Generalised Weber Functions

Andreas Enge
INRIA, LFANT
CNRS, IMB, UMR 5251
Univ. Bordeaux, IMB
33400 Talence
France
andreas.enge@inria.fr

François Morain
INRIA Saclay–Île-de-France
& LIX (CNRS/UMR 7161)
École polytechnique
91128 Palaiseau Cedex
France
morain@lix.polytechnique.fr

20 December 2013

Abstract

A generalised Weber function is given by $\mathfrak{w}_N(z) = \eta(z/N)/\eta(z)$, where $\eta(z)$ is the Dedekind function and N is any integer; the original function corresponds to $N = 2$. We classify the cases where some power $\mathfrak{w}_N^e$ evaluated at some quadratic integer generates the ring class field associated to an order of an imaginary quadratic field. We compare the heights of our invariants by giving a general formula for the degree of the modular equation relating $\mathfrak{w}_N(z)$ and $j(z)$. Our ultimate goal is the use of these invariants in constructing reductions of elliptic curves over finite fields suitable for cryptographic use.

1 Introduction

Let K be an imaginary quadratic field of discriminant $\Delta < 0$. We are interested in orders $\mathcal{O}$ of K having discriminant $D = c^2\Delta$. The principal order of discriminant Δ is $\mathcal{O}_K$, which is generated by $\omega = \frac{1+\sqrt{\Delta}}{2}$ if $\Delta \equiv 1 \pmod 4$ resp. $\omega = \frac{\sqrt{\Delta}}{2}$ if $\Delta \equiv 0 \pmod 4$. For any order $\mathcal{O}$ of discriminant D, let K_D denote the ring class field that is associated to it. It is well-known that if j denotes the modular invariant, then $K_D = K(j(c\omega))$; so $K_D/K \simeq K[X]/(H_D(X))$, where the *class polynomial* H_D is the minimal polynomial of $j(c\omega)$. It can be used to obtain elliptic curves over finite fields with a number of points known in advance, with applications to cryptology,

2010 Mathematics Subject Classification: 11G15, 14K22
Key words: complex multiplication, class invariants, eta quotients

in particular based on the Weil or Tate pairing (cf. [13]), and primality proving [1].

Since the class polynomial has a rather large height, it is desirable to find smaller defining polynomials to speed up the computations. There is a long history of such studies, going back to at least Weber [27]; see, e.g., [2, 26, 20] for connections with the class number 1 problem. Generally modular functions f and special arguments $\alpha \in \mathcal{O}$ are considered such that the *singular value* $f(\alpha)$ lies in K_D, in which case $f(\alpha)$ is called a *class invariant.*

Our ultimate goal is to build elliptic curves having CM, and this is done using a so-called modular equation (with integer coefficients) relating a modular function f to j. For this to be efficient, we need $f(\alpha)$ to have a small height *and* the corresponding modular equation to be of small genus (with a predilection for genus 0).

Part of the literature has concentrated on the functions introduced by Weber, quotients of two η-functions with a transformation of level 2 applied to one of them, see [23, 14, 15, 22] besides the already cited sources. This is a perfect case for us, since the genus of the associated modular curve is 0.

Results on more general η-quotients are given in [18, 17, 19, 14, 8, 12]. All of them are obtained using the modern tool for determining the Galois action of the class group of $\mathcal{O}$ on singular values of modular functions, namely Shimura's reciprocity law [25]. The present article is no exception to this rule. For the sake of self-containedness and the reader's ease, we briefly summarise in §2 the reciprocity law in the version of [22], which is most suited to actual computations.

In this article, we propose a systematic study of class invariants obtained as singular values of the *generalised Weber* functions $\mathfrak{w}_N$, defined and studied in §3, which are quotients of two η-functions with a transformation of level N applied to one of them. These appear in [22, Table 1] and as a special case of [19]. While there is some overlapping between this article and [19], we follow a different approach: The authors of [19] use an ideal in the class group to transform the η-function, and the norm of the ideal implicitly determines the level; they then proceed to prove which root of unity is needed for twisting the function so that a minimal power of it yields a class invariant. On the other hand, we start with a fixed level and thus a fixed generalised Weber function and determine the minimal power yielding class invariants without using additional roots of unity.

A first result on the "canonical" power $\mathfrak{w}_N^s$ is readily obtained in §4 by a direct application of Shimura reciprocity. Examining the Galois action on the singular values in §5 allows us to determine the precise conditions under which lower powers $\mathfrak{w}_N^e$ with $e \mid s$ yield class invariants in §6.

While there is always some transformation level N (or, equivalently, an ideal in the class group) such that the corresponding generalised Weber function yields a class invariant, fixing the level first as we do it in this study implies control over the height of the class invariants. Indeed, this height, an important measure for the complexity of computing a class polynomial, is asymptotically given as a function of the degrees of the modular polynomials relating the modular function to the j-invariant. Thus, the generalised Weber functions can be ordered totally with respect to their computational efficiency, see §7, and the invariants can be compared directly to other invariants in the literature, cf. [7, 10].

Unlike [19], we explicitly consider levels N that are not coprime to 6, a considerable source of complication, which is justified since the corresponding functions tend to yield class invariants of lower height, see the formulæ in §7.2 and Table 7.2. Otherwise said, the corresponding modular curves, related to 2- and 3-torsion points on elliptic curves, have a lower genus than would be expected from the size of N alone. This makes it easier to construct the associated elliptic curves with complex multiplication; in particular, [21] shows how $\mathfrak{w}_3$ can be used to directly write down the correct twist of the elliptic curve with the desired number of points over a finite field.

Existing results in the literature often only state when a singular value is a class invariant; to obtain the class polynomial, however, one needs an explicit description of its algebraic conjugates. These can be worked out using Shimura reciprocity again; following the approach of N-systems introduced in [22], we obtain synthetic and simple descriptions of the conjugates, and moreover determine when the class invariant has a minimal polynomial with rational coefficients, that is, it defines the real subfield of the class field over $\mathbb{Q}$.

2 Class invariants by Shimura reciprocity

In the following, we denote by $f \circ M$ the action of matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \mathrm{Sl}_2(\mathbb{Z})/\{\pm 1\}$ on modular functions given by

$$(f \circ M)(z) = f(Mz) = f\left(\frac{az+b}{cz+d}\right).$$

For $n \in \mathbb{N}$, let $\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}$ be the principal congruence subgroup of level n; for a congruence subgroup Γ' such that $\Gamma(n) \subseteq \Gamma' \subseteq \Gamma$, denote by $\mathbb{C}_{\Gamma'}$ the field of modular functions for Γ'. One of the most important congruence subgroups is given by $\Gamma^0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \pmod{n} \right\}$.

Definition 2.1. *The set $\mathcal{F}_n$ of modular functions of level n rational over the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ is given by all functions f such that*

1. *f is modular for $\Gamma(n)$ and*

2. *the q-expansion of f has coefficients in $\mathbb{Q}(\zeta_n)$, that is,*

$$f \in \mathbb{Q}(\zeta_n)\left(\left(q^{1/n}\right)\right),$$

where $q^{1/n} = e^{2\pi iz/n}$.

The function field extension $\mathcal{F}_n/\mathbb{Q}(j)$ has Galois group isomorphic to $\mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$, where the isomorphism is defined by the following action of matrices on functions:

- $(f \circ M)(z) = f(Mz)$ as above for $M \in \Gamma$; this implies in particular that also the q-expansion of $f \circ M$ has coefficients in $\mathbb{Q}(\zeta_n)$;
- $f \circ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ for $\gcd(d, n) = 1$ is obtained by applying to the q-expansion of f the automorphism $\zeta_n \mapsto \zeta_n^d$;
- any other matrix M that is invertible modulo n may be decomposed as $M \equiv M_1 \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} M_2 \pmod{n}$ with $\gcd(d, n) = 1$ and $M_1, M_2 \in \Gamma$, and
$$(f \circ M)(z) = \left(\left((f \circ M_1) \circ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \right) \circ M_2 \right) (z).$$

Shimura reciprocity makes a link between the Galois group of the function field $\mathcal{F}_n$ and the Galois groups of class fields generated over an imaginary-quadratic field by singular values of modular functions.

Theorem 2.2 (Shimura's reciprocity law, Th. 5 of [22], Th. 5.1.2 of [24])**.** *Let f be a function in $\mathcal{F}_n$, $\Delta < 0$ a fundamental discriminant and $\mathcal{O}$ the order of $K = \mathbb{Q}(\sqrt{\Delta})$ of conductor c. In the following, all $\mathbb{Z}$-bases of ideals are written as column vectors. Let $\mathfrak{a} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}_{\mathbb{Z}}$ with basis quotient $\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{H}$ be a proper ideal of $\mathcal{O}$, $\mathfrak{m}$ an ideal of $\mathcal{O}_K$ of norm m prime to cn, $\overline{\mathfrak{m}}$ its conjugate ideal and $M \in \mathrm{Gl}_2(\mathbb{Z})$ a matrix of determinant m such that $M \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$ is a basis of $\mathfrak{a}(\overline{\mathfrak{m}} \cap \mathcal{O})$. If f does not have a pole in α, then*

- *$f(\alpha)$ lies in the ray class field modulo cn over K and*
- *the Frobenius map $\sigma(\mathfrak{m})$ acts as*
$$f(\alpha)^{\sigma(\mathfrak{m})} = (f \circ mM^{-1})(M\alpha).$$

In the following, we are particularly interested in *class invariants*, that is, values $f(\alpha)$ that lie not only in a ray class field, but even in a ring class field. Using Shimura's reciprocity law, [22, Th. 4] gives a very general criterion for class invariants, which is the basis for our further investigations.

Theorem 2.3. *Let $f \in \mathbb{C}_{\Gamma^0(n)}$ for some $n \in \mathbb{N}$ be such that f itself and $f \circ S$ have rational q-expansions. Denote by $\alpha \in \mathbb{H}$ a root of the primitive form $[A, B, C]$ of discriminant D with $\gcd(A, n) = 1$ and $n \mid C$. If α is not a pole of f, then $f(\alpha) \in K_D$.*

The conjugates of $f(\alpha)$ are then derived generically in a form that is well suited for computations in [22, Prop. 3 and Th. 7], [24, Th. 5.2.4].

Theorem 2.4. *An n-system for the discriminant D is a complete system of equivalence classes of primitive quadratic forms $[A_i, B_i, C_i] = A_i X^2 + B_i X + C_i$, $i = 1, \ldots, h(D)$, of discriminant $D = B_i^2 - 4A_iC_i$, such that* $\gcd(A_i, n) = 1$ *and* $B_i \equiv B_1 \pmod{2n}$. *Such a system exists for any n. To these quadratic forms, we associate in the following the quadratic numbers $\alpha_i = \frac{-B_i+\sqrt{D}}{2A_i}$.*

Let $f \in \mathcal{F}_n$ be such that $f \circ S$ with $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has a rational q-expansion. If $f(\alpha_1) \in K_D$, then a complete system of conjugates of $f(\alpha_1)$ under the Galois group of K_D is given by the $f(\alpha_i)$, and the characteristic polynomial of $f(\alpha_1)$ over K is

$$H_D[f] = \prod_{i=1}^{h(D)} (X - f(\alpha_i)).$$

3 The generalised Weber functions $\mathfrak{w}_N$

In this section we examine the general properties of the function $\mathfrak{w}_N$, with the aim in mind of applying Theorem 2.3 to its powers.

Let z be any complex number and put $q = e^{2i\pi z}$. Dedekind's η-function is defined by [5]

$$\eta(z) = q^{1/24} \prod_{m \geqslant 1} (1 - q^m).$$

The Weber functions are [27, § 34, p. 114]

$$\mathfrak{f}(z) = \zeta_{48}^{-1} \frac{\eta((z+1)/2)}{\eta(z)}, \quad \mathfrak{f}_1(z) = \frac{\eta(z/2)}{\eta(z)}, \quad \mathfrak{f}_2(z) = \sqrt{2}\,\frac{\eta(2z)}{\eta(z)}.$$

The modular invariant j is recovered via [27, § 54, p. 179]:

$$j(z) = \frac{(\mathfrak{f}^{24} - 16)^3}{\mathfrak{f}^{24}} = \frac{(\mathfrak{f}_1^{24} + 16)^3}{\mathfrak{f}_1^{24}} = \frac{(\mathfrak{f}_2^{24} + 16)^3}{\mathfrak{f}_2^{24}}.$$

The functions $-\mathfrak{f}^{24}$, $\mathfrak{f}_1^{24}$ and $\mathfrak{f}_2^{24}$ are the three roots of the modular polynomial

$$\Phi_2^c(F, j) = F^3 + 48\,F^2 + F(768 - j) + 4096,$$

that describes the curve $X_0(2)$.

