}}\right) : t\theta + s \in (\mathcal{O}/N\mathcal{O})^* \right\}.$$

*The function value $h(\theta)$ is a class invariant if and only if the group $W_{N,\theta}$ acts trivially on $h$.*

*Proof.* [5, cor. 4]. □

The above theorem can be applied in order to show that a modular function gives rise to a class invariant and was used with success in order to prove that several functions were indeed class invariants. Also A. Gee and P. Stevenhagen provided us with an explicit way of describing the Galois action of $\mathrm{Cl}(\mathcal{O})$ on the class invariant so that we can construct the minimal polynomial of the ring class field.

We will now describe an algorithm that will allow us to find class invariants. As a result we will obtain a whole $\mathbb{Q}$-vector space of class invariants.

Let $V$ be a finite dimensional vector space consisting of modular functions of level $N$ so that $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ acts on $V$. Notice that every element $a \in \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ can be written as $b\cdot\begin{pmatrix}1 & 0\\ 0 & d\end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$. The group $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ is generated by the elements $S = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ and $T = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. The action of $S$ on functions $g \in V$ is defined to be $g \circ S = g(-1/z) \in V$ and the action of $T$ is defined as $g \circ T = g(z+1) \in V$.

Here a technical difficulty arises: how can one compute efficiently the decomposition of an element in $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ as a product of the generators $S$, $T$? Observe that by the Chinese remainder theorem we can write

$$\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z}) = \prod_{p|N} \mathrm{GL}(2,\mathbb{Z}/p^{v_p(N)}\mathbb{Z}),$$

where $v_p(N)$ denotes the power of $p$ that appears in the decomposition in prime factors. Working with the general linear group over a field has advantages and one can use lemma 6 in [5] in order to express an element of determinant one in $\mathrm{SL}(2,\mathbb{Z}/p^{v_p(N)}\mathbb{Z})$ as word in elements $S_p, T_p$ where $S_p$ and $T_p$ are $2 \times 2$ matrices which reduce to $S$ and $T$ modulo $p^{v_p(N)}$ and to the identity modulo $q^{v_q(N)}$ for prime divisors $q$ of $N$, $p \neq q$.

This way the problem is reduced to the problem of finding the matrices $S_p, T_p$ (this is easy using the Chinese remainder theorem), and expressing them as products of $S, T$. For example, a matrix $S_7$ in $\mathrm{GL}(2,\mathbb{Z}/24\cdot 7\mathbb{Z})$ that reduces to $S$ modulo 7 but to the identity modulo 24 can be easily computed, $S_7 = \begin{pmatrix}49 & 48\\ 120 & 49\end{pmatrix}$. This matrix has determinant $-3359 \equiv 1 \mod 24 \cdot 7$. In order to decompose such a matrix as a product of $S, T$ elements we observe that left multiplication by $S$ interchanges the rows of a $2 \times 2$ matrix and also multiplies the first row by $-1$ while left multiplication by $T^k$ adds the second row multiplied by $k$ to the first. So by successive divisions and interchanges we can arrive at an upper triangular matrix of the form $\begin{pmatrix}\pm 1 & a\\ 0 & \pm 1\end{pmatrix}$. Then we can multiply by $S^2 = -\mathrm{Id}$ if necessary in order to arrive at a matrix of the form $T^a$. This algorithm was explained to me by V. Metaftsis. For the cases $N = 24\cdot 5$ and $N = 24\cdot 7$ using magma [1] we were able to compute that

$$\begin{aligned}
T_3 &= T^{-80},\\
T_8 &= T^{-15},\\
T_5 &= T^{-24},\\
S_3 &= S\cdot T^{-10}\cdot S\cdot T^{18}\cdot S^{-1}\cdot T^{10}\cdot S^{-1}\cdot T^{-18}\cdot S\cdot T^{-10}\cdot S\cdot T^{-10}\cdot S\cdot T^{-21}\cdot\\
&\quad \cdot S^{-1}\cdot T^{9}\cdot S^{-1}\cdot T^{77}\cdot S\cdot T^{5}\cdot S\cdot T^{2}\cdot S\cdot T^{5}\cdot S,\\
S_8 &= S^{-1}\cdot T^{-10}\cdot S\cdot T^{-10}\cdot S\cdot T^{-21}\cdot S^{-1}\cdot T^{9}\cdot S^{-1}\cdot T^{59}\cdot S\cdot T^{3}\cdot S\cdot T^{-4}\cdot S^{-1}\cdot\\
&\quad \cdot T^{9}\cdot S^{-1}\cdot T^{-6}\cdot S\cdot T^{8}\cdot S\cdot T^{2}\cdot S\\
S_5 &= S^{-1}\cdot T^{11}\cdot S\cdot T^{11}\cdot S^{-1}\cdot T^{11}\cdot S\cdot T^{-10}\cdot S\cdot T^{18}\cdot S^{-1}\cdot T^{10}\cdot S^{-1}\cdot T^{-18}\cdot\\
&\quad \cdot S\cdot T^{-10}\cdot S\cdot T^{-10}\cdot S\cdot T^{-21}\cdot S^{-1}\cdot T^{9}\cdot S^{-1}\cdot T^{64}\cdot S\cdot T^{5}\cdot S\cdot T^{5}\cdot S
\end{aligned}$$

