Certain CM class fields with smaller generators

Ömer Küçüksakallı*, Osmanbey Uzunkol†‡

July 24, 2013

Abstract

We introduce an algorithm that computes explicit class fields of an imaginary quadratic field K for a given modulus $\mathfrak{f} \subset \mathcal{O}_K$ more efficiently than the use of their classical counterparts. Therein, we prove the fact that certain values of a simple quotient of Siegel ϕ-function are elements in the ray class field $K_{\mathfrak{f}}$ of K.[1]

1 Introduction

Inspired by Kronecker-Weber theorem [Hil1896], Hilbert's 12th problem asks to generate the maximal abelian extension of a given number field explicitly using singular values of an analytical function. This problem can be regarded as finding a generalization of the exponential function appearing in Kronecker-Weber theorem. In the case of imaginary quadratic number fields K, Hilbert's 12. problem, also known as Kronecker's Jugendtraum, has an affirmative answer. The first proof of this fact was given by Hasse in 1927 in [Has27], and this was significantly simplified by Deuring in 1958 in [Deu58] using the theory of complex multiplication (CM-Theory) of elliptic curves and their j-invariants. More precisely, as a preliminary step one needs to construct the maximal unramified abelian extension (Hilbert class field H_K) of the imaginary quadratic number field K using a suitable value of j-function. All other (ramified) class fields of K are constructed by

*Middle East Technical University, Department of Mathematics, 06800, Ankara, Turkey (komer@metu.edu.tr).

†Carl von Ossietzky Universität Oldenburg, Institut für Mathematik, D-26111, Oldenburg, Germany (osmanbey.uzunkol@gmail.com).

‡Both authors are partially supported by a joint research project funded by BMBF (01DL12038) and Tübitak (TBAG-112T011).

[1] 2010 AMS MSC-class: 11G15, 11G16, 11F03.

adjoining suitable torsion values of Weber functions to the Hilbert class field H_K, see for instance [Sil94] for a rather modern treatment. The preliminary step is not necessary in the case of rational field $\mathbf{Q}$ due to the triviality of its class group.

Shimura's reciprocity law connects class field theory of imaginary quadratic number fields and arithmetic of modular functions by means of bringing Artin's reciprocity law and Galois theory of the field $\mathcal{F}$ of all arithmetical modular functions together, see [Sh71, Chapter 6]. It enables us to find an explicit action of absolute abelian Galois group of an imaginary quadratic field on the singular values $g(\tau)$, where $g \in \mathcal{F}$ and τ is an imaginary quadratic number lying in complex upper half plane $\mathfrak{h}$. However, computations are rather involved due to the presence of roots of unity in the functions.

CM-theory of elliptic curves plays also a vital role in construction of elliptic curves (CM-construction) with prescribed properties, such as known number of rational points, over finite fields. This CM-construction can be realized much better by using suitable generators of Hilbert class fields (or more generally ring class fields) having minimal polynomials with much smaller coefficients than coefficients of the minimal polynomials of the values of $j-$function used in the classical construction, see [Gee01, EngMor09, LePoUz09, Uz13] for more details. We refer to [AtMr93] and [Mor07] for applications of CM-construction in primality proving, or [BSS99], [BSS05] and [FST06] for applications in group and pairing based cryptography.

Let $m \not\equiv 2 \bmod 4$ be a natural number, and a be an integer such that $2 \leq a \leq m-1$. Let further $\mathbf{Q}_{(m)}$ be the corresponding ray class field over $\mathbf{Q}$. As is well known $\mathbf{Q}_{(m)}$ is the m-th real cyclotomic field $\mathbf{Q}(\zeta_m + \zeta_m^{-1})$ and can be obtained by adjoining the values of $\psi(z) = 1 - e^{2\pi i z}$ at rational numbers a/m to $\mathbf{Q}$. Moreover, real cyclotomic units are given by a nice expression, see [Wa97, p. 144]:

$$\zeta_m^{(1-a)/2} \frac{1-\zeta_m^a}{1-\zeta_m} = \pm \frac{\sin(\pi a/m)}{\sin(\pi/m)} \in \mathcal{O}_{\mathbf{Q}_{(m)}}^*.$$

There are analogues elliptic units in the in the case of imaginary quadratic number fields. Our aim in this paper is to introduce an algorithm to compute explicit class fields generated by these special units. Furthermore, we prove that these units yield 'smaller' generators for certain class fields than their classical counterparts. In the realm of Hilbert's 12. Problem, it is indeed the raison d'être of this paper to provide smaller primitive elements for class fields in the ray class field $K_{\mathfrak{f}}$ over K, without any restriction on the modulus $\mathfrak{f}$ of K, as special values of a single analytical function, namely certain values of a simple quotient of Siegel ϕ-function.

By using Kronecker's limit formula, Ramachandra introduced in 1964 primitive generators given as a product of values of various analytical functions, see [Ram64]. This ray class invariants are not suitable for explicit computations due to the presence of a very large product. A variant of Schertz's conjecture ([Sch97, p. 386]), recently proven in [JKS11, Remark 3.7, p. 424], states that

$$\phi(0, 1/N, \tau)^{12N/\gcd(6,N)} \tag{1.1}$$

generates $K_{(N)}$ over K if $K \neq \mathbf{Q}(\sqrt{-1}), \mathbf{Q}(\sqrt{-3})$ and $N \geq 2$. Under rather restrictive conditions, Bettner and Schertz showed in [BeSch01] that the expression

$$\zeta\Theta = \zeta \prod_{i=1}^{s} \phi(u_i, v_i, \tau_i)^{n_i}, \tag{1.2}$$

with specially chosen $u_i, v_i \in \mathbf{R}$, $\tau_i \in \mathfrak{h}$, $n_i \in \mathbf{Z}$ and a suitable root of unity ζ turns out to be an element of $K_{(N)}$ in some cases. They also conjectured that these elements are generators for $K_{(N)}$ over K if $\zeta\Theta \in K_{\mathfrak{f}}$.

One important advantage of ray class invariants introduced in this paper is that a factor of $r(N) := 12N/\gcd(6, N)$ can be gained by using a suitable simple quotient of Siegel ϕ-function heuristically in comparison to the generators in (1.1). We have also smaller elements of $K_{\mathfrak{f}}$ compared to the elements in the expression (1.2). Another main advantage is that we have no restriction on the ideal $\mathfrak{f}$ of $\mathcal{O}_K$ in comparison to both cases (1.1) and (1.2). In particular, we can pick a conductor $\mathfrak{f}$ that is not necessarily generated by a natural number N unlike the expression (1.1).

2 Shimura's Reciprocity Law

Let K be an imaginary quadratic number field of discriminant d_K, and $\mathcal{O}_K$ be its ring of integers. We formulate the results in this paper for the case of complex multiplication by the maximal order $\mathcal{O}_K$. For simplicity we denote the maximal order $\mathcal{O}_K$ by $\mathcal{O}$ for a fixed K.

In this section, we present an explicit version of Shimura's reciprocity law introduced by Gee and Stevenhagen, see [Gee01] and [Stev01], respectively. Unless otherwise stated or proved, the assertions of this section can be found in [Lang87], [Sta80] and [Sh71]. Moreover, we introduce the definition and transformation formulas of Siegel ϕ-function. For a detailed treatment, we refer to the Stark's paper [Sta80].