For an integer $N > 1$, let the *generalised Weber function* be defined by

$$\mathfrak{w}_N = \frac{\eta(z/N)}{\eta(z)}.$$

As shown in the following, there is a canonical exponent t such that $\mathfrak{w}_N^t$ is modular for $\Gamma^0(N)$. Its minimal polynomial $\Phi_N^c(F, j)$ over $\mathbb{C}(j)$ is a model for $X_0(N)$. The other roots of this polynomial can be expressed in terms of η, too, a topic to which we come back in §7.

We need to know the behaviour of $\mathfrak{w}_N$ under unimodular transformations, which can be broken down to the transformation behaviour of $\eta(z/K)$ for $K = 1$ or N. This has been worked out in [9, Th. 3].

Theorem 3.1. *Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ be normalised such that $c \geqslant 0$, and $d > 0$ if $c = 0$. Write $c = c_1 2^{\lambda(c)}$ with c_1 odd; by convention, $c_1 = \lambda(c) = 1$ if $c = 0$. Define*

$$\varepsilon(M) = \left(\frac{a}{c_1}\right) \zeta_{24}^{ab+c(d(1-a^2)-a)+3c_1(a-1)+\frac{3}{2}\lambda(c)(a^2-1)}.$$

For $K \in \mathbb{N}$ write

$$ua + vKc = \delta = \gcd(a, Kc) = \gcd(a, K).$$

Then

$$\eta\left(\frac{z}{K}\right) \circ M = \varepsilon \begin{pmatrix} \frac{a}{\delta} & -v \\ \frac{Kc}{\delta} & u \end{pmatrix} \sqrt{\delta(cz+d)}\, \eta\left(\frac{\delta z + (ub + vKd)}{\frac{K}{\delta}}\right),$$

where the square root is chosen with positive real part.

Theorem 3.2. *The function w_N has a rational q-expansion. Denote by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ the matrix belonging to the inversion $z \mapsto -\frac{1}{z}$. If N is a square, then $\mathfrak{w}_N \circ S$ has a rational q-expansion. Otherwise, $\mathfrak{w}_N^2 \circ S$ has a rational q-expansion.*

Let the subscript 1 and the function λ have the same meaning for a positive integer n as in Theorem 3.1, that is, $n = n_1 2^{\lambda(n)}$ with n_1 odd. If $M = \begin{pmatrix} a & Nb_0 \\ c & d \end{pmatrix} \in \Gamma^0(N)$, then $\mathfrak{w}_N \circ M = \varepsilon\, \mathfrak{w}_N$ with

$$\varepsilon = \left(\frac{a}{N_1}\right) \zeta_{24}^{(N-1)(-b_0 a + c(d(1-a^2)-a))} \zeta_4^{c_1 \frac{(N_1-1)(a-1)}{2}} (-1)^{\frac{\lambda(N)(a^2-1)}{8}}. \tag{3.1}$$

Let $t = \frac{24}{\gcd(N-1, 24)}$ measure how far $N-1$ is from being divisible by 24, and let e and s be such that $t \mid s \mid 24$ and $e \mid s$. If N_1 is a square or e is even, then $\mathfrak{w}_N^e$ is modular for $\Gamma\left(\frac{s}{e}\right) \cap \Gamma^0\left(\frac{s}{e}N\right)$. Otherwise, $\mathfrak{w}_N^e$ is modular for $\Gamma\left(\frac{s}{e}N_1\right) \cap \Gamma^0\left(\frac{s}{e}N\right)$. In both cases, $\mathfrak{w}_N^e \in \mathcal{F}_{\frac{s}{e}N} \subseteq \mathcal{F}_{24N}$.

Proof. The q-expansion of w_N is rational since that of η is. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. By Theorem 3.1 applied to $K = 1$ and N, we have

$$\mathfrak{w}_N \circ M = \varepsilon \begin{pmatrix} \frac{a}{\delta} & -v \\ \frac{Nc}{\delta} & u \end{pmatrix} \varepsilon \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \sqrt{\delta}\, \frac{\eta\left(\frac{\delta z + (ub + vNd)}{\frac{N}{\delta}}\right)}{\eta(z)} \tag{3.2}$$

with $\delta = \gcd(a, N) = ua + vNc$.

In the special case $M = S$ we obtain $\delta = N$, $v = 1$, $u = 0$ and

$$\mathfrak{w}_N \circ S = \sqrt{N}\,\frac{\eta(Nz)}{\eta(z)},$$

which proves the assertion on the q-expansion of $\mathfrak{w}_N \circ S$.

Assume now that $M \in \Gamma^0(N)$. Letting $b = Nb_0$, we have $\delta = 1$, $u = d$ and $v = -b_0$ since $ad - bc = 1$. Thus, (3.2) specialises as

$$\mathfrak{w}_N \circ M = \varepsilon \begin{pmatrix} a & b_0 \\ Nc & d \end{pmatrix} \varepsilon \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \frac{\eta(z/N)}{\eta(z)} = \varepsilon\, \mathfrak{w}_N(z)$$

with

$$\varepsilon = \left(\frac{a}{c_1 N_1}\right)\left(\frac{a}{c_1}\right)^{-1} \zeta_{24}^{(b_0-b)a+c(N-1)(d(1-a^2)-a)+3c_1(N_1-1)(a-1)+\frac{3}{2}(\lambda(Nc)-\lambda(c))(a^2-1)},$$

which proves (3.1).

We need to examine under which conditions $\varepsilon^e = 1$. The Legendre symbol vanishes when N_1 is a square, e is even or $a \equiv 1 \pmod{N_1}$. The exponent of ζ_{24} becomes divisible by $s(N-1)$ and thus by 24 whenever $\frac{s}{e}$ divides b_0 and c.

In the case of odd N, we have $\lambda(N) = 0$ and $N = N_1$, and the condition on a implies that the exponent of ζ_4 is divisible by 4.

In the case of even N, the coefficient a is odd since $\det M = 1$, and

$$\varepsilon^e = (-1)^{e\left(c_1 \frac{(N_1-1)(a-1)}{4} + \lambda(N)\frac{a^2-1}{8}\right)}.$$

For even e, there is nothing to show. If e is odd, then $8 \mid t \mid s$ implies that $a \equiv 1 \pmod 8$, which finishes the proof. □

4 Full powers of $\mathfrak{w}_N$

To be able to apply Theorem 2.3 directly to powers of $\mathfrak{w}_N$, we are interested in the minimal exponent s such that $\mathfrak{w}_N^s$ is invariant under $\Gamma^0(N)$ and $\mathfrak{w}_N^s \circ S$ has a rational q-expansion. From Theorem 3.2, we recover the integer $t = 24/(\gcd(N-1, 24))$ and recall that $s = 2t$ if t is odd and N is not a square, and $s = t$ otherwise.

4.1 Arithmetical prerequisites

We begin with the following purely arithmetical lemma.

Lemma 4.1. *Let N be an integer. For a prime p, denote by v_p the p-adic valuation. Let $D = c^2\Delta$ be a discriminant with fundamental part Δ. Then D admits a square root B modulo $4N$ if and only if for each prime p dividing N, one of the following holds.*

1. $\left(\frac{\Delta}{p}\right) = +1$;

2. $\left(\frac{\Delta}{p}\right) = -1$ *and* $v_p(N) \leqslant 2v_p(c)$;

3. $\left(\frac{\Delta}{p}\right) = 0$ *and* $v_p(N) \leqslant 2v_p(c) + 1$.

Proof. The Chinese remainder theorem allows to argue modulo the different prime powers dividing N. The argumentation is slightly different for p odd and even, and we give some hints only for $p = 2$.

When $\Delta \equiv 1 \bmod 8$, Δ admits a square root modulo any power of 2.

When Δ is even, then $\Delta \equiv 8$ or $12 \pmod{16}$, and Δ is a square modulo 8, but not modulo any higher power of 2. Therefore, $c^2\Delta$ is a square modulo $4N$ if and only if $v_2(c^2) + 3 \geqslant v_2(4N)$.

When $\Delta \equiv 5 \bmod 8$, Δ has a square root modulo 4 but not modulo 8, so that $v_2(c^2) + 2 \geqslant v_2(4N)$ is needed in that case. □

In the following, arithmetical conditions on a prime p to be representable by the principal form of discriminant D will be needed. We take the following form of Dirichlet's theorem from [3, Ch. 4] (alternatively, see [4, Chap 18, G]). For an integer p, let $\chi_4(p) = \left(\frac{-1}{p}\right)$ and $\chi_8(p) = \left(\frac{2}{p}\right)$. The *generic characters* of $D = c^2\Delta$ are defined as follows:

(a) $\left(\frac{p}{q}\right)$ for all odd primes q dividing D;

(b) if D is even:

- (i) $\chi_4(p)$ if $D/4 \equiv 3, 4, 7 \pmod 8$;
- (ii) $\chi_8(p)$ if $D/4 \equiv 2 \pmod 8$;
- (iii) $\chi_4(p) \cdot \chi_8(p)$ if $D/4 \equiv 6 \pmod 8$;
- (iv) $\chi_4(p)$ and $\chi_8(p)$ if $D/4 \equiv 0 \pmod 8$.

Note that if D is fundamental (i.e., $c = 1$), then case (iv) cannot occur and in case (i), we may have $D/4 \equiv 3, 7 \pmod 8$ only.

Theorem 4.2. *An integer p such that* $\gcd(p, 2cD) = 1$ *is representable by some class of forms in the principal genus of discriminant D if and only if all generic characters $\chi(p)$ have value $+1$. In particular, this condition is necessary for representability by the principal class.*

4.2 Class invariants

Theorem 4.3. *Let N be an integer and $t = \frac{24}{\gcd(N-1, 24)}$. If t is odd and N is not a square, let $s = 2t$, otherwise, let $s = t$. Suppose D satisfies Lemma 4.1. Consider an N-system of forms $[A_i, B_i, C_i]$ with roots $\alpha_i = \frac{-B_i + \sqrt{D}}{2A_i}$ such that $B_i \equiv B \pmod{2N}$, as introduced in 2.4. Then the singular values $\mathfrak{w}_N^s(\alpha_i)$ lie in the ring class field K_D, and they form a complete set of Galois conjugates.*

Proof. Once the existence of B is verified, the form $[1, B, C]$ with $C = \frac{B^2-D}{4}$ is of discriminant D and satisfies $N \mid C$. The assertion of the theorem is then a direct consequence of Theorems 2.3 and 3.2. $\square$

Sometimes, the characteristic polynomial of $\mathfrak{w}_N^s$ is real, so that its coefficients lie in $\mathbb{Z}$ instead of the ring of integers of $\mathbb{Q}(\sqrt{D})$. It is then interesting to determine the pairs of quadratic forms that lead to complex conjugates.

Theorem 4.4. *Under the assumptions of Theorem 4.3, let* $B \equiv 0 \pmod{N}$*, which is possible whenever* N *is odd and* $N \mid D$*, or* N *is even and* $4N \mid D$*. Then the characteristic polynomial of* $\mathfrak{w}_N^s$ *is real. More precisely, if* α_i *and* α_j *are roots of inverse forms of the* N*-system, then* $\mathfrak{w}_N^s(\alpha_j) = \overline{\mathfrak{w}_N^s(\alpha_i)}$.