and

$$\begin{aligned}
T_3 &= T^{-56}, \\
T_8 &= T^{-63}, \\
T_7 &= T^{-48}, \\
S_3 &= S^{-1} \cdot T^{41} \cdot S \cdot T^{41} \cdot S^{-1} \cdot T^{101} \cdot S \cdot T^4 \cdot S \cdot T^4 \cdot S \cdot T^4 \cdot S \\
S_8 &= S^{-1} \cdot T^{41} \cdot S \cdot T^{41} \cdot S^{-1} \cdot T^{41} \cdot S \cdot T^{11} \cdot S^2 \cdot T^{-8} \cdot S \cdot T^{-40} \cdot \\
&\quad \cdot S^{-1} \cdot T^{40} \cdot S^{-1} \cdot T^{19} \cdot S^{-1} \cdot T^{-37} \cdot S \cdot T^3 \cdot S \cdot T^3 \cdot S \cdot T^3 \cdot S \\
S_7 &= S^{-1} \cdot T^{41} \cdot S \cdot T^{41} \cdot S^{-1} \cdot T^{41} \cdot S \cdot T^{-8} \cdot S \cdot T^{-40} \cdot S^{-1} \cdot T^{40} \cdot S^{-1} \cdot T^8 \cdot S \cdot \\
&\quad \cdot T^{-8} \cdot S \cdot T^{-40} \cdot S^{-1} \cdot T^{40} \cdot S^{-1} \cdot T^{22} \cdot S \cdot T^4 \cdot S \cdot T^2 \cdot S \cdot T^4 \cdot S,
\end{aligned}$$

respectively.

The action of the matrix $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ is given by the action of the elements $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on the Fourier coefficients of the expansion at the cusp at infinity [5]. Since every element in $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ can be written as a word in $S, T$ we obtain a function $\rho$:

$$\begin{tikzcd} \left(\frac{\mathcal{O}}{N\mathcal{O}}\right)^* \arrow[r, "\phi"] \arrow[rr, bend left, "\rho"] & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{GL}(V), \end{tikzcd} \tag{2.1}$$

where $\phi$ is the natural homomorphism given by Theorem 1.

## 3. Finding class invariants

The map $\rho$ defined in eq. (2.1) in the previous section is not a homomorphism. Indeed, if $e_1, \ldots, e_m$ is a basis of $V$, then the action of $\sigma$ is given in matrix notation as

$$e_i \circ \sigma = \sum_{\nu=1}^{m} \rho(\sigma)_{\nu,i} e_\nu,$$

and then since $(e_i \circ \sigma) \circ \tau = e_i \circ (\sigma\tau)$ we obtain

$$e_i \circ (\sigma\tau) = \sum_{\nu,\mu=1}^{m} \rho(\sigma)^{\tau}_{\nu,i} \rho(\tau)_{\mu,\nu} e_\mu.$$

Notice that the elements $\rho(\sigma)_{\nu,i} \in \mathbb{Q}(\zeta_N)$ and $\tau \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ act on them as well by the element $\sigma_{\det(\tau)} \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. So we arrive at the following:

**Proposition 2.** *The map $\rho$ defined in eq. (2.1) satisfies the cocycle condition*

$$\rho(\sigma\tau) = \rho(\tau)\rho(\sigma)^{\tau} \tag{3.1}$$

*and gives rise to a class in $H^1(G, \mathrm{GL}(V))$, where $G = (\mathcal{O}/N\mathcal{O})^*$. The restriction of the map $\rho$ in the subgroup $H$ of $G$ defined by*

$$H := \{x \in G : \det(\phi(x)) = 1\}$$

*is a homomorphism.*

*Remark* 3. Notice that $H^1(G, \mathrm{GL}(V))$ has the structure of a group only if $\mathrm{GL}(V)$ is abelian, i.e., only if $\dim V = 1$. In the case $\dim V \geq 2$ the set $H^1(G, \mathrm{GL}(V))$ has only the structure of a set with a distinguished element.

The basis elements $e_1, \dots e_m$ are modular functions so there is a natural notion of multiplication for them. We will consider the polynomial algebra $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]$. The group $H$ acts on this algebra in terms of the linear representation $\rho$ (recall that $\rho$ when restricted to $H$ is a homomorphism).

Classical invariant theory provides us with effective methods (Reynolds operator method, linear algebra method [10]) in order to compute the ring of invariants $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H$. Also, there is a well defined action of the quotient group $G/H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H$.

Define the vector space $V_n$ of invariant polynomials of given degree $n$:

$$V_n := \{F \in \mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H : \deg F = n\}.$$

*Remark* 4. For the applications in elliptic curves construction or in effective generation of the Hilbert class field we have to take the smallest degree $n$ such that $V_n \neq \{0\}$. Indeed, it is known that there is a polynomial relation $F(f, j)$ among the functions $j, f$, where $j$ is the $j$-invariant, since the function field $F_N$ has transcendence degree 1. It is known that this polynomial relation controls asymptotically the logarithmic height $H(P_f)$, $H(P_j)$ of the minimal polynomial of $f$ and $j$ in the following way:

$$\lim_{h(j(\tau))\to\infty} \frac{H(P_j)}{H(P_f)} = \frac{\deg_f F(f,j)}{\deg_j F(f,j)} =: r(f)$$

where the limit is taken over all CM-points $\mathrm{SL}(2,\mathbb{Z})\tau \in \mathbb{H}$ [4]. So the best result comes when the $\deg_f F(f,j)$ is large compared to $\deg_j F(f,j)$.