2.1 Class Field Theory

Let $\mathrm{Cl}(K)$ be the ideal class group of K and H be the Hilbert class field of K. We denote by $[\cdot, K]$ the Artin map on the group of finite $K-$idèles $\widehat{K^*} = \left(\prod_p' K \otimes_{\mathbf{Q}} \mathcal{O}_p\right)^* = (K \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}})^*$, i.e. idèles as quotient of the full idèle group obtained by forgetting the infinite component $\mathbf{C}^*$. In this case, we can summarize the main theorem of class field theory simply by the following exact sequence (see [Sh71, p. 115] for the general case and [Stev01, p. 165] for imaginary quadratic number fields):

$$1 \longrightarrow K^* \longrightarrow \widehat{K^*} \xrightarrow{[\cdot,K]} \mathrm{Gal}(K^{ab}/K) \longrightarrow 1, \tag{2.1}$$

where K^{ab} denotes the maximal abelian extension of K. The unit group

$$\widehat{\mathcal{O}^*} = \left(\lim_{\leftarrow N} (\mathcal{O}/N\mathcal{O})\right)^* = (\mathcal{O} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}})^* \subseteq \widehat{K^*}$$

of the profinite completion

$$\widehat{\mathcal{O}} = \lim_{\leftarrow N} (\mathcal{O}/N\mathcal{O}) = \mathcal{O} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$$

of the maximal order $\mathcal{O}$ inside $\widehat{K^*}$ is the preimage of the Artin map of $\mathrm{Gal}(K^{ab}/H)$ (see [Stev01, p. 165]). This implies that we obtain the following exact sequence by class field theory:

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \widehat{\mathcal{O}^*} \xrightarrow{[\cdot,K]} \mathrm{Gal}(K^{ab}/H) \longrightarrow 1. \tag{2.2}$$

2.2 Modular Functions

Let τ be an element in $\mathfrak{h} \cap K$ having minimal polynomial $Ax^2 + Bx + C$ such that $B^2 - 4AC = d_K$. The j-function is invariant under $\Gamma := \mathrm{SL}(2, \mathbf{Z})$, and the main theorem of complex multiplication implies that $j(\tau)$ generates the Hilbert class field H over K.

In order to generate other (ramified) abelian extensions of K, one can use modular functions. A modular function of level N is defined as a meromorphic function on $\mathfrak{h}$, which is invariant under the congruence subgroup $\Gamma(N) = \ker[\mathrm{SL}(2, \mathbf{Z}) \to \mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})]$ of Γ. A modular function of level N, whose q-expansions at every cusp have coefficients in $\mathbf{Q}(\zeta_N)$, is called arithmetical. The field of all arithmetical modular functions of level N is abbreviated by $\mathcal{F}_N$. In particular, $\mathcal{F}_1 = \mathbf{Q}(j)$. From now on we use the term modular function instead of arithmetical modular function for simplicity.

Remark 2.1. As a consequence of the main theorem of complex multiplication, we have the property that for every modular function $g \in \mathcal{F}_N$, the value $g(\tau)$, if finite, is contained in the ray class field $K_{(N)}$ of K with conductor (N), see for instance [Gee01, p. 41].

One can show that $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ with

$$\begin{aligned}\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) &\cong \mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})/\{\pm I_2\} \rtimes (\mathbb{Z}/N\mathbb{Z})^* \\ &\cong \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\pm I_2,\end{aligned}$$

where I_2 denotes the 2×2 identity matrix. The action of this Galois group on modular functions $\mathcal{F}_N$ can be described easily. If $A \in \Gamma$, then we have

$$f(z) \circ A = f(Az),$$

and if $A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]$ for $d \in \mathbf{Z}$ with $(d, N) = 1$, then

$$f(z) \circ A = \left(\sum_{n=n_0}^{\infty} \alpha_n q_N^n \right) \circ A = \sum_{n=n_0}^{\infty} \alpha_n^{\sigma} q_N^n,$$

where σ is the automorphism of $\mathbf{Q}(\zeta_N)/\mathbf{Q}$ given by $\zeta_N^{\sigma} = \zeta_N^d$.

In order to describe the idèlic interpretation of modular functions of all levels, Gee considers the following diagram of exact sequences [Gee01, p. 10]:

$$\begin{tikzcd}
1 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[d] & \mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z}) \arrow[r] \arrow[d] & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1(\zeta_N)) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[d] & \mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z}) \arrow[r] \arrow[d, "\det"] & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & 1 \arrow[r] & (\mathbf{Z}/N\mathbf{Z})^* \arrow[r] & \mathrm{Gal}(\mathcal{F}_1(\zeta_N)/\mathcal{F}_1) \arrow[r] & 1.
\end{tikzcd} \tag{2.3}$$

Let $\mathcal{F} = \cup_{N \geq 1} \mathcal{F}_N$ be the field of all modular functions. We can describe the Galois group of $\mathcal{F}$ over $\mathcal{F}_1$ simply by taking the projective limit of (2.3):

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}(2, \widehat{\mathbb{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1. \tag{2.4}$$

2.3 Reciprocity Law

We follow the explicit version of Shimura's reciprocity law due to Stevenhagen, see [Stev01]. Reciprocity law of Shimura connects the exact sequences (2.2) and (2.4) with the following reciprocity map h_τ:

$$\begin{tikzcd} 1 \arrow[r] & \mathcal{O}^* \arrow[r] & \prod_p' \mathcal{O}_p^* \arrow[r] \arrow[d, "h_\tau"] & \mathrm{Gal}(K^{ab}/H) \arrow[r] & 1 \\ 1 \arrow[r] & \{\pm 1\} \arrow[r] & \mathrm{GL}(2,\widehat{\mathbb{Z}}) \arrow[r] & \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \arrow[r] & 1, \end{tikzcd} \tag{2.5}$$

where $h_\tau : \prod_p' \mathcal{O}_p^* \to \mathrm{GL}(2,\widehat{\mathbb{Z}})$ sends the idèle $x \in \prod_p' \mathcal{O}_p^*$ to the transpose of the matrix representing the multiplication on $\widehat{\mathbb{Z}} \cdot \tau + \widehat{\mathbb{Z}}$ with respect to the basis $[\tau, 1]$ when viewed as a free $\widehat{\mathbb{Z}}-$module of rank 2. We have the following explicit formula for the reciprocity map in (2.5):

$$h_\tau : \ x = sA\tau + t \mapsto \left[\begin{smallmatrix} t-Bs & -Cs \\ sA & t \end{smallmatrix}\right]. \tag{2.6}$$

Using the reciprocity map, we obtain an action of $\widehat{\mathcal{O}^*}$ on the full arithmetic modular function field $\mathcal{F}$, [Stev01, p. 165], via

$$(g(\tau))^{[x^{-1},K]} = (g^{h_\tau(x)})(\tau).$$

Stevenhagen reduces the the reciprocity law of Shimura to the exact sequences of finite groups, [Stev01, p. 167]

$$\begin{tikzcd} 1 \arrow[r] & \mathcal{O}^* \arrow[r] & (\mathcal{O}/N\mathcal{O})^* \arrow[r] \arrow[d, "h_{\tau,N}"] & \mathrm{Gal}(K_{(N)}/H) \arrow[r] & 1 \\ 1 \arrow[r] & \{\pm 1\} \arrow[r] & \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{Gal}(\mathcal{F}_N/\mathbf{Q}(j)) \arrow[r] & 1. \end{tikzcd}$$

