On the computation of class polynomials with "Thetanullwerte" and its applications to the unit group computation

Franck Leprévost*, Michael Pohst†and Osmanbey Uzunkol‡

2009

Abstract

The classical class invariants of Weber are introduced as quotients of Thetanullwerte, enabling the computation of these invariants more efficiently than as quotients of values of the Dedekind η-function. We show also how to compute the unit group of suitable ring class fields by means of proving the fact that most of the invariants introduced by Weber are actually units in the corresponding ring class fields.

1 Introduction

Weber introduced the so-called Schläfli functions $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$ together with γ_2 and γ_3 in his 'Lehrbuch der Algebra' [Wb] as quotients of values of the Dedekind $\eta-$function in order to generate the ring class field of an imaginary quadratic field K with 'simpler' generators than by j-invariants for a given order $\mathcal{O}_t$ of conductor $t \in \mathbb{Z}^{>0}$.

Another area in which the use of the Schläfli functions turns out to be more efficient than the use of the j-invariant is to construct special elliptic curves with a known number of rational points with the theory of complex multiplication, instead of taking a random elliptic curve over a finite field and computing the cardinality of rational points (see [AtMr] and [Mor] for applications in primality proving, or [BSS1], [BSS2] and [FST] for applications in group and pairing based cryptography). The interest comes from the fact that the minimal polynomials of the singular values of the class invariants, which are derived from the Schläfli functions, have smaller heights than the corresponding minimal polynomials of

*University of Luxembourg, 162 A, avenue de la Faïencerie, L-1511 Luxembourg (franck.leprevost@uni.lu)

†TU-Berlin, Sekretariat MA 8-1, Straße des 17. Juni 136, D-10623 Berlin, Germany (pohst@mail.math.tu-berlin.de)

‡Carl von Ossietzky Universität Oldenburg, Institut für Mathematik, D-26111, Oldenburg, Germany (osmanbey.uzunkol@uni-oldenburg.de)

the singular values of the j-invariant.

In section 2, we summarize some results from the theory of modular functions and the theory of theta functions which are to be used in the following sections. Also, modified Schläfli functions will be introduced as quotients of values of Jacobi theta functions, the so-called Thetanullwerte, and their relation to the classical Schläfli functions will be proved using a result of Weber ([Wb], p. 112 and 114).

In section 3 we use the relationship between classical and modified Schläfli functions in order to express the class invariants as quotients of Thetanullwerte. Moreover, a complexity analysis of computing the Thetanullwerte and η values, due to [Dup], is given to show the efficiency of our method.

Using a theorem of Deuring, we prove the fact that most of these class invariants are units in the corresponding ring class fields in section 4. In case they are not units, we show that the absolute values of the norms of these invariants are powers 2^l with the property that the exponent l divides the class number h_t. Furthermore, we prove that we obtain better class invariants in the cases $m \equiv 3 \mod 24$ and $m = 16 \cdot k + 12$ for $k \equiv 3 \mod 6$.

Using these class units, we will show in section 5 how to compute the unit groups of the corresponding ring class fields.

Lastly, the comparison of the computation of class polynomials using values of $\eta-$function and Thetanullwerte and examples of the new class invariants are given in section 6 as well as an application to the computation of the unit group of a ring class field.

We thank the referee for the careful reading of the manuscript which led to considerable improvements in the quality of the paper.

2 Preliminaries

We write as usual the discriminant function for $\tau \in \mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ and the $j-$invariant at τ using Eisenstein series as follows (see for example [Deu], p. 3):

$$\Delta(\tau) := g_2(\tau)^3 - 27g_3(\tau)^2,\ j(\tau) := 2^6 3^3 g_2(\tau)^3 \Delta(\tau)^{-1}, \tag{1}$$

and define the Dedekind η-function by

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{k=1}^{\infty}(1-q^k) \text{ with } q = \exp(2\pi i\tau). \tag{2}$$

The theory of elliptic functions leads to the following identity (see [Deu], p. 3)

$$\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}. \tag{3}$$

The Schläfli functions of Weber can now be defined as quotients of values of the Dedekind $\eta-$function:

$$\mathfrak{f}(\tau) = \exp(-\frac{\pi i}{24})\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)},\ \mathfrak{f}_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)},\ \mathfrak{f}_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}. \tag{4}$$

These functions satisfy the following equations ([Wb], p. 114):

Theorem 1. *We have for all $\tau \in \mathbb{H}$ the following identities:*

1. $\mathfrak{f}(\tau)^8 = \mathfrak{f}_1(\tau)^8 + \mathfrak{f}_2(\tau)^8$,
2. $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$.

Lastly the functions γ_2 and γ_3 are defined as follows:

$$\gamma_2(\tau) = \sqrt[3]{j(\tau)},\ \gamma_3(\tau) = \sqrt{j(\tau) - 12^3}.$$

By [Sch], p. 327, we have the following identities:

Lemma 2.

$$\gamma_2 = \frac{\mathfrak{f}^{24} - 16}{\mathfrak{f}^8} = \frac{\mathfrak{f}_1^{24} + 16}{\mathfrak{f}_1^8} = \frac{\mathfrak{f}_2^{24} + 16}{\mathfrak{f}_2^8}.$$

Definition 3. *Let $\mathbb{H}_g$ denote the Siegel upper half plane in dimension g and $\Omega \in \mathbb{H}_g$, i. e. $\Omega = \Omega_1 + i\Omega_2$ with real $g \times g$ matrices Ω_1, Ω_2, whereby Ω_2 is positive definite. The **Riemann theta function** is defined by*

$$\theta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} exp(\pi i(n^t \Omega n + 2n^t z))$$