Proof. Notice that $B \equiv 0 \pmod{N}$ and $B_i \equiv B \pmod{2N}$ imply $-B_i \equiv B \pmod{2N}$, so that $[A_i, -B_i, C_i]$, the inverse form of $[A_i, B_i, C_i]$, satisfies the N-system constraint; thus $\mathfrak{w}_N^s(\alpha_j) = \mathfrak{w}_N^s\left(\frac{B_i+\sqrt{D}}{2A_i}\right) = \mathfrak{w}_N^s(\overline{-\alpha_i})$. On the other hand, $q(\overline{-\alpha_i}) = \overline{q(\alpha_i)}$, which implies $\mathfrak{w}_N(\overline{-\alpha_i}) = \overline{\mathfrak{w}_N(\alpha_i)}$ since $\mathfrak{w}_N$ has a rational q-expansion. $\square$

These first results, direct consequences of the Shimura reciprocity law, are meant to set the stage for the detailed and much more involved analysis of lower powers in the following chapters. For $\gcd(N, 6) = 1$, [19, Theorem 20] determines a 48-th root of unity ζ and an exponent $e \mid s$ such that $\zeta \mathfrak{w}_N^e$ yields a class invariant. With a bit of work, it can be shown that $\zeta^{s/e} = 1$ in our context, which provides an alternative proof of Theorem 4.3 without giving the algebraic conjugates of the singular value.

5 Explicit Galois action

Throughout the remainder of this section, we assume that N is a square or e is even, so that $f = \mathfrak{w}_N^e$ and $f \circ S$ have rational q-expansions by Theorem 3.2. Let α be a root of the primitive quadratic form $[A, B, C]$ of discriminant D with $\gcd(A, N) = 1$. By Theorems 3.2 and 2.2, the singular value $f(\alpha)$ lies in the ray class field modulo $c\frac{t}{e}N$ over K, and the Galois action of ideals in $\mathcal{O}_K$ can be computed explicitly. We eventually need to show that the action of principal prime ideals generated by elements in $\mathcal{O}$ is trivial, which implies that the singular value lies in the ring class field K_D. Then Theorems 3.2 and 2.4 show that the conjugates are given by the singular values in a $\frac{t}{e}N$-system.

We are only interested in the situation that $N \mid C$. Notice that under $\gcd(A, N) = 1$ this is equivalent to $4N \mid 4AC = B^2 - D$, or $B^2 \equiv D \pmod{4N}$. The remainder of this section is devoted to computing in this case the Galois action of principal prime ideals (π) with $\pi \in \mathcal{O}$ coprime to $6cN$ on the singular values according to the arithmetic properties of N and D. §6 applies these results to the determination of class invariants.

To apply Shimura reciprocity in the formulation of Theorem 2.2, we need to explicitly write down adapted bases for the different ideals. So let $\mathfrak{a} = \begin{pmatrix} A\alpha \\ A \end{pmatrix}_{\mathbb{Z}}$ be an ideal of $\mathcal{O} = \begin{pmatrix} A\alpha \\ 1 \end{pmatrix}_{\mathbb{Z}}$ with basis quotient α. Without loss of generality, we may assume that $p = \mathrm{N}(\pi) \mid C$ by suitably modifying α: Indeed, notice that the quadratic form associated to $\alpha' = \alpha - 24kN$ for some $k \in \mathbb{Z}$ is given by $[A, B', C'] = [A, B + 2A(24kN), A(24kN)^2 + B(24kN) + C]$. This form still satisfies $N \mid C'$, and furthermore $f(\alpha') = f(\alpha)$ since f is invariant under translations by $24N$ according to Theorem 3.2. Since p splits in $\mathcal{O}$ and is prime to c, the equation $AX^2 + BX + C$ has a root x modulo p. Choosing $k \in \mathbb{Z}$ such that $k \equiv x(24N)^{-1} \pmod{p}$, which is possible since $p \nmid 6N$, we obtain $p \mid C'$.

Let $\pi = u + vA\alpha$ with $u, v \in \mathbb{Z}$. From

$$p = \mathrm{N}(\pi) = u(u - vB) + v^2 AC \tag{5.1}$$

and $p \mid C$ we deduce that p divides u or $u' = u - vB$. Using $A\overline{\alpha} = -A\alpha - B$ and $N(A\alpha) = AC$, we compute

$$\overline{\mathfrak{p}}\mathfrak{a} = \overline{\pi} \begin{pmatrix} A\alpha \\ A \end{pmatrix} = \begin{pmatrix} uA\alpha + vAC \\ uA - vA^2\alpha - vAB \end{pmatrix} = \begin{pmatrix} u & vC \\ -vA & u - vB \end{pmatrix} \begin{pmatrix} A\alpha \\ A \end{pmatrix}$$

So if $p \mid u$, the matrix M of Theorem 2.2 is given by

$$M = \begin{pmatrix} u & vC \\ -vA & u - vB \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} M_1 \text{ with } M_1 = \begin{pmatrix} \frac{u}{p} & v\frac{C}{p} \\ -vA & u' \end{pmatrix} \in \Gamma^0(N)$$

since $N \mid C$ and $p \nmid N$.

If f is invariant under M_1^{-1}, the rationality of its q-expansion implies that

$$f \circ mM^{-1} = f \circ M_1^{-1} \circ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = f,$$

so that

$$f(\alpha)^{\sigma(\mathfrak{p})} = f(M\alpha) = f\left(\frac{u\alpha + vC}{-vA\alpha + u - vB}\right) = f\left(\frac{\overline{\pi}\alpha}{\overline{\pi}}\right) = f(\alpha).$$

For $p \mid u'$, we decompose in a similar manner

$$M = M_2 \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = M_2 S \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} S \text{ with } M_2 = \begin{pmatrix} u & v\frac{C}{p} \\ -vA & \frac{u'}{p} \end{pmatrix} \in \Gamma^0(N),$$

and the rationality of the q-expansion of $f \circ S$ allows to conclude if f is invariant under M_2^{-1}.

So we need the transformation of f under

$$M_1^{-1} = \begin{pmatrix} u' & -v\frac{C}{p} \\ vA & \frac{u}{p} \end{pmatrix}.$$

Rewriting (3.1), it is given by $f \circ M_1^{-1} = \zeta_{24}^{e\theta} f$ with

$$\begin{aligned}\theta =&(N-1)v\left(u'\frac{C}{Np} + A\left(\frac{u}{p}(1-u'^2) - u'\right)\right)\\ &+ 3v_1A_1(N_1-1)(u'-1) + \frac{3\lambda(N)(u'^2-1)}{2}.\end{aligned} \tag{5.2}$$

We obtain invariance provided $e\theta \equiv 0 \bmod 24$. (The treatment of M_2^{-1} is completely analogous and omitted.) In the following, we classify the values of D and B for which θ is 0 modulo some divisor of 24. It is natural to study separately $\theta \bmod 3$ and $\theta \bmod 2^\xi$ for $1 \leqslant \xi \leqslant 3$ depending on the value of N. We will give code names to the following propositions for future use.

5.1 The value of θ modulo 3

To be able to use some exponent e not divisible by 3, we need to impose $3 \mid \theta$. From the reduction of (5.2) modulo 3, namely

$$\theta = (N-1)v\left(u'\frac{C}{Np} + A\left(\frac{u}{p}(1-u'^2) - u'\right)\right) \bmod 3,$$

we immediately see that $3 \mid \theta$ for $N \equiv 1 \bmod 3$ without any further condition, which is coherent with $3 \nmid s$ in this case.

For $N \not\equiv 1 \pmod 3$, we impose $B^2 \equiv D \pmod{4N}$ to obtain divisibility of C by N (see the discussion above), and define $r \in \{0,1,2\}$ such that

$$A\frac{C}{N} = \frac{B^2 - D}{4N} \equiv r \pmod 3. \tag{5.3}$$

Notice that $r = 1$ implies $A \equiv \frac{C}{N} \pmod 3$, while $r = 2$ implies $A \equiv -\frac{C}{N} \pmod 3$.

5.1.1 The case $N \equiv 0 \bmod 3$

Proposition 5.1 (PROP30)**.** *Let $N \equiv 0 \pmod 3$, $B^2 \equiv D \pmod{4N}$ and r as in* (5.3)*. Then $3 \mid \theta$ if*

(a) $3 \mid D$ *and* $r = 1$*;*

(b) $D \equiv 1 \pmod 3$ *and* $r = 2$*.*

In these cases, B satisfies the following congruences modulo 3*:*

(a) $3 \mid B$*;*

(b) $3 \nmid B$*.*

Proof. Since $3 \mid N \mid C$ and $3 \nmid p$, $u^2 \equiv u'^2 \equiv 1 \pmod 3$ by (5.1) and

$$\theta \equiv \pm v\left(\frac{C}{Np} - A\right) \bmod 3.$$

(a) If $3 \mid B$, or equivalently $3 \mid D$, then $p \equiv u^2 \equiv 1 \pmod 3$ in (5.1). The desired result follows from (5.3).

(b) If $3 \nmid B$, which is equivalent with $D \equiv 1 \pmod 3$, only the case $3 \nmid v$ needs to be examined. Then $u \not\equiv u' \pmod 3$ and $p \equiv 2 \pmod 3$, and again (5.3) allows to conclude.

□

5.1.2 The case $N \equiv 2 \bmod 3$

Proposition 5.2 (PROP32)**.** *Let* $N \equiv 2 \pmod 3$, $B^2 \equiv D \pmod{4N}$ *and* $r \in \{1, 2\}$ *as in* (5.3)*. If* $D \equiv r \pmod 3$*, then* $3 \mid \theta$ *and* $3 \mid B$*.*

Proof. Notice that $D \equiv r \pmod 3$ is equivalent with $3 \mid B$ by (5.3). Then $u' \equiv u \pmod 3$ and

$$\theta \equiv uv \left(\frac{C}{Np} + \frac{A}{p}(1 - u^2) - A \right) \pmod 3.$$

If 3 divides u or v, we are done.

Otherwise, $u^2 \equiv v^2 \equiv 1 \pmod 3$, which implies

$$\theta \equiv \pm \left(\frac{C}{Np} - A \right) \pmod 3.$$

Writing $p \equiv 1 + AC \equiv 1 - r \pmod 3$, we see that this case is possible only for $r = 2$ and $p \equiv 2 \pmod 3$, and then $A \equiv -\frac{C}{N} \pmod 3$ and $3 \mid \frac{C}{Np} - A$. □

Note that the proposition does not hold for $r = 0$, since then $3 \mid D$, $3 \mid B$, $3 \mid AC$, and exactly one of A and C is divisible by 3 (if both were, then $[A, B, C]$ would not be primitive), causing $\theta \not\equiv 0 \bmod 3$ unless one of u or v is divisible by 3.

5.2 The value of θ modulo powers of 2

5.2.1 The case N odd

Since $N_1 = N$ and $\lambda(N) = 0$, (5.2) becomes

$$\theta \equiv (N - 1)\rho \pmod 8$$

for

$$\rho = v \left(u' \frac{C}{Np} + A \left(\frac{u}{p}(1 - u'^2) - u' \right) \right) + 3v_1 A_1 (u' - 1).$$

So θ is divisible by 8 if $N \equiv 1 \pmod 8$, which is the case in particular if N is a square. Otherwise, e is supposed to be even, so $e\theta$ is divisible by 4; if $N \equiv 1 \pmod 4$, $e\theta$ is even divisible by 8. So the only remaining case of interest is $N \equiv 3 \pmod 4$; then for $e \equiv 2 \pmod 4$, $8 \mid e\theta$ is equivalent with ρ even. We have

$$\rho \equiv v\big(u'C + A(u(1 + u') + u')\big) + u' + 1 \bmod 2.$$

Proposition 5.3 (PROP21)**.** *Let N be odd. If D is odd, then $\theta \equiv (N-1)\rho \pmod 8$ with ρ even.*

Proof. Since B is odd, $u' \equiv u + v \pmod 2$.

If one of v, A and C is even, then u and u' are odd by (5.1) (so that in fact v is even), and ρ is even.

Otherwise, v, A and C are odd, $u' = u + 1 \pmod 2$ and ρ is even as well. □

5.2.2 The case N even

Let $N = 2^{\lambda(N)} N_1$ with N_1 odd and $\lambda(N) \geqslant 1$. We study divisibility of θ by 2^ξ for increasing values of ξ. The value $\xi = 3$ is of interest only when e is odd, in which case N and thus N_1 are squares. We start with an elementary remark.

Lemma 5.4. *If $2 \mid N \mid C$, then*

(a) u and u' are odd and

$$\theta \equiv (N-1)vu'\left(\frac{C}{Np} - A\right) \pmod 4; \tag{5.4}$$

(b) moreover, if $4 \mid C$, then $2 \mid vB$.