The image of $(\mathcal{O}/N\mathcal{O})^*$ under the reciprocity map $h_{\tau,N}$ is the following subgroup of $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$:

$$\mathcal{W}_{N,\tau} = \left\{ \left[\begin{smallmatrix} t-Bs & -Cs \\ sA & t \end{smallmatrix}\right] \in \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z}) : \ s,t \in \mathbb{Z}/N\mathbb{Z} \right\}. \tag{2.7}$$

Let $\mathrm{Cl}(d_K)$ be the form class group, i.e. the group consisting of reduced binary quadratic forms. It is a well known fact that the form class group $\mathrm{Cl}(d_K)$ and the ideal class groups $\mathrm{Cl}(K)$ are isomorphic, see [Cox89, p. 50]. This isomorphism is given by mapping a reduced binary quadratic form $Q = [a,b,c]$ to the ideal class containing the fractional ideal generated by $\tau_Q = (-b + \sqrt{dk})/2a$ and 1. Gee [Gee01, Chapter 1] proved the following theorem:

Theorem 2.2. *Let $Q = [a,b,c]$ be a reduced binary quadratic form of discriminant d_K and $\tau_Q = (-b+\sqrt{dk})/2a$. Set $u_Q = (u_p)_p \in \prod_p \mathrm{GL}(2,\mathbf{Z}_p)$ with*

- *For $d_K \equiv 0 \bmod 4$:*
$$u_p = \begin{cases} \left[\begin{smallmatrix} a & b/2 \\ 0 & 1 \end{smallmatrix}\right] & \text{if } p \not| a, \\ \left[\begin{smallmatrix} -b/2 & -c \\ 1 & 0 \end{smallmatrix}\right] & \text{if } p|a \text{ and } p \not| c, \\ \left[\begin{smallmatrix} -a-b/2 & -c-b/2 \\ 1 & -1 \end{smallmatrix}\right] & \text{if } p|a \text{ and } p|c, \end{cases}$$
- *For $d_K \equiv 1 \bmod 4$:*
$$u_p = \begin{cases} \left[\begin{smallmatrix} a & (b-1)/2 \\ 0 & 1 \end{smallmatrix}\right] & \text{if } p \not| a, \\ \left[\begin{smallmatrix} -(b+1)/2 & -c \\ 1 & 0 \end{smallmatrix}\right] & \text{if } p|a \text{ and } p \not| c, \\ \left[\begin{smallmatrix} -a-(b+1)/2 & -c-(1-b)/2 \\ 1 & -1 \end{smallmatrix}\right] & \text{if } p|a \text{ and } p|c. \end{cases}$$

Let $g \in \mathcal{F}$ be a modular function. Then it holds

$$g(\tau)^{[x_Q^{-1},K]} = g^{u_Q}(\tau_Q),$$

where g is defined and finite at τ, and $x_Q = (x_p)_p$ with

$$x_p = \begin{cases} a & \text{if } p \not| a, \\ a\tau_Q & \text{if } p|a \text{ and } p \not| c, \\ a(\tau_Q - 1) & \text{if } p|a \text{ and } p|c. \end{cases}$$

In [JKS11, p. 418–420] the following theorem is proven:

Theorem 2.3. *Assume that $K \neq \mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3})$ and $N > 0$. Then there exists a bijective map Ψ with*

$$\Psi : \mathcal{W}_{N,\tau}/\{\pm I_2\} \times \mathrm{Cl}(d_K) \longrightarrow \mathrm{Gal}(K_{(N)}/K)$$

where

$$(\alpha, Q) \longmapsto (g(\tau) \mapsto g^{\alpha \cdot u_Q}(\tau_Q))_{g \in \mathcal{F}_{N,\tau}},$$

and $\mathcal{F}_{N,\tau}$ is the set of modular functions of level N, which are defined and finite at τ.

2.4 Transformation formulas for Siegel phi-function

Stark obtains elements in the ray class fields $K_{\mathfrak{f}}$ by evaluating the modular function $\phi(u,v,z)$, Siegel ϕ-function, at imaginary quadratic numbers. Set

$\gamma = uz + v$, for $u, v \in \mathbf{R}$ and $z \in \mathfrak{h}$. Siegel ϕ-function is defined by the infinite product

$$\phi(u, v, z) = -ie^{\frac{\pi iz}{6}} e^{\pi iu\gamma} (e^{\pi i\gamma} - e^{-\pi i\gamma}) \prod_{n=1}^{\infty} (1 - e^{2\pi i(nz+\gamma)})(1 - e^{2\pi i(nz-\gamma)}).$$

Proposition 2.4. *The function $\phi(u, v, z)$ satisfies the following transformation properties:*

1. $\phi(u, v+1, z) = -e^{\pi iu} \phi(u, v, z)$
2. $\phi(u+1, v, z) = -e^{-\pi iv} \phi(u, v, z)$
3. $\phi(u, v, z+1) = e^{\pi i/6} \phi(u, u+v, z)$
4. $\phi(u, v, -1/z) = e^{-\pi i/2} \phi(v, -u, z)$

Proof. This is a consequence of Kronecker's second limit formula, see for example [Sta80, p. 207-208] for details. □

Let $N > 1$, s, t be integers with $(s, t, N) = 1$. Suppose that $u = s/N, v = t/N$ and $M = 12N^2$. Then Siegel ϕ-function $\phi(u, v, z)$ is a modular function of level M, see [Sta80, p. 208]. We now consider the action of some basic matrices in $\mathrm{GL}(2, \mathbf{Z}/M\mathbf{Z})$ on modular functions $\phi(u, v, z)$. We first start with $\mathrm{SL}(2, \mathbf{Z})$ which is generated by elements $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Define the multiplicative homomorphism $\omega : \mathrm{SL}_2(\mathbf{Z}) \to \langle \zeta_{12} \rangle$ which maps $T \mapsto e^{\pi i/6}$ and $S \mapsto e^{-\pi i/2}$. This map is compatible with Proposition 2.4, and it follows

$$\phi(u, v, z) \circ A = \phi(u, v, Az) = \omega(A) \phi((u, v)A, z)$$

for an integral matrix A with $\det(A) = 1$. In particular, $S^2 = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, and we have

$$\phi(u, v, z) = -\phi(-u, -v, z).$$

In general, we do not have to decompose A in terms of S and T to be able to compute the value of $\omega(A)$. Given $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma$, define

$$\begin{aligned} p_3(A) &= ac(b^2+1) + bd(a^2+1) \\ p_4(A) &= (b^2 - a + 2)c + (a^2 - b + 2)d + ad. \end{aligned}$$