*for a column vector $z \in \mathbb{C}^g$. The **theta characteristics** for $\delta, \epsilon \in (\mathbb{Z}/2\mathbb{Z})^g$ are given by (see [Weng], p. 11)*

$$\theta\left[\delta, \epsilon\right](z, \Omega) = \sum_{n \in \mathbb{Z}^g} exp\left(\pi i\left[(n + \frac{1}{2}\delta)^t \Omega (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (z + \frac{1}{2}\epsilon)\right]\right),$$

from which it follows

$$\theta\left[\delta, \epsilon\right](-z, \Omega) = (-1)^{\delta^t \epsilon}\theta\left[\delta, \epsilon\right](z, \Omega).$$

*If we set $z = 0$, then we obtain the so-called **Thetanullwerte** (see [Weng], p. 11).*

Remark 4. *We have*

1. *The Thetanullwerte for* $\delta^t\epsilon \equiv 1 \mod 2$ *are identically zero. These are called* ***odd*** *Thetanullwerte. If we have* $\delta^t\epsilon \equiv 0 \mod 2$*, then we obtain* ***even*** *Thetanullwerte.*

2. *Hence there are* $2^{g-1}(2^g+1)$ *(resp.* $2^{g-1}(2^g-1)$*) even (respectively odd) Thetanullwerte in* $\mathbb{H}_g$*.*

Definition 5. *For* $g=1$*,* $\tau \in \mathbb{H}$ *and* $q = exp(2\pi i\tau)$*, the Thetanullwerte coincide with the classical* ***Jacobi theta functions****:*

- $\theta_{00}(\tau) := \theta[0,0](0,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2/2}$,
- $\theta_{10}(\tau) := \theta[1,0](0,\tau) = \sum_{n\in\mathbb{Z}} q^{(n+\frac{1}{2})^2/2}$,
- $\theta_{01}(\tau) := \theta[0,1](0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2/2}$,
- $\theta_{11}(\tau) := \theta[1,1](0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^{n-\frac{1}{2}} q^{(n+\frac{1}{2})^2/2}$.

It is easy to see from remark 4 that the Jacobi theta functions $\theta_{00}, \theta_{10}, \theta_{01}$ are even and θ_{11} is odd. We note that the derivative θ'_{11} of θ_{11} is also an even function.

We now give the relationship between Schläfli functions and Jacobi theta functions according to the following theorem ([Wb], p. 112 and 114):

Theorem 6. *For* $\tau \in \mathbb{H}$*, we have*

$$\theta'_{11}(\tau) = 2\pi\eta(\tau)^3,\ \theta_{00}(\tau) = \eta(\tau)\mathfrak{f}(\tau)^2,\ \theta_{01}(\tau) = \eta(\tau)\mathfrak{f}_1(\tau)^2,\ \theta_{10}(\tau) = \eta(\tau)\mathfrak{f}_2(\tau)^2.$$

Definition 7. *For* $\tau \in \mathbb{H}$*, we introduce the following modified Schläfli functions:*

$$\mathfrak{F}(\tau) := \frac{2\theta_{00}(\tau)^2}{\theta_{01}(\tau)\theta_{10}(\tau)},\ \mathfrak{F}_1(\tau) := \frac{2\theta_{01}(\tau)^2}{\theta_{00}(\tau)\theta_{10}(\tau)},\ \mathfrak{F}_2(\tau) := \frac{2\theta_{10}(\tau)^2}{\theta_{00}(\tau)\theta_{01}(\tau)}.$$

By theorems 1 and 6, one can easily see the following relation:

$$\eta(\tau)^3 = \frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2}.$$

Using this identity and the third powers of the identities in theorem 6, we deduce the following relations between classical and modified Schläfli functions:

Theorem 8. *For* $\tau \in \mathbb{H}$*:*

- $\mathfrak{F}(\tau) = \mathfrak{f}(\tau)^6$,
- $\mathfrak{F}_1(\tau) = \mathfrak{f}_1(\tau)^6$,
- $\mathfrak{F}_2(\tau) = \mathfrak{f}_2(\tau)^6$.

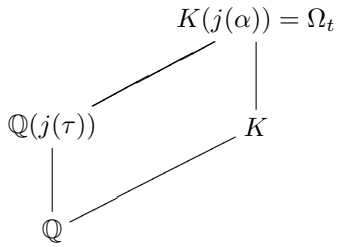
3 Class Polynomials

3.1 Class invariants and N-systems

We refer to [Lang] for the basic properties of imaginary quadratic number fields, their orders, class field theory, modular functions and the theory of complex multiplication.

Let K be an imaginary quadratic number field with the discriminant d, $\mathcal{O}_t$ denote the order of K of conductor $t \in \mathbb{Z}^{>0}$ and Cl_t be the ring class group of $\mathcal{O}_t$ with the class number h_t. We know from the theory of complex multiplication of imaginary quadratic number fields that for any number $\tau \in \mathbb{H}$ with the discriminant $t^2 d$ the value $j(\tau)$ generates the ring class field Ω_t of K, i. e. the field extension belonging to the subgroup $\mathcal{U}_t$ of the ideal group of K generated by ideals of the form (λ), $\lambda \in \mathbb{Z}$ with $\gcd(\lambda, t) = 1$ and $\lambda \equiv r \bmod t$ for a suitable $r \in \mathbb{Z}$, see [Sch], p. 327.

The values $j(\tau_i)$, $i = 1, \cdots, h_t$, from the representatives of ideals $[\tau_i, 1]$ in Cl_t with $\tau := \tau_1$ form a complete system of conjugate numbers over K. Furthermore, it is even a complete system of conjugates over $\mathbb{Q}$ ([Lang], p. 133, remark 1). As the $j(\tau)$ for all $\tau \in \mathbb{H}$ are algebraic integers, the minimal polynomial of $j(\tau)$ has coefficients in $\mathbb{Z}$. We have the property that $\mathbb{Q}(j(\tau))$ is the conjugate field to the maximal real subfield of Ω_t (see [Sch1], p. 51).