Proof. (a) u and u' are odd by (5.1), so that $u'^2 \equiv 1 \pmod 8$. Since N_1 is odd, almost all terms disappear from (5.2).

(b) We have $p = u^2 + v(-uB + vAC) \equiv u(u - vB) \bmod 4$. Since u is odd by (a), we deduce that vB must be even.

□

As discussed above, $N \mid C$ is equivalent with $B^2 \equiv D \pmod{4N}$. Then $A\frac{C}{N} = \frac{B^2-D}{4N}$; by gradually imposing more restrictions modulo powers of 2 times $4N$, we fix $A\frac{C}{N}$ modulo powers of 2.

Proposition 5.5 (PROP20)**.** *When N is even, θ is even in the following cases:*

(a) $B^2 \equiv D + 4N \pmod{8N}$;

(b) $B^2 \equiv D \pmod{8N}$ and $D \equiv 1 \pmod 8$.

Proof. (a) The conditions imply that $A(C/N)$ is odd, and Lemma 5.4(a) allows to conclude since p is odd.

(b) In that case $A(C/N)$ is even. Since A is prime to N, it is odd and therefore C/N is even, which implies in turn $4 \mid C$. By Lemma 5.4(b), we get $2 \mid vB$. Since D is odd, B is odd and v is even, and (5.4) finishes the proof.

□

Divisibility of θ by 4

We begin with a purely arithmetical lemma that will give us necessary conditions on the parameters for the equation $B^2 \equiv D + r(4N) \bmod (16N)$ to have a solution.

Lemma 5.6. *Let $r \in \{0, 1, 2, 3\}$ and N be even. Given D, suppose the equation $B^2 \equiv D + 4rN \pmod{16N}$ admits a solution in B. Then either $D \equiv 1 \bmod 8$ which implies B is odd, or D is even and D satisfies one of the conditions of the following table depending on $rN \bmod 8$, which in turn gives properties of B.*

$rN \bmod 8$	*condition on D*	$\Rightarrow D/4 \bmod 8$	$B/2$
0	$4 \bmod 32$	1	*odd*
	$16 \mid D$	0	*even*
2	$24 \bmod 32$	6	$0 \bmod 4$
	$28 \bmod 32$	7	*odd*
	$8 \bmod 32$	2	$2 \bmod 4$
4	$16 \mid D$	0	*even*
	$20 \bmod 32$	5	*odd*
6	$8 \mid\mid D$	0	$0 \bmod 4$
	$12 \bmod 32$	3	*odd*

Proof. Since $B^2 \equiv D \bmod 8$, the only possible value for odd D is $D \equiv 1 \bmod 8$, giving B odd. If D is even, then

$$\left(\frac{B}{2}\right)^2 \equiv \frac{D}{4} + rN \bmod 8$$

and since N is even, the above table makes sense.

Remembering that the only squares modulo 8 are $\{0, 1, 4\}$, the table is easily constructed and left as an exercise to the reader. $\square$

Now, we are ready to extend the result of Proposition 5.5 by considering $B^2 \equiv D + r(4N) \pmod{16N}$ with $r \in \{1, 3\}$, which yields $A\frac{C}{N} \equiv r \pmod 4$. Note that case (b) cannot be extended and we leave the proof of this to the reader.

Proposition 5.7 (PROP44)**.** *Let N be even, and suppose $B^2 \equiv D + 4N \pmod{16N}$ has a solution. Then θ is divisible by 4 if one of the following conditions is met:*

(a) $D \equiv 1 \pmod 8$*;*

(b) $16 \mid D$*;*

(c) $2 \mid\mid N$ *and* $4 \mid\mid D$*.*

Proof. If D is odd, the condition follows from Lemma 5.6. Then $u' = u - vB$ leads to $2 \mid v$ and $4 \mid \theta$.

Assuming D even, Theorem 4.2 implies that $\chi_4(p) = 1$ (or, equivalently, $p \equiv 1 \pmod 4$) when $D/4 \bmod 8 \in \{3, 4, 7, 0\}$, which immediately settles case (b). When $D/4$ is odd, we see that we cannot have the case $4 \mid N$ when comparing with the table of Lemma 5.6, and this gives us (c).

In the other cases, when $p \equiv 3 \bmod 4$, we get v odd since $AC \equiv 2 \bmod 4$ and there is no reason to have $\theta \equiv 0 \bmod 4$. □

Proposition 5.8 (PROP412)**.** *Let N be even, and suppose $B^2 \equiv D + 12N \pmod{16N}$. Then θ is divisible by 4 if one of the following conditions is met:*

(a) $D \equiv 1 \pmod 8$*;*

(b) $8 \,||\, D$ *and* $2 \,||\, N$*;*

(c) $4 \,||\, D$ *and* $4 \mid N$*.*

In the cases of D even, B satisfies the following congruences modulo 4:

(b) $4 \mid B$*;*

(c) $2 \,||\, B$*.*

Proof. The proof for D odd as well as the case distinctions for D even are the same as in Proposition 5.7. However, we now have $A\frac{C}{N} \equiv -1 \pmod 4$.

In the cases where $\chi_4(p) = 1$ (i.e., $D/4 \in \{3, 4, 7, 0\}$), we get $p \equiv 1 \pmod 4$ and $\frac{C}{Np} - A \equiv 2 \pmod 4$. Since there is no compelling reason why v should be even, θ may or may not be divisible by 4.

So we have to turn our attention to the four other cases, i.e., $D/4 \in \{1, 2, 5, 6\}$, with Lemma 5.6 in mind. If $4 \mid B$, $8 \,||\, D$ and $2 \,||\, N$, then $2 \,||\, C$, and either v is even or $p \equiv 3 \pmod 4$. In both cases, Lemma 5.4 shows that $4 \mid \theta$. If $2 \,||\, B$ and $4 \,||\, D$, suppose that furthermore $4 \mid N$. Then $4 \mid AC$, and again v is even or $p \equiv 3 \pmod 4$. □

Divisibility of θ by 8

As discussed at the beginning of §5.2.1, for generating class fields we are only interested in $\theta \bmod 8$ when N is a square, that is, $\lambda(N)$ is even and N_1 is a square; in particular, $N_1 \equiv 1 \pmod 8$. Then the following generalisation of Lemma 5.4 is immediately seen to hold:

Lemma 5.9. *If N is an even square dividing C, then*

$$\theta \equiv (N-1)vu' \left(\frac{C}{Np} - A \right) \pmod 8.$$

From the results obtained for $B^2 \equiv D + 4rN \pmod{16N}$ for $r \in \{1, 3\}$, it is natural to look at $B^2 \equiv D + 4rN \pmod{32N}$ for $r \in \{1, 3, 5, 7\}$. Then $A\frac{C}{N} \equiv r \pmod 8$.

Proposition 5.10 (PROP8)**.** *Let N be an even square, and suppose $B^2 \equiv D + 4rN \pmod{32N}$. Then θ is divisible by 8 if one of the following conditions holds:*

(a) $r = 3$ or $r = 7$, and $D \equiv 1 \pmod 8$;

(b) $r = 1$, and $32 \mid D$;

(c) $r = 5$, and $16 \mid\mid D$.

In the cases of D even, B satisfies the following congruences modulo 8:

(b1) $4 \mid\mid B$ if $4 \mid\mid N$;

(b2) $8 \mid B$ if $16 \mid N$.

(c1) $4 \mid\mid B$ if $16 \mid N$;

(c2) $8 \mid B$ if $4 \mid\mid N$.

Proof. Since $4 \mid N \mid C$, we have $p \equiv u(u - vB) \pmod 4$ by (5.1).

For D odd, B is odd and v is even as seen in Proposition 5.7. If v is divisible by 4, then θ is divisible by 8 by Lemma 5.9. If $2 \mid\mid v$, then $p \equiv 3 \pmod 4$; if furthermore $r \equiv 3 \pmod 4$, then $4 \mid \frac{C}{Np} - A$, and $8 \mid \theta$ by Lemma 5.9.

In the remaining cases of the proposition, $16 \mid D$, $4 \mid B$, $r \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 4$. If v is even, Lemma 5.9 implies that $8 \mid \theta$. From now on, we assume that v is odd. Then $p = u^2 - uvB + AC \pmod 8$, and we need to verify that $8 \mid \frac{C}{Np} - A$.

The results now follow from close inspection of

$$AC \equiv rN \pmod 8 \text{ and } \left(\frac{B}{4}\right)^2 \equiv \frac{D}{16} + r\frac{N}{4} \pmod 8.$$

Consider first the case $r = 1$ and $32 \mid D$. By Theorem 4.2, we have $\chi_4(p) = \chi_8(p) = 1$, which yields $p \equiv 1 \bmod 8$ and implies the desired divisibility of $\frac{C}{Np} - A$ by 8.

Consider now $r = 5$; it is sufficient to show that $p \equiv 5 \pmod 8$. If $16 \mid\mid D$ and $16 \mid N \mid C$, then $B \equiv 4 \pmod 8$ and $p \equiv 5 \pmod 8$. If $16 \mid\mid D$ and $4 \mid\mid N$, then $AC \equiv 4 \pmod 8$ and $32 \mid D + 4rN$, whence $8 \mid B$ and $p \equiv 5 \pmod 8$. $\square$

6 Lower powers of $\mathfrak{w}_N$

The aim of this section is to determine conditions under which singular values of lower powers of $\mathfrak{w}_N$ than those given in Theorem 4.3 yield class invariants. When N is not a square, only even powers are possible by Theorems 3.2 and 2.3. So we specialise the propositions of §5 according to the value of $N \pmod{12}$. When N is a square, odd powers may yield class invariants, and we need to distinguish more finely modulo 24. Note that then $N \in \{0, 1, 4, 9, 12, 16\} \pmod{24}$.

Throughout this section, we use the notation of Theorem 4.3. The number α is a root of the quadratic form $[A, B, C]$ of discriminant D and N is an integer such that A is prime to N and B is a square root of D modulo $4N$ according to Lemma 4.1, so that $N \mid C$. The canonical power s such that $\mathfrak{w}_N^s(\alpha)$ is a class invariant, that is, $\mathfrak{w}_N^s(\alpha) \in K_D$, is defined as in Theorem 4.3, and we wish to determine the minimal exponent e such that $\mathfrak{w}_N^e(\alpha)$ is still a class invariant. The general procedure is as follows: Given the value of N, we assemble the propositions of §5 (using their code names throughout) and deduce from them conditions on B as well as the period of D for which class invariants are obtained. In general, we can combine a condition on B related to θ mod 3 and another one related to θ mod 2^ξ. The Chinese remainder theorem is then used to find compatible values. When no particular condition modulo 3 or powers of 2 is imposed, that is, e and s have the same 3-adic or 2-adic valuation, then Theorem 4.3 already leads to the desired conclusion.

Once a power $\mathfrak{w}_N^e(\alpha)$ is identified as a class invariant, its conjugates may be obtained by an M-system for $M = \frac{s}{e}N$ containing $[A, B, C]$ as shown through Theorems 2.4 and 3.2. In more detail, one may proceed as follows:

1. Determine a form $[A, B, C]$ with root α satisfying $\gcd(A, M) = 1$ and the constraint on B so that $\mathfrak{w}_N^e(\alpha)$ is a class invariant; in general, one may choose $A = 1$.

2. Enumerate all reduced forms $[a_i, b_i, c_i]$, $i = 1, \ldots, h(D)$ of discriminant D, numbered in such a way that $[a_1, b_1, c_1] \equiv [A, B, C]$.

3. Let $[A_1, B_1, C_1] = [A, B, C]$. For $i \geqslant 2$, find a form $[A_i, B_i, C_i] \equiv [a_i, b_i, c_i]$ such that $\gcd(A_i, M) = 1$ and $B_i \equiv B \pmod{2M}$, using, for instance, the algorithm of [22, Prop. 3], [24, Th. 3.1.10].

Then a floating point approximation of the class polynomial can be computed as

$$\prod_{i=1}^{h_D} \left(X - \mathfrak{w}_N^e(\alpha_i)\right)$$

with $\alpha_i = \frac{-B_i + \sqrt{D}}{2A_i}$. Using the algorithms of [11], one obtains a quasi-linear complexity in the total size of the class polynomial.