The action of $G/H$ on $V_n$ gives rise to a cocycle

$$\rho' \in H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), \mathrm{GL}(V_n)).$$

The multidimensional Hilbert 90 theorem asserts that there is an element $P \in \mathrm{GL}(V_n)$ such that

$$\rho'(\sigma) = P^{-1}P^{\sigma}. \tag{3.2}$$

Let $v_1, \dots, v_\ell$ be a basis of $V_n$. The elements $v_i$ are by construction $H$ invariant. The elements $w_i := v_i P^{-1}$ are $G/H$ invariant since

$$(v_iP^{-1}) \circ \sigma = (v_i \circ \sigma)(P^{-1})^{\sigma} = v_i\rho(\sigma)(P^{-1})^{\sigma} = v_iP^{-1}P^{\sigma}(P^{-1})^{\sigma} = v_iP^{-1}.$$

The above computation together with Theorem 1 allows us to prove

**Proposition 5.** *Consider the polynomial ring $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]$ and the vector space $V_n$ of $H$-invariant homogenous polynomials of degree $n$. If $P$ is a matrix such that eq. (3.2) holds, then the images of a basis of $V_n$ under the action of $P^{-1}$ are class invariants.*

How can we compute the matrix $P$ so that eq. (3.2) holds? We will use a version of the Glasby-Howlett probabilistic algorithm [8]. We consider the sum

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^{\sigma}. \tag{3.3}$$

If we manage to find a $2 \times 2$ matrix in $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ such that $B_Q$ is invertible, then $P := B_Q^{-1}$. Indeed, we compute that

$$B_Q^{\tau} = \sum_{\sigma \in G/H} \rho(\sigma)^{\tau} Q^{\sigma\tau}, \tag{3.4}$$

and the cocycle condition $\rho(\sigma\tau) = \rho(\sigma)^\tau \rho(\tau)$, together with eq. (3.4) allows us to write:

$$B_Q^\tau = \sum_{\sigma \in G/H} \rho(\sigma\tau)\rho(\tau)^{-1} Q^{\sigma\tau} = B_Q \rho_\tau^{-1},$$

i.e.

$$\rho(\tau) = B_Q \left(B_Q^\tau\right)^{-1}.$$

In order to obtain an invertible element $B_Q$ we feed eq. (3.4) with random matrices $Q$ until $B_Q$ is invertible. Since noninvertible matrices are rare (they form a Zariski closed subset in the space of matrices) our first random choice of $Q$ always worked!

## 4. Examples

Consider the generalized Weber functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ defined in the work of A. Gee in [6, p. 73] as

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)},\ \mathfrak{g}_1(\tau) = \zeta_{24}^{-1} \frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},\ \mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)},\ \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

where $\eta$ denotes the Dedekind eta function:

$$\eta(\tau) = e^{2\pi i\tau/24} \prod_{n \geq 1} (1 - q^n) \ \ \tau \in \mathbb{H}, q = e^{2\pi i \tau}.$$

These are modular functions of level 72. In our previous work [14] we investigated the action of the group $W_{N,\theta}$ for the $n \equiv 19 \mod 24$ case on these modular functions and we showed that the group $G := W_{72,\theta}$ induces an action of the generalized symmetric group $\mu(12) \rtimes S_4$ on them. Any element $g$ of $G$ induces a matrix action by expressing $\mathfrak{g_i}^g$, $i = 0, 1, 2, 3$, as a linear combination of the functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$. This way we obtain a map

$$\rho : G \to \mathrm{GL}(4, \mathbb{Q}(\zeta_{72})) = \mathrm{Aut}\left(\langle \mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3 \rangle_{\mathbb{Q}(\zeta_{72})}\right). \tag{4.1}$$

In order to overcome the cocycle problem we raised everything to the 12-th power. This way the corresponding action

$$\rho_{12} : G \to \mathrm{GL}(4, \mathbb{Q}(\zeta_{72})) = \mathrm{Aut}\left(\langle \mathfrak{g}_0^{12}, \mathfrak{g}_1^{12}, \mathfrak{g}_2^{12}, \mathfrak{g}_3^{12} \rangle_{\mathbb{Q}(\zeta_{72})}\right)$$

becomes a group representation and we were able to find invariants of the action that lead to class invariants by just applying the methods of classical invariant theory for linear actions. This approach has a disadvantage; the class invariants we produce give rise to class polynomials with large coefficients.

We consider the subgroup $H$ of $G$ defined by $H := G \cap \mathrm{SL}\left(2, \frac{\mathbb{Z}}{72\mathbb{Z}}\right)$. When we restrict the map $\rho$ of eq. (4.1) we obtain a linear action and then we can construct the invariant polynomials of this action. Notice that there are no invariant polynomials of degree 1 for $H$. But we can find invariant polynomials of degree 2. For example for $n = -571$ the group $H$ has order 144 and $G$ has order 3456. We find that the polynomials

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^6 \mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^6)\mathfrak{g}_1\mathfrak{g}_2$$

are indeed invariants of the action of $H$. Then we consider the action of $G/H$, which is an abelian group of order 24 isomorphic to the group $\mathrm{Gal}(\mathbb{Q}(\zeta_{72})/\mathbb{Q})$. The quotient map gives rise to an action of

$$\bar{\rho} : G/H \to \mathrm{GL}\big(2, \mathbb{Q}(\zeta_{72})\big) = \mathrm{Aut}\big(\langle I_1, I_2 \rangle_{\mathbb{Q}(\zeta_{72})}\big).$$

TABLE 1. Minimal polynomials using the $\mathfrak{g}_0, \dots, \mathfrak{g}_3$ functions.

| Invariant | polynomial |
|---|---|
| Hilbert | $t^5 + 400497845154831586723701480652800t^4 +$<br>$818520809154613065770038265334290448384t^3 +$<br>$4398250752422094811238689419574422303726895104t^2$<br>$-1631973097517620390627491371591386284451254239232 0t$<br>$+1528305445367280381806642165003665364623231519241 0112$ |
| $\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}$ | $t^5 - 5433338830617345268674t^4 + 9070591351954265832477808 8t^3$<br>$-30493571775300305358117516197 28t^2$<br>$-39007182691222144243104374168 6448t$<br>- 12509992052647780072147837007511456 |
| $e_1$ | $t^5 - 936t^4 - 60912t^3 - 2426112t^2 - 40310784t - 3386105856$ |
| $e_2$ | $t^5 - 1512t^4 - 29808t^3 + 979776t^2 + 3359232t - 423263232$ |