Let g be one of the Schläfli functions $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$ or γ_2, γ_3. Then according to lemma 2, we have

$$\mathbb{Q}(j(\tau)) \subseteq \mathbb{Q}(g(\tau)).$$

If also the other inclusion holds, for example for a small power of one of the values of Schläfli functions, we get an alternative primitive element for the field Ω_t:

Definition 9. *A value $g(\tau)$ of a modular function g is said to be a **class invariant** if $\mathbb{Q}(g(\tau)) = \mathbb{Q}(j(\tau))$.*

In order to be able to generate the field $\mathbb{Q}(j(\tau))$ with some class invariant, we need to describe the conjugates of the invariant, which is possible according to the following definition ([Sch], p. 329) and the theorem:

Definition 10. *1. An imaginary quadratic integer $\tau \in \mathbb{H} \cap K$ is the zero of a quadratic equation of the form $Ax^2 + Bx + C = 0$, which is uniquely determined by τ if we postulate the following normalisation assumption:*

$$A, B, C \in \mathbb{Z},\ \gcd(A, B, C) = 1,\ A > 0.$$

Such an equation is called ***primitive****.*

2. Let $N \in \mathbb{Z}^{>0}$ and $\tau_1, \tau_2, \cdots, \tau_{h_t} \in \mathbb{H}$, so that

$$[\tau_1, 1], [\tau_2, 1], \cdots, [\tau_{h_t}, 1]$$

is a system of representatives of Cl_t. Let further $A_i x^2 + B_i x + C_i = 0$ be primitive equations for τ_i which satisfy the properties

$$\gcd(A_i, N) = 1 \text{ and } B_i \equiv B_j \bmod 2N, 1 \leq i, j \leq h_t.$$

*Then the elements $\tau_1, \tau_2, \cdots, \tau_{h_t}$ are called an N-**system modulo** t.*

Remark 11. *According to [Sch], p. 335, we know that there exists an N-system for every natural number in $\mathbb{Z}^{>0}$.*

We have the following theorem, which allows us to compute the class invariants as quotients of Thetanullwerte instead of computing them traditionally as values of quotients of the Dedekind $\eta-$function.

Theorem 12. *Let $\tau \in \mathbb{H}$ be a zero of a primitive equation*

$$Ax^2 + Bx + C = 0 \text{ with } \gcd(A, 2) = 1,\ B \equiv 0 \text{ mod } 32$$

with the special discriminant $D(\tau) = t^2 d =: -4m$, i. e. $D(\tau)$ is divisible by 4 with cofactor $-m$. Then the following numbers $g(\tau)$ are class invariants:

- $\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{F}(\tau) = \left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} \mathfrak{f}(\tau)^2\right)^3$ *if* $m \equiv 1 \mod 8$,
- $exp(-\frac{\pi i}{8}) \frac{\theta'_{11}(\frac{\tau+1}{2})}{\theta'_{11}(\tau)} = \mathfrak{f}(\tau)^3$ *if* $m \equiv 3 \mod 8$,
- $\frac{\mathfrak{F}(\tau)^2}{8} = \left(\frac{1}{2}\mathfrak{f}(\tau)^4\right)^3$ *if* $m \equiv 5 \mod 8$,
- $\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} exp(-\frac{\pi i}{8}) \frac{\theta'_{11}(\frac{\tau+1}{2})}{\theta'_{11}(\tau)} = \left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} \mathfrak{f}(\tau)\right)^3$ *if* $m \equiv 7 \mod 8$,
- $\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{F}_1(\tau) = \left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} \mathfrak{f}_1(\tau)^2\right)^3$ *if* $m \equiv 2 \mod 4$,
- $\left(\frac{2}{A}\right) \frac{\mathfrak{F}_1(\tau)^2}{16\sqrt{2}} = \left(\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{f}_1(\tau)^4\right)^3$ *if* $m \equiv 4 \mod 8$,

where the factor $\left(\frac{2}{A}\right)$ *denotes the Legendre symbol.*

If $\tau = \tau_1, \cdots, \tau_{h_t}$ *is a* 16*-system modulo* t*, then the singular values* $g(\tau_i)$ *above form a complete system of conjugates over* $\mathbb{Q}$*. Therefore, the minimal polynomial over* $\mathbb{Q}$ *is*

$$W_{D(\tau)}(x) = \prod_{i=1}^{h_t}(x - g_i), \text{ where } g_i := g(\tau_i),$$

and this polynomial has integer coefficients. $W_{D(\tau)}(x)$ *is called the class polynomial of* $g(\tau)$*.*

Proof: The identities between the quotients of values of the Dedekind $\eta-$function and the quotients of the Thetanullwerte follow from theorem 8 and theorem 6. The result for quotients of the values of the Dedekind $\eta-$function is a theorem of Schertz, see [Sch], p. 337. □

Remark 13. *The values in the theorem 12 are the elements of* Ω_t *also without the factor* $\left(\frac{2}{A}\right)$*. This factor is required only for writing down the conjugates for* $g(\tau)$*, see [Sch] for the details.*

For discriminants not divisible by 3*, the functions in theorem 12 without outer exponent* 3 *are also class invariants ([Sch], p. 330, theorem 2). This follows from the relation between* $\mathfrak{f}$ *and* γ_2 *in lemma 2.*

3.2 Optimality: The choice of the class invariant

The natural questions which invariants should be used in practise and how good we can construct class invariants using alternative modular functions will be discussed in this section.