Herglotz [Herg79] gives the following formula:

$$\omega(A) = \zeta_4^{p_4(A)} \zeta_3^{-p_3(A)}. \tag{2.8}$$

At the next step, we compute the action of $\left[\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right]$ on $\phi(u,v,z)$, where d is an integer relatively prime to M. The function $\phi(u,v,z)$ has coefficients in $\mathbf{Q}(\zeta_M)$, and the action of the automorphism $\sigma:\zeta_M\mapsto\zeta_M^d$ on $\phi(u,v,z)$ is obtained by multiplying v by d except $-i$ at the beginning. Note that $\sigma(-i)=-i(-1)^{(d-1)/2}$. Therefore

$$\phi(u,v,z)\circ\left[\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right]=\phi(u,vd,z)(-1)^{(d-1)/2}.$$

The action of $\left[\begin{smallmatrix}d&0\\0&1\end{smallmatrix}\right]=\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]\left[\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right]\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]$ in $\mathrm{GL}(2,\mathbf{Z}/M\mathbf{Z})$ can also be easily computed:

$$\begin{aligned}\phi(u,v,z)\circ\left[\begin{smallmatrix}d&0\\0&1\end{smallmatrix}\right]&=\phi(u,v,z)\circ\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]\\&=-i\phi(v,-u,z)\circ\left[\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right]\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]\\&=-i\phi(v,-ud,z)\circ\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]\\&=-\phi(-ud,-v,z)\\&=\phi(ud,v,z).\end{aligned}\tag{2.9}$$

3 Elliptic Units

Let K be an imaginary quadratic field and let $\mathfrak{f}\subset\mathcal{O}_K$ be a proper ideal. In this section we give an algorithm to compute a complete set of conjugates of a suitable simple quotient of values of Siegel ϕ-function over K. These special values turn out to be elliptic units in $K_{\mathfrak{f}}$. The inspiration comes from Stark's basic result for $\mathfrak{f}=\mathfrak{p}^s$ where $\mathfrak{p}$ is a degree one prime ideal coprime to $6d_K$ and $s\in\mathbf{Z}^{>0}$. [Sta80, p. 229].

Suppose f is the minimal positive integer divisible by the ideal $\mathfrak{f}\neq(1)$. For each ideal class $\mathfrak{c}$ in $\mathrm{Cl}_{\mathfrak{f}}=I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f})$, choose any ideal $\mathfrak{b}$ coprime to $\mathfrak{f}$ such that $\mathfrak{ab}$ is principal for all ideals $\mathfrak{a}$ in $\mathfrak{c}$. Furthermore, we assume that $\mathfrak{ab}=(\alpha)$ for some $\alpha\in\mathcal{O}$ and $\mathfrak{bf}=[\omega_1,\omega_2]$ where $\tau=\omega_1/\omega_2\in\mathfrak{h}$. We write $\alpha=[u,v]\left[\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right]$, where u,v are rational numbers such that fu and fv are integers. The elements

$$E(\mathfrak{c})=\phi(u,v,\tau)^{12f}\in K_{\mathfrak{f}}\tag{3.1}$$

depend only upon $\mathfrak{c}$ by [Sta80, Lemma 7]. The argument τ corresponds to a fractional ideal, and it can be transformed to τ_Q for some reduced binary quadratic form Q. Without loss of generality, we can always pick $\tau=\tau_Q$.

Let $\mathfrak{p}\subset\mathcal{O}_K$ be a degree one prime ideal in the ideal class $\mathfrak{c}$ of norm $|\mathfrak{p}|=p$ with $(p,12f)=1$. Stark shows that $E(\mathfrak{c})/E(1)^p$ is a $12f$-th power of a number in $K_{\mathfrak{f}}$. Moreover, if $K_{\mathfrak{f}}$ contains exactly W roots of unity, then

$W|12f$ and $E(\mathfrak{c})^W$ is a $12f$-th power of an algebraic integer in $K_{\mathfrak{f}}$ [Sta80, Lemma 9]. Let $\sigma_{\mathfrak{c}}$ be the element of $\mathrm{Gal}(K_{\mathfrak{f}}/K)$ corresponding the ideal class $\mathfrak{c}$ under the isomorphism $\mathrm{Gal}(K_{\mathfrak{f}}/K) \cong \mathrm{Cl}_{\mathfrak{f}}$. The action of $\sigma_{\mathfrak{c}}$ on the roots of unity is given by $\zeta_W^{\sigma_{\mathfrak{c}}} = \zeta_W^{d_{\mathfrak{c}}}$ where $d_{\mathfrak{c}} \equiv |p| \bmod W$. We define $e_{\mathfrak{c}} = W/(W, d_{\mathfrak{c}} - 1)$. Inspired by Stark, we find an element

$$\left(\frac{E(\mathfrak{c})}{E(1)}\right)^{e_{\mathfrak{c}}} \tag{3.2}$$

of norm 1 which is a $12f$-th power of an algebraic integer in $K_{\mathfrak{f}}$ by [Sta80, Theorem 1]. In particular, this process provides us examples of elliptic units.

We can choose an ideal class $\mathfrak{c}_0$ modulo $\mathfrak{f}$ such that its restriction to the Hilbert class field H contains the ideal $\mathfrak{f}$. For any choice of $\mathfrak{b}$, we have the property that $\mathfrak{b}\mathfrak{f}$ is principle if $\mathfrak{a}\mathfrak{b}$ is principle. It follows that we can choose $u_1, v_1 \in (1/f)\mathbf{Z}$ so that

$$E(\mathfrak{c}_0) = \phi(u_1, v_1, \tau_1)^{12f}. \tag{3.3}$$

If $\mathfrak{f} = (N)$, an ideal generated by a positive integer N, then we can choose $\mathfrak{b} = 1$ in the above setting and start with the pair $[u_1, v_1] = [0, 1/N]$ in the expression (3.3). Otherwise $[u_1, v_1]$ can be found by using a suitable ideal $\mathfrak{b}$ coprime to $\mathfrak{f}$.

By Stark's version of reciprocity law [Sta80, p. 223], we have

$$\sigma_{\mathfrak{c}}(E(\mathfrak{c}_0)) = E(\mathfrak{c}\mathfrak{c}_0) = \phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_{\mathfrak{c}})^{12f}$$

for some $u_{\mathfrak{c}}, v_{\mathfrak{c}} \in (1/f)\mathbf{Z}$ and $\tau_{\mathfrak{c}} = \tau_Q$ for some Q. In this case the restriction of $\mathfrak{c}$ to the Hilbert class field and the reduced binary quadratic form Q correspond to the same ideal class.

From now on we will focus on the case $\tau_{\mathfrak{c}} = \tau_1$ for simplicity. Moreover, we will assume $e_{\mathfrak{c}} = 1$, in order to construct minimal polynomials with coefficients as small as possible. We refer to Example 4.1 for a possible comparison of several cases. The conditions $\tau_{\mathfrak{c}} = \tau_1$ and $e_{\mathfrak{c}} = 1$ hold if and only if $\mathfrak{c}$ is a class of principal ideals such that $\sigma_{\mathfrak{c}}$ acts trivially on the roots of unity of $K_{\mathfrak{f}}$. Such a class $\mathfrak{c} \neq 1$ exists if and only if $K_{\mathfrak{f}} \neq H(\zeta_W)$ by class field theory.