The map $\bar{\rho}$ is again a cocycle in

$$H^1(G/H, \mathrm{GL}(2, \mathbb{Q}(\zeta_{72}))) = H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_{72})/\mathbb{Q}), \mathrm{GL}(2, \mathbb{Q}(\zeta_{72}))) = 0$$

by the multidimensional Hilbert 90 theorem. Therefore there is an element $P \in \mathrm{GL}(2, \mathbb{Q}(\zeta_{72}))$ such that

$$\bar{\rho}(\sigma) = P^{\sigma} P^{-1}.$$

The elements $(I_1, I_2) \cdot P =: (e_1, e_2)$ given by

$$e_1 := (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + 12\zeta_{72}^{6}\mathfrak{g}_0\mathfrak{g}_3 + 12\mathfrak{g}_1\mathfrak{g}_2 + 12\mathfrak{g}_1\mathfrak{g}_3,$$

$$e_2 := 12\zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_2 + (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + (-12\zeta_{72}^{12} + 12)\mathfrak{g}_1\mathfrak{g}_3 + 12\zeta_{72}^{12}\mathfrak{g}_1\mathfrak{g}_3$$

generate a $\mathbb{Q}$-vector space of class invariants.

In Table 1 we write down the Hilbert polynomial corresponding to the $j$-invariant, the invariant corresponding to $\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}$ and the polynomials corresponding to $e_1$ and $e_2$. We also examine the polynomial $\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}$ since it is one of the few class invariants known in the $D \equiv 5 \mod 24$ case.

4.1. **Generalized Weber functions.** The Weber and $\mathfrak{g}_i$ functions are special cases of the so-called *generalized Weber functions* defined as:

$$\nu_{N,0} := \sqrt{N}\frac{\eta \circ \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}}{\eta} \text{ and } \nu_{k,N} := \frac{\eta \circ \begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}}{\eta}, \ 0 \leq k \leq N-1. \tag{4.2}$$

These are known to be modular functions of level $24N$ [6, th. 5, p. 76]. Notice that $\sqrt{N} \in \mathbb{Q}(\zeta_N) \subset \mathbb{Q}(\zeta_{24 \cdot N})$ and an explicit expression of $\sqrt{N}$ in terms of $\zeta_N$ can be given by using Gauss sums [3, 3.14 p. 228].

The group $\mathrm{SL}(2, \mathbb{Z})$ acts on the $(N+1)$-th dimensional vector space generated by them. In order to describe this action we have to describe the action of the two generators $S, T$ of $\mathrm{SL}(2, \mathbb{Z})$ given by $S : z \mapsto -\frac{1}{z}$ and $T : z \mapsto z + 1$. Keep in mind that

$$\eta \circ T(z) = \zeta_{24}\eta(z) \text{ and } \eta \circ S(z) = \zeta_8^{-1}\sqrt{iz}\eta(z).$$

We compute that (see also [6, p.77])

$$\nu_{N,0} \circ S = \nu_{0,N} \text{ and } \nu_{N,0} \circ T = \zeta_{24}^{N-1}\nu_{N,0},$$

$$\nu_{0,N} \circ S = \nu_{N,0} \text{ and } \nu_{0,N} \circ T = \zeta_{24}^{-1}\nu_{1,N},$$

TABLE 2. Invariants for the group of elements of determinant 1 for $N = 7$ and $n = 91$

$$\begin{aligned}
I_1 &= {\nu_{N,0}}^2 - {\nu_{0,N}}^2 + \left(-\zeta^{42} + \zeta^{14}\right) {\nu_{1,N}}^2 + \left(\zeta^{28} - 1\right) {\nu_{2,N}}^2 - \zeta^{42} {\nu_{3,N}}^2 - \zeta^{14} {\nu_{5,N}}^2 + {\nu_{6,N}}^2, \\
I_2 &= \nu_{N,0}\, \nu_{0,N} + \zeta^{35} \nu_{N,0}\, \nu_{1,N} - \zeta^{28} \nu_{0,N}\, \nu_{2,N} + \zeta^{35} \nu_{1,N}\, \nu_{6,N} - \zeta^{35} \nu_{2,N}\, \nu_{5,N} + \\
&\quad \left(\zeta^{42} - \zeta^{14}\right) \nu_{3,N}\, \nu_{5,N} + \zeta^{21} \nu_{3,N}\, \nu_{6,N}, \\
I_3 &= \nu_{N,0}\, \nu_{2,N} + \left(\zeta^{28} - 1\right) \nu_{N,0}\, \nu_{6,N} + \zeta^{7} \nu_{0,N}\, \nu_{1,N} + \left(-\zeta^{35} + \zeta^{7}\right) \nu_{0,N}\, \nu_{5,N} \\
&\quad +\zeta^{28} \nu_{1,N}\, \nu_{3,N} + \left(\zeta^{35} - \zeta^{7}\right) \nu_{2,N}\, \nu_{3,N} - \zeta^{21} \nu_{5,N}\, \nu_{6,N}, \\
I_4 &= \nu_{N,0}\, \nu_{3,N} + \left(-\zeta^{42} + \zeta^{14}\right) \nu_{N,0}\, \nu_{5,N} + \zeta^{42} \nu_{0,N}\, \nu_{3,N} + \left(-\zeta^{35} + \zeta^{7}\right) \nu_{0,N}\, \nu_{6,N} - \zeta^{42} \nu_{1,N}\, \nu_{2,N} + \\
&\quad \left(\zeta^{35} - \zeta^{7}\right) \nu_{1,N}\, \nu_{5,N} + \left(-\zeta^{45} + \zeta^{37} + \zeta^{33} - \zeta^{25} + \zeta^{17} + \zeta^{13} - \zeta^{5} - \zeta\right) \nu_{2,N}\, \nu_{6,N}, \\
I_5 &= \nu_{N,0}\, \nu_{4,N} + \zeta^{42} \nu_{0,N}\, \nu_{4,N} + \left(-\zeta^{45} + \zeta^{37} + \zeta^{33} - \zeta^{25} - \zeta^{21} + \zeta^{17} + \zeta^{13} - \zeta^{5} - \zeta\right) \nu_{1,N}\, \nu_{4,N} - \\
&\quad \zeta^{28} \nu_{2,N}\, \nu_{4,N} + \left(\zeta^{35} - \zeta^{7}\right) \nu_{3,N}\, \nu_{4,N} + \\
&\quad \left(-\zeta^{45} + \zeta^{37} + \zeta^{33} - \zeta^{25} + \zeta^{17} + \zeta^{13} - \zeta^{5} - \zeta\right) \nu_{4,N}\, \nu_{5,N} + \nu_{4,N}\, \nu_{6,N}, \\
I_6 &= {\nu_{4,N}}^2
\end{aligned}$$