Let g be a modular function, whose value $g(\tau)$ is a class invariant. The logarithmic height of the minimal polynomial of $g(\tau)$ differs from the logarithmic height of $j(\tau)$ by a constant factor according to the following theorem of Hindry and Silverman, see [HinSil], proposition B.3.5:

Theorem 14. *Let* $r(g)$ *be the quotient*

$$r(g) = \frac{\deg_g(\Phi(g,j))}{\deg_j(\Phi(g,j))},$$

where $\Phi(g,j) = 0$ *is the modular polynomial and* $\deg_x(\Phi(x,y)$ *the degree in* x *of this polynomial.*

Then, we have

$$r(g) = \lim_{\mathcal{H}(j(\tau))\to\infty} \frac{\mathcal{H}(g(\tau))}{\mathcal{H}(j(\tau))},$$

where the limit is taken over all CM-points $\tau \in \mathbb{H}$*, which are ordered by the discriminant of the corresponding orders, and* $\mathcal{H}$ *is the absolute logarithmic heigt.*

Bröker und Stevenhagen proved the following theorem using theorem 14, see [BrSt]:

Theorem 15. *We have the following upper bound*

$$r(g) \leq 32768/325 \approx 100.82.$$

Assume the Selberg's eigenvalue conjecture holds (see [Sar]) then we have

$$r(g) \leq 96.$$

Using the definition of $r(g)$ together with theorem 12, lemma 2 and remark 13, we obtain the following theorem. It states which constant factor can be gained by using the class invariants of theorem 12.

Theorem 16. *Let the assumptions be as in theorem 12. Then we have:*

$$r(g) = \begin{cases} 6 & \text{if } m \equiv 12, 21 \bmod 24, \\ 12 & \text{if } m \equiv 6, 9, 18 \bmod 24, \\ 18 & \text{if } m \equiv 4, 5, 13, 20 \bmod 24, \\ 24 & \text{if } m \equiv 3, 15 \bmod 24, \\ 36 & \text{if } m \equiv 1, 2, 10, 14, 17, 22 \bmod 24, \\ 72 & \text{if } m \equiv 7, 11, 19, 23 \bmod 24. \end{cases}$$

By theorems 16 and 13, we obtain $r(g) = 72$ for class invariants $g(\tau) = \mathfrak{f}(\tau)$ and $g(\tau) = \frac{1}{\sqrt{2}}\mathfrak{f}(\tau)$ in the cases $m \equiv 3 \bmod 8$ and $m \equiv 7 \bmod 8$, respectively, if the discriminant is not divisible by 3. Hence, these are almost optimal class invariants.

It is an open question whether there is a modular function g with $r(g) = 96$, whose suitable values are class invariants.

3.3 Analysis: θ versus η

An asymptotically fast algorithm for the numerical computation of the n significant bits of one of the Thetanullwerte evaluated at $\tau \in \mathbb{H}$ is given by [Dup]. He uses the connection between arithmetic geometric means (AGM) of complex numbers and Thetanullwerte. He proved that the computation can be done in $\mathcal{O}(M(n) \log n)$ bit operations, where $M(n)$ denotes the time complexity of multiplying two n bit integers. We explain now, how one can compute the n significant bits of a value of the Dedekind $\eta-$function using his algorithm.

Definition 17. *We define κ und κ' For $\tau \in \mathbb{H}$ as follows:*

- $\kappa(\tau) = \left(\frac{\theta_{10}(\tau)}{\theta_{00}(\tau)}\right)^2$,
- $\kappa'(\tau) = \left(\frac{\theta_{01}(\tau)}{\theta_{00}(\tau)}\right)^2$.

Theorem 18. *Using the identity*

$$\eta(\tau)^{12} = \frac{\kappa'(\tau)^2(1-\kappa'(\tau)^2)\theta_{00}(\tau)^{12}}{16}$$

one can compute $\eta(\tau)^{12}$ *in* $O(\mathcal{M}(n)\log n)$ *bit operations.*

Proof: By [Dup], p. 19, we have

$$\mathfrak{f}(\tau)^{24}\kappa'(\tau)^2(1-\kappa'(\tau)^2) = 16.$$

Now, by the theorem 6 we have $\mathfrak{f}(\tau)^{24}\eta(\tau)^{12} = \theta_{00}(\tau)^{12}$. This implies

$$\eta(\tau)^{12} = \frac{\kappa'(\tau)^2(1-\kappa'(\tau)^2)\theta_{00}(\tau)^{12}}{16}.$$

As one can compute the n significant bits of one of the Thetanullwerte evaluated at $\tau \in \mathbb{H}$ in $\mathcal{O}(M(n)\log n)$, we can compute $\eta(\tau)^{12}$ also in $\mathcal{O}(M(n)\log n)$.□

Note that the same arguments for computing $\eta(\tau)^{12}$ are given in [Dup], p. 18 and 19. However, the power of $\theta_{00}(\tau)$ is not stated correctly, see [Dup], p. 19, line 6.

Therefore, we need to extract the 12th root of η^{12} in order to evaluate n significant bits of the η-function evaluated at τ, which can be done by means of Newton iteration. This computation has the complexity $\mathcal{O}(M(n))$. Hence, if we compute the class invariants as quotients of Thetanullwerte, we save the time needed to take a 12th root using Newton iteration. Note that by taking a 12th root no precision is lost in general, see [Dup], p. 4. This means that the precision we need is in both cases the same. We save just $\mathcal{O}(M(n))-$bit operations using the Thetanullwerte by avoiding the Newton iteration.

Note also that, in order to compute a value $\eta(\tau)$ using theorem 18, we need to compute both $\theta_{00}(\tau)$ and $\theta_{01}(\tau)$. Hence, we need approximately twice as many coefficients in the computation of $\eta(\tau)$ as that of $\theta_{00}(\tau)$ or $\theta_{01}(\tau)$.

We refer to the last section for the comparison of computing class polynomials using η and θ representations.