Remark 3.1. If the equality $K_{\mathfrak{f}} = H(\zeta_W)$ holds, then one can easily generate the ray class field $K_{\mathfrak{f}}$ using class invariants of H together with cyclotomic elements. Hence, from this point of view the condition $K_{\mathfrak{f}} \neq H(\zeta_W)$ is not a restriction.

3.1 Explicit Conjugates

Let $\mathfrak{c}$ be an ideal class modulo $\mathfrak{f}$ such that $\tau_{\mathfrak{c}} = \tau_1$ and $e_{\mathfrak{c}} = 1$. We want to compute $[u_{\mathfrak{c}}, v_{\mathfrak{c}}]$ for a given $[u_1, v_1]$. Recall that $W|12f$. Set $\ell = 12f/W$. Since $E(1)^W$ is a $12f$-the power of an element in $K_{\mathfrak{f}}$, we find that

$$G(1) := \sqrt[\ell]{E(1)} = \phi(u_1, v_1, \tau_1)^W \cdot \zeta_\ell^* \in K_{\mathfrak{f}}$$

for some ℓ-th root of unity. Let $M = 12f^2$. We can find an element $\alpha \in \mathcal{W}_{M,\tau_1}$ whose restriction to $K_{\mathfrak{f}}$ corresponds to the automorphism $\sigma_{\mathfrak{c}}$, and acts trivially on the extension $K_{\mathfrak{f}}(\zeta_\ell)/K_{\mathfrak{f}}$. Let $\widehat{\alpha} = \alpha - 1$ be the element in the group ring $\mathbf{Z}[G]$, where $G = \mathcal{W}_{M,\tau_1}/\{\pm I_2\}$. Then, it follows that:

$$G(1)^{\widehat{\alpha}} = \left[\frac{\phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_{\mathfrak{c}})}{\phi(u_1, v_1, \tau_1)}\right]^W \in K_{\mathfrak{f}},$$

where $[u_{\mathfrak{c}}, v_{\mathfrak{c}}] = [u_1, v_1] \cdot \alpha$ and $\tau_{\mathfrak{c}} = \tau_1$ hold. Furthermore, the condition $e_{\mathfrak{c}} = 1$ implies that the above quotient is a W-th power of an element in $K_{\mathfrak{f}}$ due to the equation (3.2). Since $K_{\mathfrak{f}}$ contains W-th roots of unity, we can fix that

$$\epsilon(\mathfrak{c}) := \frac{\phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_1)}{\phi(u_1, v_1, \tau_1)} \in K_{\mathfrak{f}},$$

which is well defined up to a W-th root of unity.

Remark 3.2. At this point, we could also proceed with Stark's version of reciprocity law and obtain the same action, see for instance [Kuc11]. However idèlic interpretation introduced in the first section provides us with a better treatment of the subject.

Our purpose is now to compute $\epsilon(\mathfrak{c})^\sigma$ for all $\sigma \in \mathrm{Gal}(K_{\mathfrak{f}}/K)$. Find a pair $(\beta, Q) \in \mathcal{W}_{M,\tau_1} \times \mathrm{Cl}(d_K)$ such that whose restriction to $K_{\mathfrak{f}}$ corresponds to σ. By Chinese remainder theorem one can compute the matrix $u_Q \bmod M$, see [Gee01, p. 46]. By Theorem 2.2 and Theorem 2.3, the action of $\beta \cdot u_Q \in \mathrm{GL}(2, \mathbf{Z}/M\mathbf{Z})$ on Siegel ϕ-function is given explicitly. We have

$$\phi(u, v, \tau_1)^{(\beta,Q)} = \phi([u, v] \cdot \beta \cdot u_Q, \tau_Q) \cdot \zeta_Q$$

for some 12-th root of unity ζ_Q depending on Q but not on u, v and β. The assumption $\tau_{\mathfrak{c}} = \tau_1$ enables us to cancel ζ_Q, and simplifies computations considerably. As a result we have the following formula

$$\epsilon(\mathfrak{c})^\sigma = \frac{\phi([u_{\mathfrak{c}}, v_{\mathfrak{c}}] \cdot \beta \cdot u_Q, \tau_Q)}{\phi([u_1, v_1] \cdot \beta \cdot u_Q, \tau_Q)}. \tag{3.4}$$

In the case that the assumption $\tau_{\mathfrak{c}} = \tau_1$ does not hold, one can still perform similar computations. For a possible comparison, we refer to Example 4.1.

We obtain the following algorithm which can be obtained immediately by using the explicit action given in (3.4).

Algorithm I: Computation of conjugates for $\epsilon(\mathfrak{c})$

Input: The discriminant d_K and the modulus $\mathfrak{f}$ of K.
Output: A complete system of conjugates for $\epsilon(\mathfrak{c})$ over K.

1. Compute W and check if $K_{\mathfrak{f}} = H(\zeta_W)$.
   - If YES, print: `Use class invariants together with roots of unity` and return 0.
   - If NO, find a class $\mathfrak{c} \neq 1$ in $\mathrm{Cl}_{\mathfrak{f}}$ such that $e_{\mathfrak{c}} = 1$ and $\tau_{\mathfrak{c}} = \tau_1$. Go to the next step.
2. Compute $[u_1, v_1]$. Go to the next step.
3. Construct $\widehat{\alpha}$ and compute $[u_{\mathfrak{c}}, v_{\mathfrak{c}}]$. Go to the next step.
4. Compute the list $[Q_1, \ldots, Q_m]$ of all reduced binary quadratic forms in $\mathrm{Cl}(d_K)$ which is in one-to-one correspondence with $\mathrm{Gal}(H/K)$, and the list $[\beta_1, \ldots, \beta_n]$ of matrices from $\mathcal{W}_{M,\tau_1}/\{\pm I_2\}$ whose restriction to $K_{\mathfrak{f}}$ is in one-to-one correspondence with $\mathrm{Gal}(K_{\mathfrak{f}}/H)$. Go to the next step.
5. Compute the lists $[u_{Q_1}, \ldots, u_{Q_m}]$ and $[\tau_{Q_1}, \ldots, \tau_{Q_m}]$. Go to the next step.
6. for $1 \leq i \leq n$, for $1 \leq j \leq m$
   - Compute
   $$\epsilon(i,j) = \frac{\phi([u_{\mathfrak{c}}, v_{\mathfrak{c}}] \cdot \beta_i \cdot u_{Q_j}, \tau_{Q_j})}{\phi([u_1, v_1] \cdot \beta_i \cdot u_{Q_j}, \tau_{Q_j})}.$$
7. Return the matrix ϵ.

We implemented this algorithm in PARI/GP, see [PARI], for constructing class fields and comparing our results with the existing ones. We can summarize the construction above with the following theorem:

Theorem 3.3. *Let $\mathfrak{f}$ be an ideal of $\mathcal{O}$, and f be the smallest positive integer in $\mathfrak{f}$. Suppose that $K_{\mathfrak{f}} \neq H(\zeta_W)$, and let further $\mathfrak{c} \neq 1$ be an ideal class of principle ideals such that $\sigma_{\mathfrak{c}}$ acts trivially on ζ_W. Then there exists an algorithm which computes numbers $u_{\mathfrak{c}}, v_{\mathfrak{c}}, u_1, v_1 \in \frac{1}{f}\mathbf{Z}$ such that*

$$\epsilon(\mathfrak{c}) = \frac{\phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_1)}{\phi(u_1, v_1, \tau_1)} \in K_{\mathfrak{f}}.$$

Moreover, there exists another algorithm which computes the complete system of conjugates of $\epsilon(\mathfrak{c})$ over K.