for $1 \leq k < N-1$ and $N$ is prime:

$$\nu_{k,N} \circ S = \left(\frac{-c}{n}\right) i^{\frac{1-n}{2}} \zeta_{24}^{N(k-c)} \text{ and } \nu_{k,N} \circ T = \zeta_{24}^{-1} \nu_{k+1,N},$$

where $c = -k^{-1} \mod N$. The computation of the action of $S$ on $\eta$ is the most difficult, see [9, eq. 8, p. 443].

Assume that $N = 5$ and $D = -91$. We compute that the group $H$ of determinant 1 has invariants

$$\nu_{5,0} + (\zeta^{25} - \zeta^{5})\nu_{3,5} \text{ and } \nu_{0,5} + (\zeta^{31} - \zeta^{23} - \zeta^{19} - \zeta^{15} + \zeta^{7} + \zeta^{3})\nu_{1,5}.$$

Using our method we arrive at the final invariants:

$$\begin{aligned}
I_1 &= (-1224\zeta^{28} + 612\zeta^{20} + 2740\zeta^{16} + 1516\zeta^{4} - 612)\nu_{5,0} \\
&\quad +(4256\zeta^{28} - 2128\zeta^{20} - 1516\zeta^{16} + 2740\zeta^{4} + 2128)\nu_{0,5} \\
&\quad +(-1224\zeta^{31} - 2740\zeta^{27} + 612\zeta^{15} + 1224\zeta^{11} + 1516\zeta^{3})\nu_{1,5} \\
&\quad +(1516\zeta^{29} - 612\zeta^{25} + 1224\zeta^{13} - 1516\zeta^{9} - 2740\zeta)\nu_{3,5},
\end{aligned}$$

$$\begin{aligned}
I_2 &= (-1952\zeta^{28} + 976\zeta^{20} + 2128\zeta^{16} + 176\zeta^{4} - 976)\nu_{5,0} \\
&\quad +(2304\zeta^{28} - 1152\zeta^{20} - 176\zeta^{16} + 2128\zeta^{4} + 1152)\nu_{0,5} \\
&\quad +(-1952\zeta^{31} - 2128\zeta^{27} + 976\zeta^{15} + 1952\zeta^{11} + 176\zeta^{3})\nu_{1,5} \\
&\quad +(176\zeta^{29} - 976\zeta^{25} + 1952\zeta^{13} - 176\zeta^{9} - 2128\zeta)\nu 3, 5.
\end{aligned}$$

The $\mathbb{Q}$-vector space generated by these two functions consists of class functions. We can now compute the corresponding polynomials:

$$t^2 - 3060t - 28090800 \text{ and } t^2 - 4880t - 71443200.$$

Just for comparison the Hilbert polynomial corresponding to the $j$ invariant is:

$$t^2 + 10359073013760t - 3845689020776448.$$

For $N = 7$ and $n = 91$ we have computed the invariants for the group $H$ of elements of determinant 1 and we present the results in Table 2. On these invariants the group $\mathrm{Gal}(\mathbb{Q}(\zeta_{24\cdot 7})/\mathbb{Q})$ acts and we finally arrive at six invariant functions that over $\mathbb{Q}$ generate a vector space of invariant polynomials. We present in Table 3 just one of them.