Another reason to use the quotients of Thetanullwerte instead of the values of quotients of Dedekind $\eta-$function is that Thetanullwerte are functions which can be generalized to any genus. Since there is no analogue of the notion of smaller class invariants for genus > 1, the representation of class invariants as quotients of Thetanullwerte can be used to generalize the notion of class invariants at least to genus two, see [Uz], p. 117.

4 Class Units

In this section, we prove that most of the invariants introduced by the above theorems are actually units in the corresponding ring class fields. This enables us to compute the unit group of ring class fields by using these explicit units, which will be discussed in the next section. We begin with a theorem of Deuring

([Deu], p. 43). (Note that, although some of the results given in this section are stated in [Birch], proofs are not given.)

Let P be a primitive matrix of determinant p, where p is a prime number, i. e.

$P = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ with $\det(P) = p$ and $\gcd(a,b,c,d) = 1$.

For the quotient (see [Deu], p. 11)

$$\varphi_P(\tau) := p^{12}\frac{\Delta\left(P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right)}{\Delta\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}}, \text{ where } \Delta\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \omega_2^{-12}\Delta(\tau) \tag{5}$$

we have the following theorem of Deuring, see [Deu], p. 43

Theorem 19. *Let $t > 0$ be an integer, p be a prime number and $l \geq 0$ be the greatest power of p with $p^l | t$. Let further a, b, c and d be integers such that the matrix $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant p. Assume that $\{\omega_1, \omega_2\}$ is a basis of a fractional $\mathcal{O}_t$-ideal I with $\tau := \frac{\omega_1}{\omega_2} \in \mathbb{H}$.*

1. *If p splits completely in K, i. e. $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, then*
   (a) *$\varphi_P(\tau)$ is a unit if $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis of a fractional $\mathcal{O}_{tp}$-ideal,*
   (b) *$\frac{\varphi_P(\tau)}{p^{12}}$ is a unit if $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis of a fractional $\mathcal{O}_{tp^{-1}}$-ideal,*
   (c) *In the case $l = 0$, $\frac{\varphi_P(\tau)}{\overline{\mathfrak{p}}^{12}}$ and $\frac{\varphi_P(\tau)}{\mathfrak{p}^{12}}$ are units if $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis of ideals $I_{\mathcal{O}_t}\mathfrak{p}_{\mathcal{O}_t}$ and $I_{\mathcal{O}_t}\overline{\mathfrak{p}}_{\mathcal{O}_t}$, respectively.*
2. *If p ramifies in K, i. e. $(p) = \mathfrak{p}^2$, then*
   (a) *$\frac{\varphi_P(\tau)}{p^{\frac{6}{p^{l+1}}}}$ is a unit if $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis of a fractional $\mathcal{O}_{tp}$-ideal,*
   (b) *$\frac{\varphi_P(\alpha)}{p^{12-\frac{6}{p^l}}}$ is a unit if $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis of a fractional $\mathcal{O}_{tp^{-1}}$-ideal,*
   (c) *$\frac{\varphi_P(\tau)}{p^6}$ is a unit if $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis of the ideal $I_{\mathcal{O}_t}\mathfrak{p}_{\mathcal{O}_t}$.*
3. *If p is inert in K, i. e. $(p) = \mathfrak{p}$, then*
   (a) *$\frac{\varphi_P(\alpha)}{p^{\frac{12}{p^l(p+1)}}}$ is a unit if $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis of a fractional $\mathcal{O}_{tp}$-ideal,*

(b) $\frac{\varphi_P(\alpha)}{p^{12\left[1-\frac{1}{p^{l-1}(p+1)}\right]}}$ *is a unit if* $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ *is a basis of a fractional* $\mathcal{O}_{tp^{-1}}$*-ideal.*

Theorem 20. *Let* $g(\tau)$ *be the class invariants as in Theorem 12. Then* $g(\tau)$ *is a unit if* $m \equiv 1, 5, 7 \mod 8$ *or* $m \equiv 2 \mod 4$*, where* $D(\tau) = -4m$*.*

Proof: We will prove the theorem using the equations 3 and 4 in each case.

Let $\tau \in \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'}) =: K$ with $\Delta(\tau) = -4m = t^2 d = t'^2 d'$, where d' is square free.

In the cases $m \equiv 1, 5 \mod 8$, or equivalently $m \equiv 1 \mod 4$, we have $t' \equiv 0 \mod 2$ as otherwise d' would not be a square-free integer. Letting $t' = 2s$ yields $s^2 d' \equiv -1 \mod 4$, which shows that s must be an odd integer and hence $s^2 \equiv 1 \mod 4$ and $d' \equiv -1 \mod 4$.

Hence, for $m \equiv 1 \mod 4$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{d'}]$ and $(2) = \mathfrak{p}^2$, since 2 ramifies in $\mathcal{O}_K$. Considering the basis $\{\tau, 1\}$ of $\mathcal{O}_t$ together with the matrix $P = \begin{pmatrix}1 & t\\ 0 & 2\end{pmatrix}$ we have $P\begin{pmatrix}\tau\\ 1\end{pmatrix} = [\tau + t, 2]$ as a basis of the ideal $\mathfrak{p}\mathcal{O}_t$.

Applying the result of theorem 19 (2 (c)), we have the property that $\frac{\varphi_P(\tau)}{2^6}$ is a unit, which means

$$2^{-6}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)}$$

is a unit. Now

- For $m \equiv 1 \mod 8$, we obtain by the equations 3 and 4

$$2^{-6}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)} = g(\tau)^4 = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}(\tau)^2}{\sqrt{2}}\right)^3\right)^4,$$

  which shows that the invariant $g(\tau)$ is a unit.

- For $m \equiv 5 \mod 8$, we obtain similarly

$$2^{-6}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)} = g(\tau)^2 = \left(\left(\frac{\mathfrak{f}(\tau)^4}{2}\right)^3\right)^2,$$

  which shows that the invariant $g(\tau)$ is a unit.