In all our experiments, the value $\epsilon(\mathfrak{c})$ appears to be indeed a generator of $K_{\mathfrak{f}}$ over K. Moreover, the proof of [JKS11, Lemma 3.3] suggests also that our quotient is a generator of $K_{\mathfrak{f}}/K$. Hence, we have the following conjecture.

Conjecture 3.4. The elliptic unit $\epsilon(\mathfrak{c})$ generates $K_{\mathfrak{f}}$ over K if the conditions of Theorem 3.3 hold.

The following corollary follows immediately from Algorithm I.

Corollary 3.5. *Let the conditions of Theorem 3.3 hold, and Conjecture 3.4 be true. Then there exists an algorithm which computes the minimal polynomial $h(x) \in \mathcal{O}[x]$ of the generator $\epsilon(\mathfrak{c})$ of $K_{\mathfrak{f}}$ over K.*

Remark 3.6. Let $\mathfrak{c}$ be an ideal class modulo $\mathfrak{f} = (N)$, and let further $h_{\mathfrak{c}}(x)$ and $h_\phi(x)$ be the minimal polynomials of $\epsilon(\mathfrak{c})$ and $\phi(0, 1/N, \tau_1)^{12N/(6,N)}$ of [JKS11] over $\mathbf{Q}$, respectively. Furthermore, suppose that $\gamma_{\mathfrak{c}}$ and γ_ϕ be the logarithm of maximum of absolute values of the coefficients of $h_{\mathfrak{c}}(x)$ and $h_\phi(x)$, respectively.

We compare heuristically the values $\gamma_{\mathfrak{c}}$ and γ_ϕ. We expect that the reduction factor can be measured by the exponent

$$r(N) := \frac{\gamma_\phi}{\gamma_{\mathfrak{c}}} \approx \frac{12N}{\gcd(6, N)}$$

for arbitrarily large N.

This reduction factor gives significantly better results compared with the analogues results derived from the gonality estimates of modular curves and their relation to the celebrated Selberg's eigenvalue conjecture for class invariants, i.e. generators of ring class fields. In that case, the reduction factor is a constant bounded by 96 conjecturally and by 100.82 provably, see [BrSt08, p. 25], whereas our method yields a reduction factor depending linearly on N which turns out to be very efficient especially for the cases of large conductor and large discriminant.

4 Examples

Example 4.1. Let $K = \mathbf{Q}(\sqrt{-91})$ and $\mathfrak{f} = (5)$. The form class group of the discriminant $d_K = -91$ is given by

$$\mathrm{Cl}(d_K) = \{[1,1,23],[5,3,5]\}.$$

Moreover, we find that

$$\mathcal{W}_{5,\tau_1}/\{\pm I_2\} = \left\{ \begin{array}{l} \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & -23 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -23 \\ 1 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 & -23 \\ 1 & 3 \end{smallmatrix}\right], \\ \left[\begin{smallmatrix} -2 & -46 \\ 2 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -46 \\ 2 & 2 \end{smallmatrix}\right] \end{array} \right\}.$$

Giving these two sets is equivalent to enumerate all ideal classes in the ray class group by Theorem 2.3. We may choose $[u_1, v_1] = [0, 1/5]$. The function $\phi(a/5, b/5, z)$ is modular of level $M = 12 \cdot 5^2$ provided that $(5, a, b) = 1$. The number of roots of unity in the ray class field $K_{(5)}$ is given by $W = 10$. It follows that $\ell = 12 \cdot 5/10 = 6$.

Part 1: Let $\mathfrak{c}_1$ be the ideal class corresponding to the pair

$$(\left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right], [5,3,5]).$$

We find that $u_Q \equiv \left[\begin{smallmatrix} 293 & 169 \\ 276 & 49 \end{smallmatrix}\right] \bmod M$, where $Q = [5,3,5]$. The matrix $\alpha = \left[\begin{smallmatrix} 9 & -46 \\ 2 & 11 \end{smallmatrix}\right]$ is an element of $\mathcal{W}_{M,\tau_1}$ congruent to $\left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right]$ modulo 5, and the determinant of $\alpha \cdot u_Q$ is congruent to 1 modulo ℓ. We compute that $\det(\alpha \cdot u_Q) \equiv 3 \bmod W$, and as a result obtain $e_{\mathfrak{c}_1} = 5$. Now the calculation of $[0, 1/5] \cdot \alpha \cdot u_Q$ gives us

$$\epsilon(\mathfrak{c}_1) = \left[\frac{\phi\left(\frac{3622}{5}, \frac{877}{5}, \tau_Q\right) \cdot \zeta_Q}{\phi\left(0, \frac{1}{5}, \tau_1\right)} \right]^5 \in K_{(5)}.$$

Here ζ_Q is a 12-th root of unity depending only on the matrix u_Q. Its precise value can be found by the action of the matrix u_Q on Siegel ϕ-function $\phi(u, v, z)$. It requires computing a decomposition of u_Q in terms of S, T and $\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]$. This computation can be eliminated if we choose $\mathfrak{c}$ as in the following part.

Part 2: Now let $\mathfrak{c}_2$ be the ideal class corresponding to the pair

$$\left(\left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right], [1,1,23]\right).$$

We find that $u_Q \equiv \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \bmod M$. Observe that $\alpha = \left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right]$ has determinant congruent to 1 modulo ℓ. We find that $\det(\alpha \cdot u_Q) = 1$ and therefore $e_{\mathfrak{c}_2} = 1$. Now the calculation of $[0, 1/5] \cdot \alpha \cdot u_Q$ gives us

$$\epsilon(\mathfrak{c}_2) = \frac{\phi\left(\frac{2}{5}, \frac{1}{5}, \tau_1\right)}{\phi\left(0, \frac{1}{5}, \tau_1\right)} \in K_{(5)}.$$

Let $h_1(x)$ and $h_2(x)$ be the minimal polynomials of $\epsilon(\mathfrak{c}_1)$ and $\epsilon(\mathfrak{c}_2)$ over $\mathbf{Q}$, respectively. The absolute values of coefficients of $h_1(x)$ is much larger than the absolute values of coefficients of $h_2(x)$ due to the presence of the exponent 5. As a comparison we give the largest values c_1 and c_2 of the absolute value of the coefficients of polynomials $h_1(x)$ and $h_2(x)$, respectively:

$$c_1 = 1403930602698432087892972100920 2946,$$

$$c_2 = 910425.$$

As expected, we find that $\log(c_1)/\log(c_2) \approx 5.73015$.