Note that the conditions on B of §5 can be summarised as $B^2 \equiv D+4rN \pmod{4RN}$, where r is defined modulo R and the only primes dividing R are 2 and 3. For the sake of brevity, we denote such a condition by $r{:}R$. So if no particular condition beyond $B^2 \equiv D \pmod{4N}$ is required, this is denoted by 0:1.

We will give more details for the first non-trivial cases and be briefer in the sequel, since the results rapidly become unweildy. We add numerical examples for these cases.

6.1 The case N odd

6.1.1 $N \not\equiv 0 \bmod 3$

This is the simplest case. We may use PROP32, PROP21 or both of them. Whenever $N \equiv 2 \pmod 3$ and $3 \nmid D$, then PROP32 applies; moreover, the resulting condition $3 \mid B$ is automatically satisfied, and we gain a factor of 3 in the exponent. Similarly if D is odd, then PROP21 applies without any restriction on B, and we gain a factor of 2 in the exponent.

N mod 12	s	B	D	e	proposition(s)
5	6	1:3	$D \equiv 1 \bmod 3$	2	PROP32
5	6	2:3	$D \equiv 2 \bmod 3$	2	PROP32
7	4	0:1	$2 \nmid D$	2	PROP21
11	12	0:1	$2 \nmid D$	6	PROP21
11	12	1:3	$D \equiv 1 \bmod 3$	4	PROP32
11	12	2:3	$D \equiv 2 \bmod 3$	4	PROP32
11	12	1:3	$D \equiv 1 \bmod 6$	2	PROP32+PROP21
11	12	2:3	$D \equiv 5 \bmod 6$	2	PROP32+PROP21

Letting $D = c^2\Delta$, we put $\omega = \sqrt{\Delta/4}$ if $4 \mid \Delta$ and $\omega = (1+\sqrt{\Delta})/2$ otherwise. Here are some numerical examples:

N	f	$-D$	$H_D[f]$
5	$\mathfrak{w}_5^2$	11	$X - \omega - 1$
5	$\mathfrak{w}_5^2$	4	$X - 1 - 2\,\omega$
7	$\mathfrak{w}_7^2$	3	$X - 3\,\omega + 1$
11	$\mathfrak{w}_{11}^6$	39	$X^4 + (27\,\omega - 73)\,X^3 + (1656\,\omega - 8914)\,X^2$
			$+\,(7947\,\omega - 139058)\,X - 515016\,\omega + 1000693$
11	$\mathfrak{w}_{11}^4$	8	$X + 7 + 6\,\omega$
11	$\mathfrak{w}_{11}^4$	28	$X + 8\,\omega - 7$
11	$\mathfrak{w}_{11}^2$	11	$X - 2\,\omega + 1$
11	$\mathfrak{w}_{11}^2$	7	$X - 2\,\omega + 3$

6.1.2 The case $N \equiv 3 \pmod{12}$

The situation becomes more intricate when $\gcd(N, 6) \neq 1$. For $N \equiv 3 \pmod{12}$, we have $s = 12$, and N cannot be a square. Therefore we need an even exponent e. Since already the full power $\mathfrak{w}_N^{12}$ can only be used when D is a square modulo $4N$, we only have to consider $D \in \{0, 1, 4, 9\}$ (mod 12). Then PROP30 applies; moreover, PROP21 applies whenever D is odd, resulting in the following table.

N mod 12	s	B	D mod 12	e	propositions(s)
3	12	0:1	$1, 9$	6	PROP21
3	12	1:3	$0, 9$	4	PROP30(a)
3	12	2:3	$1, 4$	4	PROP30(b)
3	12	1:3	9	2	PROP30(a)+PROP21
3	12	2:3	1	2	PROP30(b)+PROP21

The entries in the first and last line for $D \equiv 1 \pmod{12}$ may seem redundant; but note that they induce differently severe restrictions on B. The entry $D \equiv 1 \pmod{12}$ in the third line, as well as $D \equiv 9 \pmod{12}$ in the second line, are redundant, however: Since PROP21 does not induce any additional restriction on B, the lower exponent is available for precisely the same quadratic forms. In the following, we will present only tables that have been reduced accordingly.

However, the previous table does not yet contain the full truth. A line in the table means that if there is a solution to $B^2 \equiv D + 4rN \pmod{4RN}$ with D in the given residue class D_0 modulo 12, then $\mathfrak{w}_N^e$ yields a class invariant. Examining this equation modulo the part of $4RN$ that contains only 2 and 3 yields further restrictions. Write $N = N_6 N'$ such that the only primes dividing N_6 are 2 and 3 and $\gcd(N', 6) = 1$. Then we need to ensure that $D + 4rN \equiv D$ is a square modulo N'; this is guaranteed by Lemma 4.1, since otherwise we would not even consider the full power $\mathfrak{w}_N^s$. We furthermore need to examine under which conditions

$$D + 4N_6 rN' \text{ is a square modulo } 4RN_6 \text{ and } D \equiv D_0 \pmod{12}.$$

Concerning the second to last line, for instance, the condition becomes

$$D + 12\frac{N}{3} \text{ is a square modulo 36 and } D \equiv 9 \pmod{12}.$$

Thus, $D + 12\frac{N}{3} \equiv 9 \pmod{36}$, and depending on $\frac{N}{3}$ mod 3, only one value of $D \pmod{36}$ remains.

For $N = 3$, for instance, or more generally $\frac{N}{3} \equiv 1 \pmod 3$, we obtain the following class invariants.

B	D mod 36	e
0:1	$0, 12$	12
0:1	$9, 21$	6
1:3	24	4
2:3	$4, 16, 28$	4
1:3	33	2
2:3	$1, 13, 25$	2

To illustrate this, we give the following table of examples:

N	f	$-D$	$H_D[f]$
3	$\mathfrak{w}_3^{12}$	24	$X^2 - 162\,X + 729$
3	$\mathfrak{w}_3^{6}$	15	$X^2 - 3\,(2\,\omega - 1)\,X - 27$
3	$\mathfrak{w}_3^{4}$	12	$X - 3$
3	$\mathfrak{w}_3^{4}$	8	$X - 1 - 2\,\omega$
3	$\mathfrak{w}_3^{2}$	3	$X - \omega - 1$
3	$\mathfrak{w}_3^{2}$	11	$X - \omega$

6.1.3 The case $N \equiv 9 \bmod 12$

We have $s = 3$ for squares in that family (for instance, $N = 3^{2n}$) and may then reach $\mathfrak{w}_N$. Otherwise, $s = 6$, and the only possible smaller exponent is 2.

N	s	B	D	e	propositions(s)
9 mod 12, $\neq \square$	6	1:3	0 mod 3	2	PROP30a
9 mod 12, $\neq \square$	6	2:3	1 mod 3	2	PROP30b
9 mod 12, $= \square$	3	1:3	0 mod 3	1	PROP30a
9 mod 12, $= \square$	3	2:3	1 mod 3	1	PROP30b

We give two examples, one for $N = 21$, the second for $N = 9$. For the former, we find

B	D mod 252	e
0:1	0, 9, 21, 36, 57, 72, 81, 84, 93, 120, 144, 156, 165, 189, 225, 228	6
1:3	60, 105, 141, 168, 177, 204, 240, 249	2
2:3	1, 4, 16, 25, 28, 37, 49, 64, 85, 88, 100, 109, 112, 121, 133, 148, 169, 172, 184, 193, 196, 205, 217, 232	2

N	f	$-D$	$H_D[f]$
21	$\mathfrak{w}_{21}^{6}$	24	$X^2 + (108 + 102\,\omega)\,X - 6345 + 2754\,\omega$
21	$\mathfrak{w}_{21}^{2}$	3	$X + \omega + 4$
21	$\mathfrak{w}_{21}^{2}$	20	$X^2 + (-2 + 4\,\omega)\,X - 19 - 4\,\omega$

For $N = 9$, we get:

B	D mod 108	e
0:1	9, 36	3
1:3	0, 45, 72, 81	1
2:3	1, 4, 13, 16, 25, 28, 37, 40, 49, 52, 61, 64, 73, 76, 85, 88, 97, 100	1

N	f	$-D$	$H_D[f]$
9	$\mathfrak{w}_9^{3}$	72	$X^2 - 18\,X + 27$
9	$\mathfrak{w}_9$	27	$X - \omega - 1$
9	$\mathfrak{w}_9$	8	$X - 1 - \omega$

6.2 The case N even

A look at §5 immediately shows the complexity of the results when N is even. We distinguish the cases $\lambda = 1$ (in which N cannot be a square) and $\lambda \geqslant 2$ with N a square or not.

6.2.1 The case $\lambda = 1$

Three values are concerned, namely $N \bmod 12 \in \{2, 6, 10\}$. We have $s = 24$ for $N \bmod 12 \in \{2, 6\}$, whereas $s = 8$ for $N \equiv 10 \pmod{12}$.

N mod 12	s	B	D	e	proposition(s)
2	24	1:2	—	12	PROP20a
2	24	0:2	1 mod 8	12	PROP20b
2	24	1:3	1 mod 3	8	PROP32
2	24	2:3	2 mod 3	8	PROP32
2	24	1:4	1, 4 mod 8; 0 mod 16	6	PROP44
2	24	3:4	1 mod 8; 8 mod 16	6	PROP412ab
2	24	1:2∩1:3	1 mod 3	4	PROP20a+PROP32
2	24	1:2∩2:3	2 mod 3	4	PROP20a+PROP32
2	24	0:2∩1:3	1 mod 24	4	PROP20b+PROP32
2	24	0:2∩2:3	17 mod 24	4	PROP20b+PROP32
2	24	1:4∩1:3	1, 4 mod 24; 16 mod 48	2	PROP44+PROP32
2	24	1:4∩2:3	17, 20 mod 24; 32 mod 48	2	PROP44+PROP32
2	24	3:4∩1:3	1 mod 24; 40 mod 48	2	PROP412ab+PROP32
2	24	3:4∩2:3	17 mod 24; 8 mod 48	2	PROP412ab+PROP32
6	24	1:2	—	12	PROP20a
6	24	0:2	1 mod 8	12	PROP20b
6	24	1:3	0 mod 3	8	PROP30a
6	24	2:3	1 mod 3	8	PROP30b
6	24	1:4	1, 4 mod 8; 0 mod 16	6	PROP44
6	24	3:4	1 mod 8; 8 mod 16	6	PROP412ab
6	24	1:2∩1:3	0 mod 3	4	PROP20a+PROP30a
6	24	1:2∩2:3	1 mod 3	4	PROP20a+PROP30b
6	24	0:2∩1:3	9 mod 24	4	PROP20b+PROP30a
6	24	0:2∩2:3	1 mod 24	4	PROP20b+PROP30b
6	24	1:4∩1:3	9, 12 mod 24; 0 mod 48	2	PROP44+PROP30a
6	24	1:4∩2:3	1, 4 mod 24; 16 mod 48	2	PROP44+PROP30b
6	24	3:4∩1:3	9 mod 24; 24 mod 48	2	PROP412ab+PROP30a
6	24	3:4∩2:3	1 mod 24; 40 mod 48	2	PROP412ab+PROP30b
10	8	1:2	—	4	PROP20a
10	8	0:2	1 mod 8	4	PROP20b
10	8	1:4	1, 4 mod 8; 0 mod 16	2	PROP44
10	8	3:4	1 mod 8; 8 mod 16	2	PROP412ab

The case $N = 2$ corresponds to Weber's classical functions. We present the case $N = 6$ in more detail, illustrating the complexity of the process.