In the case $m \equiv 7 \mod 8$, using a similar argument as above, we have $t' \equiv 0 \mod 2$, $-d' \equiv 3 \mod 4$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$, and 2 splits completely in $\mathcal{O}_K$. Using theorem 19 (1(b)) with the basis $\{\tau + t, 1\}$ of an $\mathcal{O}_{2t}$-ideal and $P = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$, we have,

$$\frac{\varphi_P(\tau + t)}{2^{12}} = g(\tau)^8 = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}(\tau)}{\sqrt{2}}\right)^3\right)^8$$

is a unit, which shows that the invariant $g(\tau)$ is also a unit in this case.

In the last case $m \equiv 2 \mod 4$, we have $t \equiv 1 \mod 2$, $d' \equiv 2 \mod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, and 2 ramifies in $\mathcal{O}_K$. Using the theorem 19 (2(c)) again as in the first case but with an odd t,

$$2^{-6}\frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = g(\tau)^4 = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}_1(\tau)^2}{\sqrt{2}}\right)^3\right)^4$$

is a unit, which shows that the invariant $g(\tau)$ is also a unit. □

Remark 21. *1. According to the theorem 12, the invariants in theorem 20 are units in the corresponding ring class fields.*

2. For other cases, i. e. $m \equiv 3 \mod 8$ and $m \equiv 12 \mod 16$, we know that the invariants are not units in the ring class field. However, we use theorem 19 to show that there are units related to these invariants, hence we are going to show that the constant coefficients of minimal polynomials of these invariants are all powers of 2, say 2^l, with $l|h$.

We are going to show also that in the cases $m \equiv 3 \mod 24$ and $m \equiv 4 \mod 16$, we can get better class invariants. Furthermore, it will be shown that in the case $m \equiv 4 \mod 16$ the invariant given in the theorem 12 is also a unit in the ring class field.

Theorem 22. *Let $g(\tau)$ be the class invariant as in theorem 12 and h_t be the class number of the discriminant of τ.*

1. *For $m \equiv 3 \mod 8$:*
   - (a) *$\tilde{g}(\tau) := g(\tau)/2$ is a class invariant and a unit if $m \equiv 3 \mod 24$,*
   - (b) *$g(\tau)$ has the norm 2^l with $h_t = 3l$ if $m \equiv 11, 19 \mod 24$.*
2. *For $m \equiv 4 \mod 8$:*
   - (a) *$g(\tau)$ is a unit if $m \equiv 4 \mod 16$,*
   - (b) *For $m \equiv 4 \mod 16$, we write $m = 16k + 12$, then we have:*
     - *$g(\tau)$ has the norm 2^l with $h_t = 2l$ if $k \equiv 0, 1, 5 \mod 6$,*
     - *$g(\tau)$ has the norm 2^l with $h_t = 6l$ if $k \equiv 2, 4 \mod 6$,*
     - *$\tilde{g}(\tau) := g(\tau)/2$ is a class invariant with norm 2^l and $h_t = 2l$ if $k \equiv 3 \mod 6$.*

Proof: For $m \equiv 3 \mod 8$, we obtain with a similar argument as in the proof of theorem 20, $d = d' \equiv 5 \mod 8$, $t \equiv 2 \mod 4$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, and 2 is inert in $\mathcal{O}_K$.

Considering the basis $\{\tau+t, 1\}$ of an $\mathcal{O}_{2t}$-ideal with the matrix $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, we obtain $P \begin{pmatrix} \tau+t \\ 1 \end{pmatrix} = [\tau+t, 2]$ as a basis of an $\mathcal{O}_t$-ideal. Applying theorem 19, 3(b),

$$2^{-8}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)}$$

is a unit, since $t \equiv 2 \mod 4$ implies $l = 1$ and $12\left(1-(1/2^{1-1}3)\right) = 8$ and thus by the equations 4 and 3

$$2^{-8}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)} = \left(\frac{\mathfrak{f}^3}{2}\right)^8 = (\frac{g(\tau)}{2})^8.$$

In the cases $m \equiv 11, 19 \mod 24$, the function $\mathfrak{f}(\tau)$ is a class invariant by remark 13, since $\gcd(3, D(\tau)) = 1$. Hence, in these cases $g(\tau)$ has norm $2^{8h_t/24}$, which means $l = h_t/3$.

In the case $m \equiv 3 \mod 24$, we have $3|D(\tau)$, which means $l = h_t$ for $\mathfrak{f}(\tau)^3$, implying $\tilde{g}(\tau) = \mathfrak{f}(\tau)^3/2$ is a class invariant and a unit.

For $m \equiv 4 \mod 8$, we obtain

$$d' \equiv \begin{cases} 3 \mod 4 & \text{if } m \equiv 4 \mod 16, \\ 1 \mod 4 & \text{if } m \equiv 12 \mod 16. \end{cases}$$

Now for $m \equiv 4 \mod 16$, we get $\mathcal{O}_K = \mathbb{Z}[\sqrt{d'}]$, 2 ramifies in $\mathcal{O}_K$ with $t \equiv 2 \mod 4$, and hence $l = 1$. Applying theorem 19 (2(b)) for $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ with the basis $\{\tau+t, 1\}$ of an $\mathcal{O}_{2t}$-ideal, we obtain the unit

$$2^{-9}\frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}_1(\tau)^4}{2\sqrt{2}}\right)^3\right)^2 = g(\tau)^2,$$

since $2^{12-\frac{6}{2^1}} = 2^9$, which shows that $g(\tau)$ is a unit in the case $m \equiv 4 \mod 16$.