TABLE 3. An invariant coming from generalized Weber functions for $N = 7$

$$\begin{aligned}
F_1 \quad = \quad & (-4\zeta^{44} + 4\zeta^{36} + 4\zeta^{32} + 4\zeta^{16} - 4\zeta^{4} + 48)\nu_{N,0}^2 \\
& +(4\zeta^{46} + 12\zeta^{42} - 4\zeta^{38} - 4\zeta^{34} - 4\zeta^{30} + 4\zeta^{26} + 4\zeta^{22} - 4\zeta^{14} + 4\zeta^{6} + 4\zeta^{2})\nu_{N,0}\nu_{0,N} \\
& +(-8\zeta^{45} + 4\zeta^{41} + 8\zeta^{37} + 8\zeta^{33} - 8\zeta^{25} - 8\zeta^{21} + 12\zeta^{17} + 8\zeta^{13} - 12\zeta^{5} - 8\zeta)\nu_{N,0}\nu_{1,N} \\
& +(-4\zeta^{36} + 16\zeta^{28} - 4\zeta^{16} + 4\zeta^{8} + 4\zeta^{4})\nu_{N,0}\nu_{2,N} \\
& +(16\zeta^{47} - 28\zeta^{35} + 16\zeta^{27} - 16\zeta^{19} + 28\zeta^{7} + 16\zeta^{3})\nu_{N,0}\nu_{3,N} \\
& +(-8\zeta^{38} - 8\zeta^{34} + 8\zeta^{26} + 16\zeta^{14} + 8\zeta^{6})\nu_{N,0}\nu_{4,N} \\
& +(12\zeta^{45} - 28\zeta^{37} - 12\zeta^{33} + 28\zeta^{25} - 12\zeta^{17} - 12\zeta^{13} + 12\zeta^{5} + 28\zeta)\nu_{N,0}\nu_{5,N} \\
& +(-4\zeta^{44} + 4\zeta^{36} + 4\zeta^{32} + 4\zeta^{16} - 4\zeta^{4} - 16)\nu_{N,0}\nu_{6,N} \\
& +(4\zeta^{44} - 4\zeta^{36} - 4\zeta^{32} - 4\zeta^{16} + 4\zeta^{4} - 48)\nu_{0,N}^2 \\
& +(-4\zeta^{43} + 16\zeta^{35} - 4\zeta^{23} + 4\zeta^{15} + 4\zeta^{11})\nu_{0,N}\nu_{1,N} \\
& +(-4\zeta^{46} - 12\zeta^{42} + 4\zeta^{30} - 4\zeta^{22} + 12\zeta^{14} - 4\zeta^{2})\nu_{0,N}\nu_{2,N} \\
& +(16\zeta^{45} + 16\zeta^{41} - 16\zeta^{33} + 28\zeta^{21} - 16\zeta^{13})\nu_{0,N}\nu_{3,N} \\
& +(-8\zeta^{44} + 8\zeta^{32} + 24\zeta^{28} + 8\zeta^{8} - 24)\nu_{0,N}\nu_{4,N} \\
& +(-4\zeta^{47} - 4\zeta^{43} + 4\zeta^{35} - 4\zeta^{27} - 4\zeta^{23} + 4\zeta^{19} + 4\zeta^{15} + 4\zeta^{11} + 12\zeta^{7} - 4\zeta^{3})\nu_{0,N}\nu_{5,N} \\
& +(16\zeta^{46} - 12\zeta^{42} - 16\zeta^{38} - 16\zeta^{34} - 16\zeta^{30} + 16\zeta^{26} + 16\zeta^{22} - 16\zeta^{14} + 16\zeta^{6} + 16\zeta^{2})\nu_{0,N}\nu_{6,N} \\
& +(4\zeta^{46} - 48\zeta^{42} - 4\zeta^{30} + 4\zeta^{22} + 48\zeta^{14} + 4\zeta^{2})\nu_{1,N}^2 \\
& +(-16\zeta^{45} - 16\zeta^{41} + 16\zeta^{33} - 28\zeta^{21} + 16\zeta^{13})\nu_{1,N}\nu_{2,N} \\
& +(-4\zeta^{44} + 4\zeta^{32} + 16\zeta^{28} + 4\zeta^{8} - 16)\nu_{1,N}\nu_{3,N} \\
& +(8\zeta^{47} + 8\zeta^{43} - 8\zeta^{35} + 8\zeta^{27} + 8\zeta^{23} - 8\zeta^{19} - 8\zeta^{15} - 8\zeta^{11} - 16\zeta^{7} + 8\zeta^{3})\nu_{1,N}\nu_{4,N} \\
& +(-16\zeta^{46} + 12\zeta^{42} + 16\zeta^{38} + 16\zeta^{34} + 16\zeta^{30} - 16\zeta^{26} - 16\zeta^{22} + 16\zeta^{14} - 16\zeta^{6} - 16\zeta^{2})\nu_{1,N}\nu_{5,N} \\
& +(-8\zeta^{45} + 4\zeta^{41} + 8\zeta^{37} + 8\zeta^{33} - 8\zeta^{25} - 8\zeta^{21} + 12\zeta^{17} + 8\zeta^{13} - 12\zeta^{5} - 8\zeta)\nu_{1,N}\nu_{6,N} \\
& +(4\zeta^{44} - 4\zeta^{32} + 48\zeta^{28} - 4\zeta^{8} - 48)\nu_{2,N}^2 \\
& +(4\zeta^{47} + 4\zeta^{43} - 4\zeta^{35} + 4\zeta^{27} + 4\zeta^{23} - 4\zeta^{19} - 4\zeta^{15} - 4\zeta^{11} - 12\zeta^{7} + 4\zeta^{3})\nu_{2,N}\nu_{3,N} \\
& +(-8\zeta^{46} - 24\zeta^{42} + 8\zeta^{38} + 8\zeta^{34} + 8\zeta^{30} - 8\zeta^{26} - 8\zeta^{22} + 8\zeta^{14} - 8\zeta^{6} - 8\zeta^{2})\nu_{2,N}\nu_{4,N} \\
& +(8\zeta^{45} - 4\zeta^{41} - 8\zeta^{37} - 8\zeta^{33} + 8\zeta^{25} + 8\zeta^{21} - 12\zeta^{17} - 8\zeta^{13} + 12\zeta^{5} + 8\zeta)\nu_{2,N}\nu_{5,N} \\
& +(16\zeta^{36} + 12\zeta^{28} + 16\zeta^{16} - 16\zeta^{8} - 16\zeta^{4})\nu_{2,N}\nu_{6,N} \\
& +(4\zeta^{46} - 48\zeta^{42} - 4\zeta^{38} - 4\zeta^{34} - 4\zeta^{30} + 4\zeta^{26} + 4\zeta^{22} - 4\zeta^{14} + 4\zeta^{6} + 4\zeta^{2})\nu_{3,N}^2 \\
& +(-16\zeta^{45} + 8\zeta^{41} + 16\zeta^{37} + 16\zeta^{33} - 16\zeta^{25} - 16\zeta^{21} + 24\zeta^{17} + 16\zeta^{13} - 24\zeta^{5} - 16\zeta)\nu_{3,N}\nu_{4,N} \\
& +(4\zeta^{36} - 12\zeta^{28} + 4\zeta^{16} - 4\zeta^{8} - 4\zeta^{4})\nu_{3,N}\nu_{5,N} \\
& +(4\zeta^{47} + 8\zeta^{35} + 4\zeta^{27} - 4\zeta^{19} - 8\zeta^{7} + 4\zeta^{3})\nu_{3,N}\nu_{6,N} \\
& +(-12\zeta^{36} + 12\zeta^{28} - 12\zeta^{16} + 12\zeta^{8} + 12\zeta^{4})\nu_{4,N}^2 \\
& +(8\zeta^{47} + 16\zeta^{35} + 8\zeta^{27} - 8\zeta^{19} - 16\zeta^{7} + 8\zeta^{3})\nu_{4,N}\nu_{5,N} \\
& +(-8\zeta^{38} - 8\zeta^{34} + 8\zeta^{26} + 16\zeta^{14} + 8\zeta^{6})\nu_{4,N}\nu_{6,N} \\
& +(-4\zeta^{38} - 4\zeta^{34} + 4\zeta^{26} - 52\zeta^{14} + 4\zeta^{6})\nu_{5,N}^2 \\
& +(16\zeta^{45} - 12\zeta^{37} - 16\zeta^{33} + 12\zeta^{25} - 16\zeta^{17} - 16\zeta^{13} + 16\zeta^{5} + 12\zeta)\nu_{5,N}\nu_{6,N} \\
& +(-4\zeta^{44} + 4\zeta^{36} + 4\zeta^{32} + 4\zeta^{16} - 4\zeta^{4} + 48)\nu_{6,N}^2,
\end{aligned}$$