Example 4.2. Let $\mathfrak{f}$ be a product of degree one prime ideals such that $(\mathfrak{f}, 6\bar{\mathfrak{f}}) = 1$. There exists an integer t_1 with $\tau_1 \equiv t_1 \bmod \bar{\mathfrak{f}}$ by Chinese remainder theorem. We have $\bar{\mathfrak{f}} = (f, \tau_1 + t_1)$. Consider the decomposition of the principal ideal $(\tau_1 + t_1) = \bar{\mathfrak{f}}\mathfrak{a}$ for some $\mathfrak{a} \in \mathfrak{c}_0$. Choosing $\mathfrak{b} = \bar{\mathfrak{f}}$, we find that $E(\mathfrak{c}_0) = \phi(1/f, t_1/f, \tau_1)^{12f} \in K_{\mathfrak{f}}$. Thus we can choose $[u_1, v_1] = [1/f, t_1/f]$.

In this case, we have $K_{\mathfrak{f}} \cap K_{\bar{\mathfrak{f}}} = H$, and it follows that all roots of unity in $K_{\mathfrak{f}}$ lie in H. Let $\mathfrak{c} \neq 1$ be any ideal class in $\mathrm{Cl}_{\mathfrak{f}}$ consisting of principal ideals. The action of $\sigma_{\mathfrak{c}}$ is trivial on the roots of unity of $K_{\mathfrak{f}}$, since $\zeta_W \in H$. Set $M = 12f^2$. For a given $\sigma \in \mathrm{Gal}(K_{\mathfrak{f}}/H)$, we can find a matrix $\alpha_a = \left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right] \in \mathcal{W}_{M,\tau_1}$ whose restriction to $K_{\mathfrak{f}}$ corresponds to σ. Recall that $\ell = 12f/W$. Without loss of generality we assume that $\det(\alpha_a) = a^2 \equiv 1 \pmod{\ell}$. Then any conjugate of $\epsilon(\mathfrak{c})$ can be found by using the formula

$$\epsilon(\mathfrak{c})^{(\beta,Q)} = \frac{\phi([\frac{1}{f}, \frac{t_1}{f}] \cdot \alpha_a \cdot \alpha_b \cdot u_Q, \tau_Q)}{\phi([\frac{1}{f}, \frac{t_1}{f}] \cdot \alpha_b \cdot u_Q, \tau_Q)} = \frac{\phi([\frac{ab}{f}, \frac{abt_1}{f}] \cdot u_Q, \tau_Q)}{\phi([\frac{b}{f}, \frac{bt_1}{f}] \cdot u_Q, \tau_Q)}$$

where (α_b, Q) is any pair with $b \in (\mathbf{Z}/M\mathbf{Z})^*$ and $Q \in \mathrm{Cl}(d_K)$.

Example 4.3. In this example we compare the result of Algorithm I with the example given in [JKS11, Example 3.8]. Let $K = \mathbf{Q}(\sqrt{-10})$ and let $\mathfrak{f} = (6)$. It turns out that $K_{\mathfrak{f}}$ has 24 roots of unity. We find that

$$\mathcal{W}_{6,\tau_1}/\{\pm I_2\} = \left\{ \begin{array}{l} \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & -10 \\ 1 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 3 & -10 \\ 1 & 3 \end{smallmatrix}\right], \left[\begin{smallmatrix} 5 & -10 \\ 1 & 5 \end{smallmatrix}\right], \\ \left[\begin{smallmatrix} 1 & -20 \\ 2 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 3 & -20 \\ 2 & 3 \end{smallmatrix}\right], \left[\begin{smallmatrix} 5 & -20 \\ 2 & 5 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & -30 \\ 3 & 1 \end{smallmatrix}\right] \end{array} \right\}.$$

Among the 8 principal ideal classes only those two corresponding to 1 and $2\sqrt{-10} + 3$ have matrices with determinant congruent to 1 modulo 24. We compute the value $\ell = 12 \cdot f/24 = 3$. Thus we shall use $\alpha = \left[\begin{smallmatrix} 3 & -20 \\ 2 & 3 \end{smallmatrix}\right] \in \mathcal{W}_{M,\tau_1}$, where $M = 12 \cdot 6^2$. The matrix α has determinant congruent to 1 modulo ℓ. It follows that

$$\epsilon(\mathfrak{c}) = \frac{\phi(\frac{2}{6}, \frac{3}{6}, \tau_1)}{\phi(0, \frac{1}{6}, \tau_1)}$$

is an element of $K_{(6)}$. Multiplying $\epsilon(\mathfrak{c})$ with $\zeta_{12}^5 \in K_{(6)}$, a real element with the minimal polynomial

$$\min(\epsilon(\mathfrak{c})\zeta_{12}^5, K) = \begin{array}{l} x^{16} + 8x^{15} - 18x^{14} - 68x^{13} + 50x^{12} \\ +108x^{11} - 44x^{10} - 28x^9 + 63x^8 \\ -28x^7 - 44x^6 + 108x^5 + 50x^4 - 68x^3 \\ -18x^2 + 8x + 1 \end{array}$$

can be found. This has much smaller coefficients than the following minimal polynomial computed in [JKS11]:

$$\min\left(\phi^{12}\left(0, \frac{1}{6}, \tau_1\right), K\right) = \begin{array}{l} x^{16} + 20560x^{15} - 1252488x^{14} - 829016560x^{13} \\ -8751987701092x^{12} + 217535583987600x^{11} \\ +181262520621110344x^{10} + 43806873084101200x^9 \\ -278616280004972730x^8 + 139245187265282800x^7 \\ -8883048242697656x^6 + 352945014869040x^5 \\ +23618989732508x^4 - 1848032773840x^3 \\ +49965941112x^2 - 425670800x + 1. \end{array}$$

Similar to the previous example, we compare the largest values c_1 and c_2 of the absolute values of the coefficients of polynomials $h_1(x)$ and $h_2(x)$, respectively:

$$c_1 = 278616280004972730,$$

$$c_2 = 108.$$

As expected, we find that $\log(c_1)/\log(c_2) \approx 8.57913$.

Example 4.4. Let $K = \mathbf{Q}(\sqrt{-11})$ and $\mathfrak{f} = (9)$. We compare in this example the result of Algorithm I with the example given in [BeSch01, Example 3]. Bettner and Schertz introduce an element $\Theta \in K_{\mathfrak{f}}$ with the following minimal polynomial:

$$\min(\Theta, K) = \begin{array}{l} x^{18} + 9x^{17} + 36x^{16} + (-8\tau_1 + 91)x^{15} \\ +(-78\tau_1 + 150)x^{14} + (-294\tau_1 + 45)x^{13} \\ +(-492\tau_1 - 479)x^{12} + (-120\tau_1 - 1020)x^{11} \\ +(816\tau_1 - 327)x^{10} + (1068\tau_1 + 1469)x^9 \\ +(-18\tau_1 + 1707)x^8 + (-882\tau_1 - 357)x^7 \\ +(-288\tau_1 - 1523)x^6 + (516\tau_1 - 345)x^5 \\ +(390\tau_1 + 540)x^4 + (2\tau_1 + 219)x^3 \\ +(-6\tau_1 - 15)x^2 + (6\tau_1 + 15)x + 1. \end{array}$$