B	D mod 288	e
0:1	0, 36, 96, 132, 144, 180, 240, 276	24
1:2	60, 252	12
1:3	48, 84, 192, 228	8
2:3	4, 16, 52, 64, 100, 112, 148, 160, 196, 208, 244, 256	8
3:4	24, 72, 168, 216	6
1:4	9, 33, 81, 105, 153, 177, 225, 249	6
1:4	108, 204	6
1:2 $\cap$ 1:3	156	4
1:2 $\cap$ 2:3	28, 124, 220	4
3:4 $\cap$ 1:3	120, 264	2
1:4 $\cap$ 1:3	57, 129, 201, 273	2
1:4 $\cap$ 1:3	12	2
3:4 $\cap$ 2:3	40, 88, 136, 184, 232, 280	2
1:4 $\cap$ 2:3	1, 25, 49, 73, 97, 121, 145, 169, 193, 217, 241, 265	2
1:4 $\cap$ 2:3	76, 172, 268	2

N	f	$-D$	$H_D[f]$
6	$\mathfrak{w}_6^{24}$	12	$X + 186624$
6	$\mathfrak{w}_6^{12}$	36	$X^2 - 3888\,\omega\,X + 1259712$
6	$\mathfrak{w}_6^{8}$	60	$X^2 + (432\,\omega - 720)\,X + 20736$
6	$\mathfrak{w}_6^{8}$	32	$X^2 + (112 + 64\,\omega)\,X - 1088 - 3584\,\omega$
6	$\mathfrak{w}_6^{6}$	72	$X^2 - 216\,X - 5832$
6	$\mathfrak{w}_6^{6}$	39	$X^4 + (3\,\omega - 42)\,X^3 + (486\,\omega + 108)\,X^2$
			$+ (-648\,\omega + 9072)\,X + 6561\,\omega - 45198$
6	$\mathfrak{w}_6^{6}$	84	$X^4 + (324 + 60\,\omega)\,X^3 + 14688\,X^2$
			$+ (69984 - 12960\,\omega)\,X + 46656$
6	$\mathfrak{w}_6^{4}$	132	$X^4 + (144 - 12\,\omega)\,X^3 + 2196\,X^2$
			$+ (5184 + 432\,\omega)\,X + 1296$
6	$\mathfrak{w}_6^{4}$	68	$X^4 + (-32 + 4\,\omega)\,X^3 + (-204 - 96\,\omega)\,X^2$
			$+ (1152 - 144\,\omega)\,X - 752 + 256\,\omega$
6	$\mathfrak{w}_6^{2}$	24	$X^2 - \omega\,X - 6$
6	$\mathfrak{w}_6^{2}$	15	$X^2 + (-2\,\omega - 2)\,X + 3\,\omega - 3$
6	$\mathfrak{w}_6^{2}$	276	$X^8 + (-12 - 4\,\omega)\,X^7 + (132 + 6\,\omega)\,X^6$
			$-144\,X^5 - 576\,X^4 - 864\,X^3 + (4752 - 216\,\omega)\,X^2$
			$+ (-2592 + 864\,\omega)\,X + 1296$
6	$\mathfrak{w}_6^{2}$	8	$X + 2 + \omega$
6	$\mathfrak{w}_6^{2}$	23	$X^3 - 6\,X^2 + (-\omega + 15)\,X + \omega - 15$
6	$\mathfrak{w}_6^{2}$	20	$X^2 + (2 - 2\,\omega)\,X - 4 - 2\,\omega$

6.2.2 The case $\lambda \geqslant 2$

We have to study three values of N mod 12, namely, 0, 4 and 8, for which $s = 24$, 8, and 24, respectively. The cases $N \equiv 0$ or 4 authorise squares, so that the results become somewhat lengthy.

When $N \equiv 4 \bmod 12$, we find

N	s	B	D	e	proposition(s)
4 mod 12	8	1:2	—	4	PROP20a
4 mod 12	8	1:2	1 mod 8	4	PROP20b
4 mod 12	8	1:4	1 mod 8	2	PROP44a
4 mod 12	8	1:4	0 mod 16	2	PROP44b
4 mod 12	8	3:4	1 mod 8	2	PROP412a
4 mod 12	8	3:4	4 mod 8	2	PROP412c
4 mod 12, $= \square$	8	3:8	1 mod 8	1	PROP8a
4 mod 12, $= \square$	8	7:8	1 mod 8	1	PROP8a
4 mod 12, $= \square$	8	1:8	0 mod 32	1	PROP8b
4 mod 12, $= \square$	8	5:8	16 mod 32	1	PROP8c

When $N \equiv 8 \bmod 12$, it cannot be a square, and the results are:

N mod 12	s	B	D	e	proposition(s)
8	24	1:2	—	12	PROP20a
8	24	1:2	1 mod 8	12	PROP20b
8	24	1:4	1 mod 8	6	PROP44a
8	24	1:4	0 mod 16	6	PROP44b
8	24	3:4	1 mod 8	6	PROP412a
8	24	3:4	4 mod 8	6	PROP412c
8	24	1:3	1 mod 3	8	PROP32
8	24	2:3	2 mod 3	8	PROP32
8	24	$1{:}2 \cap 1{:}3$	1 mod 3	4	PROP20a+PROP32
8	24	$1{:}2 \cap 2{:}3$	2 mod 3	4	PROP20a+PROP32
8	24	$1{:}2 \cap 1{:}3$	1 mod 24	4	PROP20b+PROP32
8	24	$1{:}2 \cap 2{:}3$	17 mod 24	4	PROP20b+PROP32
8	24	$1{:}4 \cap 1{:}3$	1 mod 24	2	PROP44a+PROP32
8	24	$1{:}4 \cap 2{:}3$	17 mod 24	2	PROP44a+PROP32
8	24	$1{:}4 \cap 1{:}3$	16 mod 48	2	PROP44b+PROP32
8	24	$1{:}4 \cap 2{:}3$	32 mod 48	2	PROP44b+PROP32
8	24	$3{:}4 \cap 1{:}3$	1 mod 24	2	PROP412a+PROP32
8	24	$3{:}4 \cap 2{:}3$	17 mod 24	2	PROP412a+PROP32
8	24	$3{:}4 \cap 1{:}3$	4 mod 24	2	PROP412c+PROP32
8	24	$3{:}4 \cap 2{:}3$	20 mod 24	2	PROP412c+PROP32

Finally, for $N \equiv 0 \bmod 12$, we obtain the following results:

N	s	B	D	e	proposition(s)
12	24	1:2	—	12	PROP20a
12	24	1:2	1 mod 8	12	PROP20b
12	24	1:4	1 mod 8	6	PROP44a
12	24	1:4	0 mod 16	6	PROP44b
12	24	3:4	1 mod 8	6	PROP412a
12	24	3:4	4 mod 8	6	PROP412c
12	24	1:3	0 mod 3	8	PROP30a
12	24	2:3	1 mod 3	8	PROP30b
12	24	1:2 $\cap$ 1:3	0 mod 3	4	PROP20a+PROP30a
12	24	1:2 $\cap$ 2:3	1 mod 3	4	PROP20a+PROP30b
12	24	1:2 $\cap$ 1:3	9 mod 24	4	PROP20b+PROP30a
12	24	1:2 $\cap$ 2:3	1 mod 24	4	PROP20b+PROP30b
12	24	1:4 $\cap$ 1:3	9 mod 24	2	PROP44a+PROP30a
12	24	1:4 $\cap$ 2:3	1 mod 24	2	PROP44a+PROP30b
12	24	1:4 $\cap$ 1:3	0 mod 48	2	PROP44b+PROP30a
12	24	1:4 $\cap$ 2:3	16 mod 48	2	PROP44b+PROP30b
12	24	3:4 $\cap$ 1:3	9 mod 24	2	PROP412a+PROP30a
12	24	3:4 $\cap$ 2:3	1 mod 24	2	PROP412a+PROP30b
12	24	3:4 $\cap$ 1:3	12 mod 24	2	PROP412c+PROP30a
12	24	3:4 $\cap$ 2:3	4 mod 24	2	PROP412c+PROP30b
12	24	3:8	1 mod 8	3	PROP8a
12	24	7:8	1 mod 8	3	PROP8a
12	24	1:8	0 mod 32	3	PROP8b
12	24	5:8	16 mod 32	3	PROP8c
12	24	3:8 $\cap$ 1:3	9 mod 24	1	PROP8a+PROP30a
12	24	3:8 $\cap$ 2:3	1 mod 24	1	PROP8a+PROP30b
12	24	7:8 $\cap$ 1:3	9 mod 24	1	PROP8a+PROP30a
12	24	7:8 $\cap$ 2:3	1 mod 24	1	PROP8a+PROP30b
12	24	1:8 $\cap$ 1:3	0 mod 96	1	PROP8b+PROP30a
12	24	1:8 $\cap$ 2:3	64 mod 96	1	PROP8b+PROP30b
12	24	5:8 $\cap$ 1:3	48 mod 96	1	PROP8c+PROP30a
12	24	5:8 $\cap$ 2:3	16 mod 96	1	PROP8c+PROP30b

For $N = 4$, these results translate as follows:

B	D mod 128	e
0:1	$\equiv 4 \pmod{32}$	8
1:2	16, 32, 80, 96	4
3:4	$\equiv 20 \pmod{32}$	2
1:4	64	2
3:8	$\equiv 1 \pmod{8}$	1
1:8	0	1
5:8	$\equiv 48 \pmod{64}$	1

N	f	$-D$	$H_D[f]$
4	$\mathfrak{w}_4^8$	28	$X - 48\,\omega + 32$
4	$\mathfrak{w}_4^4$	32	$X^2 - 8\,\omega\,X - 16$
4	$\mathfrak{w}_4^2$	12	$X - 2\,\omega$
4	$\mathfrak{w}_4^2$	64	$X^2 + (-4 - 4\,\omega)\,X + 4\,\omega$
4	$\mathfrak{w}_4$	7	$X - \omega$
4	$\mathfrak{w}_4$	128	$X^4 + (-4 - 2\,\omega)\,X^3 + 6\,\omega\,X^2 + (8 - 4\,\omega)\,X - 4$
4	$\mathfrak{w}_4$	16	$X - 1 - \omega$

The precise results for $N = 16$ are the following:

B	D mod 512	e
0:1	$\equiv 16 \pmod{128}$	8
1:2	64, 128, 320, 384	4
3:4	$\equiv 4 \pmod{32}$	2
1:4	256	2
3:8	$\equiv 1 \pmod{8}$	1
1:8	0, 192, 448	1
5:8	$\equiv 80 \pmod{128}$	1

N	f	$-D$	$H_D[f]$
16	$\mathfrak{w}_{16}^8$	112	$X^2 + (12288\,\omega - 8192)\,X - 196608\,\omega - 917504$
16	$\mathfrak{w}_{16}^4$	128	$X^4 + (128 + 192\,\omega)\,X^3 + 6656\,\omega\,X^2$
			$+\,(-32768 + 49152\,\omega)\,X - 65536$
16	$\mathfrak{w}_{16}^2$	28	$X + 2\,\omega - 4$
16	$\mathfrak{w}_{16}^2$	256	$X^4 + (16 - 48\,\omega)\,X^3 + (-288 + 288\,\omega)\,X^2$
			$+\,(768 - 256\,\omega)\,X - 256\,\omega$
16	$\mathfrak{w}_{16}$	7	$X - \omega - 1$
16	$\mathfrak{w}_{16}$	64	$X^2 - 4\,X + 4$
16	$\mathfrak{w}_{16}$	48	$X^2 + 4\,X + 4$

6.3 Reality of class polynomials

The argumentation of the proof of Theorem 4.4 carries over to the lower powers of $\mathfrak{w}_N$ and shows that the class polynomial is real whenever for some form $[A, B, C]$ in the $\frac{s}{e}N$-system the inverse form $[A, -B, C]$ satisfies the congruence constraints of the system as well. This is precisely the case when B is divisible by $\frac{s}{e}N$. In particular, this implies that $N \mid D$, and inspection of the previous results proves the following theorem.

Theorem 6.1. *Under the general assumptions of § 6, the characteristic polynomial of $\mathfrak{w}_N^e(\alpha)$ is real whenever $N \mid D$ and $\frac{s}{e}N \mid B$. For $e < s$, this is possible only in the following cases:*

(a) N odd:

N	s	B	D	e
5 mod 12	6	1:3	1 mod 3	2
5 mod 12	6	2:3	2 mod 3	2
11 mod 12	12	1:3	1 mod 3	4
11 mod 12	12	2:3	2 mod 3	4
3 mod 12	12	1:3	6 mod 9	4
9 mod 12, $\neq \square$	6	1:3	18 mod 27	2
9 mod 12, $= \square$	3	1:3	18 mod 27	1

(b) $2 \mid\mid N$ *and* $4 \mid D$

(b1) $\frac{s}{e}$ *is even and* $8 \mid\mid D$

(b2) $\frac{s}{e} = 3$

(c) $4 \mid N$ *and* $16 \mid D$

Proof. We again start from $B^2 \equiv D + 4rN \pmod{4RN}$, where in fact $R = \frac{s}{e}$ is a non-trivial divisor of 24. Then the hypotheses of the theorem translate as $B = NRB'$ and $D = ND'$, so that

$$NR^2 B'^2 \equiv D' + 4r \pmod{4R}. \tag{6.1}$$

This immediately implies

$$D' \equiv -r \pmod 3 \qquad \text{if } 3 \mid R \tag{6.2}$$

$$4 \mid D' \qquad \text{if } 2 \mid R \tag{6.3}$$

(a) The assertions are a direct consequence of (6.2) and (6.3), together with the tables in §6.1.