The corresponding polynomials for each class invariant are

$$\begin{array}{ll}
t^2 + (420 - 8\sqrt{-91})t - 20048, & t^2 + (672 + 40\sqrt{-91})t - 57344, \\
t^2 + (672 + 112\sqrt{-91})t - 137984, & t^2 + (1218 + 30\sqrt{-91})t - 171136, \\
t^2 + (630 - 66\sqrt{-91})t - 74592, & t^2 + (798 + 54\sqrt{-91})t - 91168.
\end{array}$$

Notice that the class polynomials have coefficients in $\mathcal{O} = \mathbb{Z}[\theta]$. Only if the value of the class function at $\theta$ is real, then the class polynomial is in $\mathbb{Z}[t]$. For the construction of elliptic curves this is not a problem; we still can take the coefficients modulo a prime ideal of $\mathcal{O}$ above $p$ and the values are either in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$.

## 5. Comparison — conclusions

How effective are the polynomials constructed by this method compared to other methods? Let us compute the Hilbert class field of $\mathbb{Q}(\sqrt{-299}) = \mathbb{Q}(\sqrt{D})$. Using our method we arrive at the following invariants

$$\begin{aligned}
I_1 &= 12\zeta^{12}\mathfrak{g}_0^2 + (-12\zeta^{12} + 12)\mathfrak{g}_1^2 + 36\mathfrak{g}_2\mathfrak{g}_3,\\
I_2 &= 36\zeta^{12}\mathfrak{g}_0^2 + 12\mathfrak{g}_2\mathfrak{g}_3,\\
I_3 &= 24\zeta^{12}\mathfrak{g}_0^2 + (-12\zeta^{18} + 24\zeta^{6})\mathfrak{g}_0\mathfrak{g}_1 + 24\mathfrak{g}_2\mathfrak{g}_3,\\
I_4 &= 12\zeta^{12}\mathfrak{g}_0^2 + (-12\zeta^{18} + 24\zeta^{6})\mathfrak{g}_0\mathfrak{g}_1 + 36\mathfrak{g}_2\mathfrak{g}_3,
\end{aligned}$$

with corresponding minimal polynomials

$$\begin{aligned}
P_1 = {} & T^8 - 132T^7 - 3600T^6 - 1057536T^5 + 67578624T^4 + 2988223488T^3 +\\
& 159765073920T^2 + 5279816908800T + 59659100356608,\\
P_2 = {} & T^8 + (-36\sqrt{D} - 240)T^7 + (-1080\sqrt{D} + 37656)T^6 + (163296\sqrt{D} + 6612192)T^5 +\\
& (19346688\sqrt{D} + 50471424)T^4 + (630415872\sqrt{D} - 19422706176)T^3 +\\
& (-5925685248\sqrt{D} - 990861465600)T^2 + (-1731321298944\sqrt{D} + 1227669405696)T -\\
& 75541764243456\sqrt{D} - 516837998592,\\
P_3 = {} & T^8 + (-24\sqrt{D} - 612)T^7 + (-864\sqrt{D} + 27504)T^6 + (-82944\sqrt{D} + 4126464)T^5 +\\
& (26002944\sqrt{D} + 3939840)T^4 + (376233984\sqrt{D} - 5667397632)T^3 +\\
& (-14941863936\sqrt{D} - 771342372864)T^2 + (-264582070272\sqrt{D} + 27642125795328)T +\\
& 13454127267840\sqrt{D} - 355534235172864,\\
P_4 = {} & T^8 + (-12\sqrt{D} - 516)T^7 + (-504\sqrt{D} - 72)T^6 + (10368\sqrt{D} + 3680640)T^5 +\\
& (20476800\sqrt{D} + 273849984)T^4 + (-430728192\sqrt{D} - 22758423552)T^3 +\\
& (-39195518976\sqrt{D} - 559365875712)T^2 + (-114339299328\sqrt{D} + 36926863884288)T +\\
& 55540735672320\sqrt{D} + 99976764063744
\end{aligned}$$