On the other hand, we compute $\epsilon(\mathfrak{c}) = \phi(7/3, -2/9, \tau_1)/\phi(0, 1/9, \tau_1)$ with the minimal polynomial below:

$$\min(\epsilon(\mathfrak{c}), K) = \begin{array}{l} x^{18} + 3x^{17} + (-6\tau_1 + 3)x^{16} + (5\tau_1 - 4)x^{15} \\ +(-6\tau_1 + 18)x^{14} + (3\tau_1 - 3)x^{13} \\ +(-12\tau_1 + 40)x^{12} + (-6\tau_1 + 6)x^{11} \\ +(-15\tau_1 + 63)x^{10} - 2x^9 + (15\tau_1 + 78)x^8 \\ +(6\tau_1 + 12)x^7 + (12\tau_1 + 52)x^6 + (-3\tau_1 - 6)x^5 \\ +(6\tau_1 + 24)x^4 + (-5\tau_1 - 9)x^3 + (6\tau_1 + 9)x^2 \\ +3x + 1. \end{array}$$

Let c_Θ and $c_{\epsilon(\mathfrak{c})}$ be the absolute values of the coefficients with largest absolute value of $\min(\Theta, K)$ and $\min(\epsilon(\mathfrak{c}), K)$, respectively. We find that $\log(c_\Theta)/\log(c_{\epsilon(\mathfrak{c})}) \approx 1.76212$. Note that this is not the only advantage. For different modulus, it is possible to compute polynomials with smaller coefficients using Algorithm I than the polynomials in [BeSch01] heuristically. Furthermore, there is no restriction on the underlying modulus $\mathfrak{f}$ whereas the method in [BeSch01] is only applicable in very restrictive cases, and rather complicated with possibly higher powers when N gets larger.

5 Possible Applications

We list in this section possible further applications and generalizations of the construction in Algorithm I.

First of all, it could be interesting to investigate whether the set of elliptic units $\epsilon(\mathfrak{c})$ constructed by Algorithm I together with the units from Hilbert class field generate a subgroup of the unit group $U(\mathcal{O}_{K_\mathfrak{f}})$ of finite index.

Secondly we aim at investigating the result of Klebel, [Kle96], to find power integral basis of class fields over Hilbert class field by means of employing the elliptic units $\epsilon(\mathfrak{c})$ in a forthcoming research project. The existence of such a basis yields a solution of certain Diophantine equations, see [Gaa02].

In a forthcoming paper we plan to generalize Algorithm I to the case of complex multiplication by an arbitrary order $\mathcal{O}$, see [KucUz13].

Lastly it could be interesting to investigate the elements of Hilbert class field, or more generally ring class fields, coming from relative norms over H of elliptic units $\epsilon(\mathfrak{c})$ constructed by Algorithm I. This could possibly yield other source of class invariants. These invariants could be used in the applications of CM-theory such as primality proving, group and pairing based cryptography, see for instance [AtMr93], [Mor07], [BSS99], [BSS05] or [FST06].

References

[AtMr93] A. O. L. Atkin, F. Morain, *Elliptic Curves and Primality Proving*, Math. Comp. **61** (1993), 29–67

[BeSch01] S. Bettner, R. Schertz, *Lower Powers of Elliptic Units* Journal de Théorie des Nombres de Bordeaux **13** (2001), 339–351

[BrSt08] R. M. Bröker, P. Stevenhagen, *Constructing Elliptic Curves of Prime Order*, Computational Arithmetic Geometry, edited by K. E. Lauter and K. A. Ribet, Contemp. Math., **463** (2008), 17–28

[BSS99] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press (1999)

[BSS05] I. Blake, G. Seroussi, N. Smart, *Advances in Elliptic Curves in Cryptography*, Cambridge University Press (2005)

[Cox89] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class field Theory, and Complex Multiplication*, New York, Wiley (1989)

[Deu58] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzykl. d. math. Wiss., 2. Auflage, **10**, Stuttgart (1958)

[EngMor09] A. Enge, F. Morain *Generalized Weber Functions I*, preprint (2009), http://hal.inria.fr/inria-00385608/

[FST06] D. Freeman, M. Scott, E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*, Journal of Cryptology **23**, Issue 2 (2010), 224–280

[Gaa02] I. Gaal, *Diophantine Equations and Power Integral Bases*, Birkhäuser Mathematik (2002)

[Gee01] A. Gee, *Class Fields by Shimura Reciprocity*, Phd Thesis, Universiteit Leiden (2001)

[Has27] H. Hasse, *Neue Begründung der komplexen Multiplikation I and II*, J. reine angew. Math. **157** (1927), 115–139, **165** (1931), 64–88

[Herg79] G. Herglotz, *Über das quadratische Reziprozitätsgesetz in imaginären quadratischen Zahlkörpern*, Leipzig Ber. 73 (1921), 303–310; Gesammelte Schriften, §20, Vandenhoeck and Ruprecht, Göttingen (1979)

[Hil1896] D. Hilbert, *Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Körper*, Nach. K. Ges. Wiss. Göttingen (1896), 29–39 (Ges. Abh., 53–62)

[JKS11] H. J. Jung, J. K. Koo, D. H. Shin, *Ray Class Invariants over Imaginary Quadratic Fields*, Tohoku Math. J. **63** (2011), 413–426

[Kle96] M. Klebel *Zur Theorie der Potenzganzheitzbasen bei relativen galoischen Zahlkörpern*, Dissertation, Universität Augsburg (1996)

[Kuc11] Ö. Küçüksakalli, *Class Numbers of Ray Class Fields of Imaginary Quadratic Fields*, Math. Comp. **80**, no. 274 (2011), 1099–1122

[KucUz13] Ö. Küçüksakalli, O. Uzunkol , *Class Fields of Arbitrary Orders of Imaginary Quadratic Number Fields with smaller Generators*, in preparation (2013)

[Lang87] S. Lang, *Elliptic Functions; second edition*. Springer-Verlag, Graduate Texts in Math. **112**, (1987)

[LePoUz09] F. Leprévost, M. E. Pohst, O. Uzunkol *On the Computation of Class Polynomials with "Thetanullwerte" and its Applications to the Unit Group Computation*, Experimental Mathematics, 20(3) (2011), 271–281

[Mor07] F. Morain, *Implementing the Asymptotically fast Version of the Elliptic Curve Primality Proving Algorithm*, Math. Comp. **76** (2007), 493–505

[PARI] PARI/GP, version `2.3.2`, `http://pari.math.u-bordeaux.fr/`, Bordeaux (2006)

[Ram64] K. Ramachandra, *Some Applications of Kronecker's Limit Formula*, Ann. of Math. 2 **80** (1964), 104–148

[Sch97] R. Schertz, *Construction of Ray Class Fields by Elliptic Units* Journal de Théorie des Nombres de Bordeaux **9** (1997), 383–394

[Sh71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press (1971)

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer Verlag, Chapter II (1994)

[Sta80] H. M. Stark, *L-Functions at $s = 1$. IV. First Derivatives at $s = 0$*, Adv. in Math. **35**, no. 3 (1980), 197–235

[Stev01] P. Stevenhagen, *Hilbert's 12th Problem, Complex Multiplication and Shimura Reciprocity,* Advanced Studies in Pure. Math. 30, 'Class Field Theory - its centenary and prospect' (2001), 161–176

[Uz13] O. Uzunkol, *Generalized Class Invariants with 'Thetanullwerte'*, Turk. J. Math. **37** (2013), 165–181

[Wa97] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, second edition (1997)