(b) If N is even, from $N \mid D$ we immediately have $4 \mid D$.

If R is even, then moreover (6.3) yields that $8 \mid D$. Going through the table in §6.2.1 shows that then r is odd, and (6.1) implies that $D' \equiv -4r \equiv 4 \pmod 8$ and $8 \mid\mid D$.

(c) If $4 \mid N$, then (6.1) shows that $4 \mid D'$, whence $16 \mid D$.

$\square$

We end this section with related results concerning the functions $\sqrt{D}\,\mathfrak{w}_N^e$. Since $\sqrt{D} \in \mathcal{O}$, a singular value $\sqrt{D}\,\mathfrak{w}_N^e(\alpha)$ is a class invariant if and only if $\mathfrak{w}_N^e(\alpha)$ is, and integrality of the class polynomial coefficients carries over. In some cases, however, the additional factor $\sqrt{D}$ may lead to rational class polynomials.

Lemma 6.2. *Let $N \not\equiv 1 \pmod 8$, $\alpha = \frac{-B+\sqrt{D}}{2}$ and e be such that $\frac{s}{e}$ is even, $\frac{s}{2e}N \mid B$ and $\frac{s}{e}N \nmid B$. Then $\mathfrak{w}_N(\alpha)^e \in i\mathbb{R}$.*

Proof. Write $\mathfrak{w}_N = f_0 f_1$, where $f_0 = q^{-\frac{N-1}{24N}}$ and f_1 is a power series in $q^{1/N}$. Notice that if $N \mid B$, then $q^{1/N}(\alpha) = e^{2\pi i\alpha/N} \in \mathbb{R}$. So $\mathfrak{w}_N^e(\alpha)$ is real up to the factor $f_0(\alpha)^e$, which itself is real up to the factor $e^{\frac{2\pi i}{4} \cdot \frac{s(N-1)}{24} \cdot \frac{2eB}{sN}}$. This is an odd power of i under the hypotheses of the lemma; $N \not\equiv 1 \pmod 8$ is needed to ensure that $\frac{s(N-1)}{24}$ is odd. $\square$

Lemma 6.3. *Let f be a modular function and $\alpha \in \mathcal{O}$ such that $f(\alpha)$ is a class invariant and a real number. Then $H_D[f] \in \mathbb{Q}[X]$.*

Proof. This is a trivial application of Galois theory. The complex conjugate $\overline{f(\alpha)}$ is a root of $\overline{H_D[f]}$. Since $\overline{f(\alpha)} = f(\alpha)$, this implies that $\overline{H_D[f]}$ is a multiple of the minimal polynomial $H_D[f]$ of $f(\alpha)$, so both are the same, and $H_D[f]$ has coefficients in $K \cap \mathbb{R} = \mathbb{Q}$. $\square$

Combining the lemmata yields the following result.

Theorem 6.4. *Under the general assumptions of §6, the characteristic polynomial of $\sqrt{D}\,\mathfrak{w}_N^e(\alpha)$ is real whenever $N \not\equiv 1 \pmod 8$, $N \mid D$, $\frac{s}{e}$ is even, $\frac{s}{2e}N \mid B$ and $\frac{s}{e}N \nmid B$.*

For instance, we may apply this theorem to the cases $N \in \{2, 3, 4, 7\}$, in which Propositions 5.3 or 5.5 hold:

N	D	B	e
2	12 mod 16	± 2	12
	24 mod 96	± 12	6
3	9 mod 12	± 3	6
7	21 mod 28	± 7	2
4	0 mod 32	± 4	4

As numerical examples, we find:

$$H_{-72}[\sqrt{-72}\,\mathfrak{w}_2^6] = X^2 + 720X + 576,$$

$$H_{-51}[\mathfrak{w}_3^6](X) = X^2 + 6\sqrt{-51}X - 27,$$
$$H_{-51}[\sqrt{-51}\,\mathfrak{w}_3^6](X) = X^2 - 306X + 1377.$$

7 Heights and comparison with other invariants

Let f be a modular function yielding class invariants and $\Phi[f](F, J)$ the associated modular polynomial such that $\Phi[f](f, j) = 0$. It is shown in [7] that asymptotically for $|D| \to \infty$, the height of the class invariant $f(\alpha)$ is $c(f)$ times the height of $j(\alpha)$, where

$$c(f) = \frac{\deg_J(\Phi[f])}{\deg_F(\Phi[f])} \tag{7.1}$$

depends only on f. It is then clear that $c(f^r) = rc(f)$ for rational r. So to obtain $c(\mathfrak{w}_N^e)$, it is sufficient to determine the degrees of the modular polynomials of the full power $\mathfrak{w}_N^s$, where s is as defined in Theorem 4.3.

7.1 Modular polynomials for $\mathfrak{w}_N^s$

Since $\mathfrak{w}_N^s$ is modular for $\Gamma^0(N)$ by Theorem 3.2, we have

$$\Phi_N^{\mathrm{c}} := \Phi[\mathfrak{w}_N^s] = \prod_{M \in \Gamma^0(N) \backslash \Gamma} (F - \mathfrak{w}_N^s \circ M).$$

So $\deg_F \Phi_N^{\mathrm{c}} = \psi(N) = N \prod_{p \text{ prime}, \, p \mid N} \left(1 + \frac{1}{p}\right)$. The degree in J is obtained by examining the q-developments of the conjugates $\mathfrak{w}_N^s \circ M$ of $\mathfrak{w}_N^s$.

Proposition 7.1 (Oesterlé)**.** *The cosets of* $\Gamma^0(N) \backslash \Gamma$ *can be split into the following three families:*

$$T^\nu = \left(\begin{array}{cc} 1 & \nu \\ 0 & 1 \end{array}\right), 0 \leqslant \nu < N,$$

$$S = \left(\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array}\right),$$

$$M_{k,k'} = \left(\begin{array}{cc} k & kk' - 1 \\ 1 & k' \end{array}\right)$$

with $1 < k < N$, $\gcd(k, N) > 1$ *and* $0 \leqslant k' < \mu(k)$ *where* $\mu(k)$ *is the smallest integer for which* $\gcd(\mu(k)k - 1, N) = 1$.

Using (3.2), we find

Proposition 7.2.

$$(\mathfrak{w}_N^s \circ T)(z) = \mathfrak{w}_N(z + \nu)^s, 0 \leqslant \nu < N,$$

$$(\mathfrak{w}_N^s \circ S)(z) = \left(\sqrt{N} \, \frac{\eta(Nz)}{\eta(z)}\right)^s,$$

$$(\mathfrak{w}_N^s \circ M_{k,k'})(z) = \left(\zeta_{k,k'} \sqrt{\delta_k} \, \frac{\eta\left(\frac{\delta_k z + c_{k,k'}}{N/\delta_k}\right)}{\eta(z)}\right)^s,$$

where $\delta_k = \gcd(k, N)$, $\zeta_{k,k'}$ *is a 24-th root of unity and* $c_{k,k'}$ *is a rational integer.*

The proposition shows in particular that all conjugates of $\mathfrak{w}_N^s$ have integral and that $\mathfrak{w}_N^s$ and $\mathfrak{w}_N^s \circ S$ have rational q-expansions. The q-expansion principle now implies that $\Phi_N^c \in \mathbb{Z}[F, J]$, cf. [6, §3]

Theorem 7.3.
$$\deg_J \Phi_N^c = \frac{s}{24}(N - 1 + S(N))$$
where

$$S(N) = \sum_{k:1<k<N, 1<\delta_k=\gcd(k,N)<\sqrt{N}} \mu(k)\left(1 - \frac{\delta_k^2}{N}\right). \tag{7.2}$$

Proof. Consider Φ_N^c as a polynomial in F with coefficients in $\mathbb{Z}[J]$. Following the same reasoning as in [9], we see that the coefficient of highest degree in J is obtained when all conjugates are multiplied together whose q-expansions have strictly negative order; since the q-expansion of j starts with q^{-1}, the degree in J is then the opposite of this order. The $\mathfrak{w}_N(z+\nu)^s$ have negative order $-\frac{s(N-1)}{24N}$ and contribute a total of $-\frac{s(N-1)}{24}$. The function $\mathfrak{w}_N^s \circ S$ has positive order. The conjugates coming from $M_{k,k'}$ have order $\frac{s}{24}\left(\frac{\delta_k^2}{N} - 1\right)$, which is negative whenever $\delta_k < \sqrt{N}$. □

Let us note a list of useful corollaries.

Proposition 7.4. *When $N = \ell^n$ for a prime ℓ and $n \geqslant 1$, then*
$$S(N) = \begin{cases} (\ell^m - 1)^2 & \text{if } n = 2m+1, \\ (\ell^m - 1)(\ell^{m+1} - 1) & \text{if } n = 2m+2. \end{cases}$$

Proof. The k occurring in (7.2) are the $(k_1 + \ell k_2)\ell^r$ with $1 \leqslant k_1 < \ell$, $1 \leqslant r \leqslant m$ and $0 \leqslant k_2 < \ell^{n-r-1}$ (so that $k < N$); they yield $\delta_k = \ell^r$ and $\mu(k) = 1$. Hence,
$$S(N) = \sum_{r=1}^{m} (\ell - 1)\ell^{n-r-1}\left(1 - \ell^{2r-n}\right) = \left(\ell^{n-m-1} - 1\right)\left(\ell^m - 1\right).$$
□

Corollary 7.5. *When N is prime or the square of a prime, then* $\deg_J \Phi_N^c = \frac{s(N-1)}{24}$.

Proposition 7.6. *When $N = p_1 p_2$ for two primes $p_2 \geqslant p_1$, then $S(N) = p_2 - p_1$.*

Proof. The case $p_1 = p_2$ is already proven. So it remains to consider $p_1 < \sqrt{N} < p_2$, and the integers k contributing to $S(N)$ are the $\tilde{k}p_1$ with $1 \leqslant \tilde{k} < p_2$. Among these, only one is such that $\gcd(k-1, N) \neq 1$, namely the k with $\tilde{k} \equiv 1/p_1 \pmod{p_2}$; for this one, $\mu(k) = 2$. Therefore
$$S(N) = \left((p_2 - 2)\cdot 1 + 1 \cdot 2\right)\left(1 - \frac{p_1^2}{N}\right) = p_2 - p_1.$$
□

With some more effort, the constant coefficient $\Phi_N^c(0, J)$ could be obtained as the product of all conjugates, but it is not needed in the following.