These are smaller than the coefficients of the Hilbert polynomial by a factor of logarithmic height up to 6 but are not as efficient as the Ramanujan class invariant corresponding to

$$\mathfrak{g}_2\mathfrak{g}_3 = \frac{1}{48}I_2 - \frac{1}{16}I_3 + \frac{1}{16}I_4,$$

which has a very small minimal polynomial

$$T^8 + T^7 - T^6 - 12T^5 + 16T^4 - 12T^3 + 15T^2 - 13T + 1.$$

How can we select the most efficient class invariant? Notice that every element in the $\mathbb{Q}$-vector space generated by the invariants $I_i$ constructed by our algorithm is a class invariant. Also all elements in the $\mathbb{Z}$-module generated by $I_i$ will give rise to class invariants with coefficients in $\mathcal{O}$. Of course (as the above example in $\mathbb{Q}(\sqrt{-299})$ indicates) there might be elements of the form $\sum \lambda_i I_i$ with some $\lambda_i \in \mathbb{Q} - \mathbb{Z}$. So far it seems a difficult problem to select the most efficient class function among all class functions. This problem is equivalent to minimizing the logarithmic height function on a lattice and seems out of reach for now. For the case of generalized Weber functions it seems that monomials of the Weber invariants are the best choices. However there are cases, for example the $D \equiv 5 \mod 24$ case, where no monomial invariants exist. Our method in this case provides much better invariants than the invariants constructed in [14], as one can see from Table 1.

## Acknowledgment

We would like to thank V. Metaftsis for his help on expressing matrices in $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ in terms of $S, T$. Also, we would like to thank the magma algebra team for providing us with a free extension of the license to their system. Finally, we would like to thank the anonymous referee for his comments and suggestions.

## References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[2] Keith Conrad, *Galois Descent* Expository article on authors website http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/galoisdescent.pdf

[3] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR1215934 (94d:11078)

[4] Marc Hindry and Joseph H. Silverman, *Diophantine geometry, An introduction*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. MR1745599 (2001e:11058)

[5] Alice Gee, *Class invariants by Shimura's reciprocity law*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 45–72 (English, with English and French summaries). Les XXèmes Journées Arithmétiques (Limoges, 1997). MR1730432 (2000i:11171)

[6] Alice Gee, *Class Fields by Shimura Reciprocity*, Ph.D. thesis, Leiden University available online at http://www.math.leidenuniv.nl/nl/theses/44.

[7] Alice Gee and Peter Stevenhagen, *Generating class fields using Shimura reciprocity*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 441–453, DOI 10.1007/BFb0054883. MR1726092 (2000m:11112)

[8] S. P. Glasby and R. B. Howlett, *Writing representations over minimal fields*, Comm. Algebra **25** (1997), no. 6, 1703–1711, DOI 10.1080/00927879708825947. MR1446124 (98c:20019)

[9] William B. Hart, *Schläfli modular equations for generalized Weber functions*, Ramanujan J. **15** (2008), no. 3, 435–468, DOI 10.1007/s11139-007-9087-8. MR2390280 (2009d:11069)

[10] Gregor Kemper and Allan Steel, *Some algorithms in invariant theory of finite groups*, (Essen, 1997), Progr. Math., vol. 173, Birkhäuser, Basel, 1999, pp. 267–285. MR1714617 (2000j:13009)

[11] Elisavet Konstantinou, Aristides Kontogeorgis, Yannis C. Stamatiou, and Christos Zaroliagis, *Generating prime order elliptic curves: difficulties and efficiency considerations*, Information security and cryptology—ICISC 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, pp. 261–278, DOI 10.1007/11496618_20. MR2214104 (2007a:94194)

[12] Elisavet Konstantinou and Aristides Kontogeorgis, *Computing polynomials of the Ramanujan $t_n$ class invariants*, Canad. Math. Bull. **52** (2009), no. 4, 583–597, DOI 10.4153/CMB-2009-058-6. MR2567152 (2011a:11200)

[13] Elisavet Konstantinou and Aristides Kontogeorgis, *Ramanujan's class invariants and their use in elliptic curve cryptography*, Comput. Math. Appl. **59** (2010), no. 8, 2901–2917, DOI 10.1016/j.camwa.2010.02.008. MR2607997 (2010m:94101)

[14] Elisavet Konstantinou and Aristides Kontogeorgis, *Ramanujan invariants for discriminants congruent to* 5 (mod 24), Int. J. Number Theory **8** (2012), no. 1, 265–287, DOI 10.1142/S1793042112500157. MR2887894

[15] Claudio Procesi, *A primer of invariant theory*, Brandeis Lecture Notes, vol. 1, Brandeis University, Waltham, MA, 1982. Notes by Giandomenico Boffi. MR743262 (86d:14045)

[16] Srinivasa Ramanujan, *Notebooks. Vols. 1, 2*, Tata Institute of Fundamental Research, Bombay, 1957. MR0099904 (20 #6340)

[17] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1. MR1291394 (95e:11048)

[18] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[19] Peter Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 161–176. MR1846457 (2002i:11110)

[20] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction. MR1745599 (2001e:11058)

[21] Noriko Yui and Don Zagier, *On the singular values of Weber modular functions*, Math. Comp. **66** (1997), no. 220, 1645–1662, DOI 10.1090/S0025-5718-97-00854-5. MR1415803 (99i:11046)

[22] H. Weber, *Lehrbuch der Algebra*, Band III, 2nd edition, Chelsea reprint, original edition 1908.

University of Athens, Panepistimioupolis 15784, Athens, Greece
*E-mail address*: kontogar@math.uoa.gr