Lastly for $m \equiv 12 \mod 16$ with $d = d' \equiv 1 \mod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$, and we have two different cases:

$$d \equiv \begin{cases} 1 \mod 8, \text{ i. e. 2 splits} & \text{if } k \equiv 1, 3, 5 \mod 6 \\ 5 \mod 8, \text{ i. e. 2 is inert} & \text{if } k \equiv 0, 2, 4 \mod 6. \end{cases}$$

Moreover, $s^2 d \equiv 2k \mod 3$, which means $\gcd(3, d) = 1$ for $k \equiv 1, 2, 4, 5 \mod 6$, and hence together with remark 13 that we can consider the invariants without the outer exponent 3. Applying analogously as above theorem 19 (3(b)) for $k \equiv 0, 2, 4 \mod 6$ and 19 (1(b)) for $k \equiv 1, 3, 5 \mod 6$

together with remark 13 for $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ with the basis $\{\tau + t, 1\}$ of an $\mathcal{O}_{2t}$-ideal, we obtain the desired results. $\square$

Remark 23. *For $l = 2, 3, 5, 7, 11, 13$ and 17 and $\tau \in \mathbb{H}$, the generalized Weber functions are defined as*

$$\mathfrak{w}_l := \frac{\eta(\frac{\tau}{l})}{\eta(\tau)}.$$

(Note that $\mathfrak{w}_l = \mathfrak{f}_1$ for $l = 2$.)
Using these functions, one can obtain new class invariants (see [Enge], p. 15 and 16 or [GeSt], p. 450). In [Uz], the possibility of representing these class invariants as quotients of Thetanullwerte is discussed. Moreover, it is shown that most of these invariants are units using theorem 19, and that better class invariants can be obtained in some cases as in theorem 20.

5 Unit Group

Due to the fact that the class invariants are units in most cases in the corresponding ring class fields by theorems 20 and 22, we know the h_t different units of the field Ω_t, which is a totally complex field of absolute degree $2h_t$. By the Dirichlet's unit theorem, we know that the unit rank of the field Ω_t is $h_t - 1$.

Since we know the conjugates of $g(\tau)$ explicitly, we can compute the full unit group, if the $h_t - 1$ conjugates of any $g(\tau)$ form a subgroup U_{Ω_t} of the unit group E_{Ω_t} of finite index. In this case one can obtain a larger subgroup U'_{Ω_t} by checking whether certain elements are $p-$th powers, see for the details [Haj] and [PhZs]. An upper bound B for the index can be found by using a lower bound for the regulator of Ω_t, which can be found using the algorithm of Fieker and Pohst, see [FiPohst].

Algorithm: Computation of Unit Group of Ω_t

Input: An order $\mathcal{O}_t$ of an imaginary quadratic number field K with the conductor t, $\tau \in \mathcal{O}_t$ and $D(\tau) = -4m$, where m satisfies the congruence conditions of the theorems 20 or 22, so that $g(\tau)$ is a unit.
Output: The generators of E_{Ω_t} of Ω_t.

1. Find $h_t - 1$ roots $\epsilon_1, \cdots, \epsilon_{h_t-1}$ of $W_{D(\tau)}(x)$, so that the upper bound B is minimal. If $B = \infty$ go to (5). If not go to (2).
2. List all prim numbers $p_i \leq B$, $i = 1, \cdots, n$.
3. For $i = 1$ to n

(a) find the power e_i of p_i, with the units $\gamma_1, \cdots, \gamma_{h_t-1}$, which form together with the roots of unity a subgroup of index $(E_{\Omega_t} : U_{\Omega_t})/p_i^{e_i}$.

(b) Set $\epsilon_1, \cdots, \epsilon_{h_t-1} := \gamma_1, \cdots, \gamma_{h_t-1}$.

4. Return the fundamental units $\gamma_1, \cdots, \gamma_{h_t-1}$ of Ω_t.

5. Return *The units form a subgroup of smaller rank.*

In all examples we computed, we observed that the suitable $h_t - 1$ conjugates of units obtained by the theorems 20 and 22 form a subgroup of finite index if $m \not\equiv 5 \bmod 8$. Although the upper bound can become too large to use the above algorithm, this method is the most efficient one to compute the unit group of the corresponding ring class fields, since the units are explicitly known. We have the following conjecture:

Conjecture 24. *If $m \not\equiv 5 \bmod 8$, the units constructed by the theorems 20 and 22 together with their conjugates form a subgroup of full rank of the corresponding unit group E_{Ω_t}.*

There are analogous results concerning elliptic units, see [Haj], which are the quotients of $\Delta-$function. They form a subgroup of full rank.

Our numerical observations and the fact that elliptic units are mostly 24th powers of the units of theorem 20 and 22 by the equation 3 support the conjecture.

6 Examples

6.1 Class units

Let l be the largest absolute value of the coefficient of the class polynomial W_D of $g(\tau)$ and l' be the largest absolute value of the coefficient of the class polynomial $\tilde{W}_D$ of $g(\tau)/2$ for the cases $m \equiv 3 \bmod 24$ and $m \equiv 4 \bmod 16$ with $k \equiv 3 \bmod 6$ as in the theorem 22.