7.2 Heights

Knowing the degrees of the modular polynomials, we can compare class invariants obtained from $\mathfrak{w}_N^e$ among themselves and with others using (7.1). Of special interest is the infinite family of invariants obtained in [8] from the double η-quotients

$$\mathfrak{w}_{p_1,p_2}^{\sigma}(z) = \left(\frac{\eta\left(\frac{z}{p_1}\right)\eta\left(\frac{z}{p_2}\right)}{\eta\left(\frac{z}{p_1 p_2}\right)\eta(z)} \right)^{\sigma},$$

where p_1, p_2 are (not necessarily distinct) primes and $\sigma = \frac{24}{\gcd(24,(p_1-1)(p_2-1))}$. These functions yield class invariants whenever $\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right) = 1$, and in some cases when $\left(\frac{D}{p_1}\right) = 0$ or $\left(\frac{D}{p_2}\right) = 0$, see [8, Cor. 3.1]. The degrees of their modular polynomials have been worked out in [9, Th. 9], and we summarise the results in the following table, in which ℓ and $p_1 \neq p_2$ are supposed to be prime numbers.

f	$c(f)$	$\deg_J \Phi_N^c$
$\mathfrak{w}_\ell^e$	$\frac{e(\ell-1)}{24(\ell+1)}$	$\frac{s(\ell-1)}{24}$
$\mathfrak{w}_{\ell^2}^e$	$\frac{e(\ell-1)}{24\ell}$	$\frac{\ell^2-1}{24}$ if $\ell > 3$
$\mathfrak{w}_{p_1 p_2}^e$	$\frac{e(p_2-1)}{24(p_2+1)}$	$\frac{s(p_2-1)(p_1+1)}{24}$
$\mathfrak{w}_N^e$	$\frac{e(N-1+S(N))}{24\psi(N)}$	$\frac{s(N-1+S(N))}{24}$
$\mathfrak{w}_{\ell,\ell}^e$	$\frac{e(\ell-1)^2}{12\ell(\ell+1)}$	$\frac{\sigma(\ell-1)^2}{12}$
$\mathfrak{w}_{p_1,p_2}^e$	$\frac{e(p_1-1)(p_2-1)}{12(p_1+1)(p_2+1)}$	$\frac{\sigma(p_1-1)(p_2-1)}{12}$

Notice that asymptotically for ℓ or p_1, $p_2 \to \infty$, the factors $c(f)$ tend to $\frac{e/2}{12}$ for $\mathfrak{w}_\ell^e$ (here, e is necessarily even), $\frac{e}{12}$ for the double η quotients and $\frac{e}{24}$ for $\mathfrak{w}_{\ell^2}^e$. For any discriminant D, there are suitable choices of primes in arithmetic progressions modulo D such that $e/2 = 1$ resp. $e = 1$ are reachable, and $c(f)$ may become arbitrarily close to $\frac{1}{12}$ resp. $\frac{1}{24}$. However, at the same time, the degrees of Φ_N^c in F and J tend to infinity, which may be undesirable in complex multiplication applications where the modular polynomial needs to be factored over a finite field.

In Table 7.2, we list in decreasing order of attractiveness the functions f together with the factors $1/c(f)$ they allow to gain in height compared to j and with the degree of the modular polynomial in J, thus completing the tables of [7] and [10, p. 21]. We limit ourselves to functions gaining a factor of at least 13 and with degree in J at most 20. The function $\mathfrak{w}_2$ is in fact the Weber function $\mathfrak{f}_1$, and leads to the same height as the other two Weber functions $\mathfrak{f}$ and $\mathfrak{f}_2$. Notice that, as indicated by the explicit formulæ, transformation levels divisible by 2 or 3 (or, in general, small primes) tend to yield smaller class invariants.

Table 1: Comparison of class invariants: height factor and degree in J

	$\mathfrak{w}_2$ 72,1	$>$	$\mathfrak{w}_4$ 48,1	$>$	$\mathfrak{w}_{2,73}$ 37,6	$>$	$\mathfrak{w}_{2,97}$ 147/4,8	$>$	$\mathfrak{w}_9$ 36,1	$=$	$\mathfrak{w}_2^2$ 36,1
$>$	$\mathfrak{w}_{16}$ 32,6	$>$	$\mathfrak{w}_{25}$ 30,1	$>$	$\mathfrak{w}_{3,13}$ 28,2	$=$	$\mathfrak{w}_{49}$ 28,2	$>$	$\mathfrak{w}_{81}$ 27,12	$>$	$\mathfrak{w}_{11^2}$ 132/5,5
$>$	$\mathfrak{w}_{13^2}$ 26,7	$>$	$\mathfrak{w}_{17^2}$ 51/2,12	$>$	$\mathfrak{w}_{3,37}$ 76/3,6	$=$	$\mathfrak{w}_{19^2}$ 76/3,15	$>$	$\mathfrak{w}_{3,61}$ 124/5,10	$>$	$\mathfrak{w}_{5,7}$ 24,2
$=$	$\mathfrak{w}_2^3$ 24,1	$=$	$\mathfrak{w}_6^2$ 24,6	$=$	$\mathfrak{w}_4^2$ 24,1	$=$	$\mathfrak{w}_3^2$ 24,1	$>$	$\mathfrak{w}_{5,13}$ 21,4	$=$	$\mathfrak{w}_{2,13}^2$ 21,2
$>$	$\mathfrak{w}_{12}^2$ 144/7,14	$>$	$\mathfrak{w}_{5,19}$ 20,6	$>$	$\mathfrak{w}_{5,31}$ 96/5,10	$>$	$\mathfrak{w}_{5,37}$ 19,12	$=$	$\mathfrak{w}_{2,37}^2$ 19,6	$>$	$\mathfrak{w}_{7,13}$ 56/3,6
$>$	$\mathfrak{w}_{2,61}^2$ 93/5,10	$>$	$\mathfrak{w}_{7,17}$ 18,8	$=$	$\mathfrak{w}_{15}^2$ 18,8	$=$	$\mathfrak{w}_8^2$ 18,8	$=$	$\mathfrak{w}_2^4$ 18,1	$=$	$\mathfrak{w}_5^2$ 18,1
$=$	$\mathfrak{w}_{10}^2$ 18,4	$>$	$\mathfrak{w}_{11,13}$ 84/5,10	$>$	$\mathfrak{w}_{3,7}^2$ 16,2	$=$	$\mathfrak{w}_{35}^2$ 16,18	$=$	$\mathfrak{w}_{21}^2$ 16,6	$=$	$\mathfrak{w}_{40}^2$ 16,18
$=$	$\mathfrak{w}_{14}^2$ 16,18	$=$	$\mathfrak{w}_{16}^2$ 16,6	$=$	$\mathfrak{w}_{28}^2$ 16,12	$=$	$\mathfrak{w}_7^2$ 16,1	$=$	$\mathfrak{w}_3^3$ 16,1	$=$	$\mathfrak{w}_6^3$ 16,6
$>$	$\mathfrak{w}_{45}^2$ 108/7,14	$>$	$\mathfrak{w}_{13,13}$ 91/6,12	$>$	$\mathfrak{w}_{55}^2$ 72/5,10	$=$	$\mathfrak{w}_{77}^2$ 72/5,20	$=$	$\mathfrak{w}_{22}^2$ 72/5,10	$=$	$\mathfrak{w}_{11}^2$ 72/5,5
$=$	$\mathfrak{w}_{33}^2$ 72/5,10	$=$	$\mathfrak{w}_{27}^2$ 72/5,15	$>$	$\mathfrak{w}_{91}^2$ 14,16	$=$	$\mathfrak{w}_{65}^2$ 14,18	$=$	$\mathfrak{w}_{13}^2$ 14,1	$>$	$\mathfrak{w}_{12}^3$ 96/7,14
$>$	$\mathfrak{w}_{2,17}^3$ 27/2,4	$=$	$\mathfrak{w}_{85}^2$ 27/2,8	$=$	$\mathfrak{w}_{34}^2$ 27/2,16	$=$	$\mathfrak{w}_{17}^2$ 27/2,4	$>$	$\mathfrak{w}_{3,19}^2$ 40/3,6	$=$	$\mathfrak{w}_{7\cdot 19}^2$ 40/3,12
$=$	$\mathfrak{w}_{57}^2$ 40/3,18	$=$	$\mathfrak{w}_{19}^2$ 40/3,3	$>$	$\mathfrak{w}_{23}^2$ 144/11,11						

8 Outlook

The presented results concern singular values of powers of $\mathfrak{w}_N$ as class invariants. It is possible to obtain smaller invariants by authorising 24-th roots of unity to enter the game. This was already done by Weber for $N = 2$ (the classical f-functions) and by Gee in [16] for $N = 3$. For instance, $\zeta_4 \mathfrak{w}_7^2$ is an invariant for $D = -40$, leading to the minimal polynomial

$$X^2 + (-5 + 2\omega)\, X + 3 - 4\,\omega.$$

Similarly, when N is not a square and e is odd, then $\mathfrak{w}_N^e \circ S$ has a q-expansion that is rational up to a factor $\sqrt{N}$, so that Theorems 2.3 and 2.4

are not applicable any more. Nevertheless, $\mathfrak{w}_N^e$ may yield class invariants; this is well-known for Weber's original functions in certain cases.

Acknowledgements. The second author wants to thank the University of Waterloo for its hospitality during his sabbatical leave; he also wants to acknowledge the warm and studious atmosphere of the Asahi Judo club of Kitchener where large parts of the results were proven. The first author was partially funded by ERC Starting Grant ANTICS 278537.

References

[1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203):29–68, 1993.

[2] B. J. Birch. Weber's class invariants. *Mathematika*, 16:283–294, 1969.

[3] D. A. Buell. *Binary quadratic forms (Classical theory and modern computations)*. Springer-Verlag, 1989.

[4] H. Cohn. *A classical invitation to algebraic numbers and class fields.* Universitext. Springer-Verlag, 1978.

[5] R. Dedekind. Erläuterungen zu den vorstehenden Fragmenten. In R. Dedekind and H. Weber, editors, *Bernhard Riemann's gesammelte mathematische Werke und wissenschaftlicher Nachlaß*, pages 438–447. Teubner, Leipzig, 1876.

[6] M. Deuring. Die Klassenkörper der komplexen Multiplikation. In *Enzyklopädie der mathematischen Wissenschaften mit Einschluß ihrer Anwendungen*, volume I 2, Heft 10, Teil II. Teubner, Stuttgart, 1958.

[7] A. Enge and F. Morain. Comparing invariants for class fields of imaginary quadratic fields. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 252–266. Springer-Verlag, 2002. 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings.

[8] A. Enge and R. Schertz. Constructing elliptic curves over finite fields using double eta-quotients. *Journal de Théorie des Nombres de Bordeaux*, 16:555–568, 2004.

[9] A. Enge and R. Schertz. Modular curves of composite level. *Acta Arith.*, 181(2):129–141, 2005.

[10] Andreas Enge. *Courbes algébriques et cryptologie.* Habilitation à diriger des recherches, Université Denis Diderot, Paris 7, 2007.

[11] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Mathematics of Computation*, 78(266):1089–1107, 2009.

[12] Andreas Enge and Reinhard Schertz. Singular values of multiple eta-quotients for ramified primes. Technical Report 768375, HAL-INRIA, 2012. To appear in LMS Journal of Computation and Mathematics.

[13] David Freemann, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, 2010.

[14] A. Gee. Class invariants by Shimura's reciprocity law. *J. Théor. Nombres Bordeaux*, 11:45–72, 1999.

[15] A. Gee and P. Stevenhagen. Generating class fields using Shimura reciprocity. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 441–453. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, June 1998, Proceedings.

[16] Alice Chia Ping Gee. *Class fields by Shimura reciprocity.* Proefschrift, Universiteit Leiden, 2001.

[17] F. Hajir. Elliptic units of cyclic unramified extensions of complex quadratic fields. *Acta Arith.*, LXIV:69–85, 1993.

[18] F. Hajir. *Unramified elliptic units.* Phd in mathematics, Princeton University, June 1993.

[19] F. Hajir and F. R. Villegas. Explicit elliptic units, I. *Duke Math. J.*, 90(3):495–521, 1997.

[20] C. Meyer. Bemerkungen zum Satz von Heegner–Stark über die imaginär-quadratischen Zahlkörper mit der Klassenzahl Eins. *Journal für die reine und angewandte Mathematik*, 242:179–214, 1970.

[21] François Morain. Computing the cardinality of CM elliptic curves using torsion points. *Journal de Théorie des Nombres de Bordeaux*, 19(3):663–681, 2007.

[22] R. Schertz. Weber's class invariants revisited. *J. Théor. Nombres Bordeaux*, 14(1):325–343, 2002.

[23] Reinhard Schertz. Die singulären Werte der Weberschen Funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, γ_2, γ_3. *Journal für die reine und angewandte Mathematik*, 286/287:46–74, 1976.

[24] Reinhard Schertz. *Complex Multiplikation.* Cambridge University Press, Cambridge, 2009.

[25] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten and Princeton University Press, 1971.

[26] H. M. Stark. On the "gap" in a theorem of Heegner. *J. Number Theory*, 1:16–27, 1969.

[27] H. Weber. *Lehrbuch der Algebra*, volume III. Chelsea Publishing Company, New York, 1902.