Let further $D = t^2 d$ be the discriminant of the order $\mathcal{O}_t$ with $h_D := h_t$. We obtained the following results for $\gamma = l/l'$ using MAGMA, see [MAGMA]:

D	h_D	l	l'	γ
-108	3	12	3	4.0
-204	6	144	9	16.0
-240	4	25464	6336	4.0
-624	8	1935551872	181257400	10.68
-684	12	86016	139	618.8201
-1356	18	86114304	25812	3336.212
-2544	20	$\leq 5.54 \cdot 10^{26}$	$\leq 6.3 \cdot 10^{24}$	≥ 87.68
-11496	36	$\leq 3.47 \cdot 10^{24}$	$4.98 \cdot 10^{15}$	≥ 696793.64
-59436	96	$\leq 2,3 \cdot 10^{66}$	$\leq 3.92 \cdot 10^{47}$	$\geq 5,63 \cdot 10^{17}$
-123888	104	$\leq 7.03 \cdot 10^{235}$	$\leq 8.30 \cdot 10^{224}$	$\geq 8.45 \cdot 10^{10}$
-4266864	1056	$\leq 1.98 \cdot 10^{2652}$	$\leq 3.65 \cdot 10^{2555}$	$\geq 5.41 \cdot 10^{96}$
-5867436	744	$\leq 7.9 \cdot 10^{777}$	$\leq 5.25 \cdot 10^{644}$	$\geq 1.5 \cdot 10^{133}$
-12677616	2000	$\leq 2 \cdot 10^{5308}$	$\leq 3.4 \cdot 10^{5127}$	$\geq 5.8 \cdot 10^{180}$
-45657072	2500	$\leq 2.6 \cdot 10^{7848}$	$\leq 3.7 \cdot 10^{7626}$	$\geq 7.1 \cdot 10^{221}$
-62506668	1992	$\leq 5.20 \cdot 10^{2346}$	$6.79 \cdot 10^{1987}$	$\geq 7.65 \cdot 10^{358}$

6.2 θ versus η

We compute the class polynomials using the invariants of theorem 12 with a fixed precision for several discriminants. We obtained the following table using MAGMA, see [MAGMA]. Moreover, the values of $\eta-$functions are computed using theorem 18.

D	h_D	Prec	η	θ	q
-104	6	8	0.04	0.01	4.0
-260	8	12	0.05	0.01	5.0
-684	12	40	0.09	0.02	4.5
-1652	20	63	0.16	0.04	4.0
-3740	28	85	0.25	0.07	3.57
-14928	32	144	0.41	0.12	3.42
-20904	40	147	0.46	0.12	3.83
-39076	52	291	1.13	0.27	4.18
-63372	96	393	2.43	0.56	4.34
-77364	112	613	10.46	2.87	3.64
-91068	122	467	5.66	1.34	4.22
-107976	144	375	4.74	1.14	4.16
-189744	168	664	15.68	3.87	4.05
-1021732	292	1517	136.4	33.33	4.09

Prec denotes the fixed precision we used, and q the quotient of the time required to compute the polynomials using eta representations by the time required to compute them using theta representations (given in seconds in the columns η and θ respectively).

6.3 Unit group

We consider the example $m = 24 \cdot 3 + 3$. In this case the class polynomial, obtained from the new class invariant by theorem 22, is

$$\tilde{W}_{-204}(x) = x^6 - 8x^5 - 3x^4 + 6x^3 + 9x^2 + 2x + 1.$$

Let $\tilde{g}(\tau)$ be the class invariant. Then the lower regulator bound $L = K(\tilde{g}(\tau))$, using computer algebra system KANT/KASH, [Pohst], is 43.3706. Using the conjugate units $\tilde{g}^{(i)}$, for $i = 1, \cdots, 5$, we compute $\det(\mathcal{R}) = 74.6592$. Hence, the upper bound for the index is $74.6592/43.3706 = 1.7214$, which means the invariants are already fundemental units of $L = K(\tilde{g}(\tau)) = K(j(\tau))$.

References

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

[Birch] B. Birch, *Weber's Class Invariants*, Mathematika **16** (1969), 283–294

[BrSt] 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**, 17-28, 2008

[BSS1] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press (1999)

[BSS2] I. Blake, G. Seroussi, N. Smart, *Advances in Elliptic Curves in Cryptography*, Cambridge University Press (2005)

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

[Dup] R. Dupont, *Fast Evaluation of Modular Functions Using Newton Iterations and the AGM*, to appear in Mathematics of Computation, 2007

[Enge] A. Enge, *Courbe Algébriques et Cryptologie*, Habilitation, Université Paris, 2007, http://www.math.u-bordeaux1.fr/ enge/vorabdrucke/Enge-Habil.pdf

[FiPohst] C. Fieker, M. Pohst *A Lower Regulator Bound for Number Fields*, Journal of Number Theory **128** (2008), 2767–2775

[FST] D. Freeman, M. Scott, E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*, http://eprint.iacr.org/2006/372.pdf (2006)

[GeSt] A. Gee, P. Stevenhagen, *Generating Class Fields Using Shimura Reciprocity*, LNCS 1423, (ANTS-III), 1998, 441–453

[Haj] F. Hajir, *Unramified Elliptic Units*, PhD Thesis, Princeton University (1988)

[HinSil] M. Hindry, J. Silverman, *Diophantine Geometry-An Introduction*, Springer-Verlag, New York, 2000

[Lang] S. Lang, *Elliptic Functions*, Addison-Wesley (1973)

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

[PhZs] M. Pohst, H. Zassenhaus *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989

[Pohst] M. Pohst, et al. *KANT/KASH* http://www.math.tu-berlin.de/ kant/kash.html

[MAGMA] MAGMA Computational Algebra System, http://magma.maths.usyd.edu.au/magma/

[Sar] P. Sarnak, *Selberg's Eigenvalue Conjecture*, Notices of AMS, vol. **42**, 1272-1277, 1995

[Sch] R. Schertz, *Weber's Class Invariant's Revisited*, Journal de Théorie des Nombres de Bordeaux **14** (2002), 325–343

[Sch1] R. Schertz, *Die singulären Werte der Weberschen Funktionen* $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2, \gamma_2, \gamma_3$, J. Reine Angew. Math **286/287** (1976), 46–74

[Uz] O. Uzunkol, *Über die Konstruktion algebraischer Kurven mittels komplexer Multiplikation* Dissertation, TU-Berlin, 2010

[Wb] H. Weber, *Lehrbuch der Algebra*, Bd. 3, 2. Aufl. Braunschweig (1908)

[Weng] A. Weng, *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*, Dissertation, Universität GH Essen (2001)