Singular values of multiple eta-quotients for ramified primes

Andreas Enge* and Reinhard Schertz†

6 May 2013

Abstract

We determine the conditions under which singular values of multiple η-quotients of square-free level, not necessarily prime to 6, yield class invariants, that is, algebraic numbers in ring class fields of imaginary-quadratic number fields. We show that the singular values lie in subfields of the ring class fields of index $2^{k'-1}$ when $k' \geqslant 2$ primes dividing the level are ramified in the imaginary-quadratic field, which leads to faster computations of elliptic curves with prescribed complex multiplication. The result is generalised to singular values of modular functions on $X_0^+(p)$ for p prime and ramified.

Keywords: complex multiplication, class invariants, eta quotients, ring class fields.

MSC 2010: 11G15, 14K22, 11Y40

Let $K = \mathbb{Q}(\sqrt{\Delta})$ be an imaginary-quadratic number field of discriminant Δ, and let $\mathcal{O}_D$ be the order of discriminant $D = c^2\Delta$ and conductor c in K. For a modular function f and an argument $\tau \in K \subseteq \mathbb{C}$ with $\Im\tau > 0$ we call the *singular value* $f(\tau)$ a *class invariant* if it lies in the *ring class field* Ω_c. This is the abelian extension of K with Galois group canonically isomorphic to $\mathrm{Cl}(\mathcal{O}_D)$ through the *Artin map* $\sigma : \mathrm{Cl}(\mathcal{O}_D) \to \mathrm{Gal}(\Omega_c/K)$, which sends a prime ideal representing an ideal class to its associated *Frobenius automorphism.* In this article, we are interested in class invariants derived from multiple η-quotients, and we examine in particular cases where those generate a subfield of the ring class field.

In §1 we define the multiple η-quotients under consideration and collect their properties, in particular their transformation behaviour under unimodular matrices. We then proceed in §2 to determine conditions under which their singular values lie in the ring

*INRIA, LFANT, F-33400 Talence, France
CNRS, IMB, UMR 5251, F-33400 Talence, France
Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France
andreas.enge@inria.fr
This research was partially funded by ERC Starting Grant ANTICS 278537.
†Universität Augsburg
schertz@math.uni-augsburg.de

class field and show how to compute their characteristic polynomials with respect to the number field extension Ω_c/K using roots of an *n-system*, suitably normalised quadratic forms of discriminant D representing the class group. The results of §3 are at the heart of this article: We show that if some or all of the primes dividing the level of the multiple η-quotient are ramified in K, then the singular values lie in fact in a subfield L of Ω_c of index a power of 2; more precisely, the Galois group of Ω_c/L is elementary abelian, so that Ω_c is a compositum of linearly disjoint quadratic extensions of L. An alternative proof for the special case that all primes are ramified leads to an interesting generalisation in §4, namely to functions of prime level invariant under the Fricke–Atkin–Lehner involution. We conclude by some class field theoretic remarks in §5, showing how this computationally less expensive construction of subfields of Ω_c may be completed to obtain the full ring class field.

1 Multiple η-quotients

In this section, we define multiple η-quotients and collect their basic properties, most of which are either well-known or readily verified.

Let η be Dedekind's function, and consider positive integers $p_1, \ldots, p_k$; in later sections, they will be distinct primes, but this restriction is not needed for the time being.

The *simple η-quotient* of level p_1 is defined by

$$\mathfrak{w}_{p_1}(z) = \frac{\eta\left(\frac{z}{p_1}\right)}{\eta(z)}, \tag{1}$$

and the *double η-quotient* of level $p_1 p_2$ by

$$\mathfrak{w}_{p_1,p_2}(z) = \frac{\eta\left(\frac{z}{p_1}\right)\eta\left(\frac{z}{p_2}\right)}{\eta\left(\frac{z}{p_1 p_2}\right)\eta(z)} = \frac{\mathfrak{w}_{p_1}(z)}{\mathfrak{w}_{p_1}\left(\frac{z}{p_2}\right)} = \frac{\mathfrak{w}_{p_2}(z)}{\mathfrak{w}_{p_2}\left(\frac{z}{p_1}\right)}. \tag{2}$$

The process may be continued inductively by letting

$$\mathfrak{w}_{p_1,\ldots,p_{k+1}} = \frac{\mathfrak{w}_{p_1,\ldots,p_k}(z)}{\mathfrak{w}_{p_1,\ldots,p_k}\left(\frac{z}{p_{k+1}}\right)}, \tag{3}$$

so that $\mathfrak{w}_{p_1,\ldots,p_k}$ is a quotient of transformed η-functions with 2^k factors in the numerator and as many in the denominator.

Let $\mathcal{F}_n$ denote the set of modular functions of level n whose q-expansions have coefficients in $\mathbb{Q}(\zeta_n)$. The powers of the multiple η-quotients are elements of $\mathcal{F}_n$ for some n, which can be determined from the transformation behaviour of η under unimodular substitutions. Here and in the following, we consider unimodular matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \mathrm{Sl}_2(\mathbb{Z})/\{\pm 1\}$, normalised such that $c \geqslant 0$, and $d > 0$ if $c = 0$.

We denote by $\cdot'$ the odd part and by $\lambda(\cdot)$ the 2-adic valuation of a number, so that $c = c'\,2^{\lambda(c)}$; by convention, $\lambda(0) = 0' = 1$. Let

$$\begin{aligned}
\bar{e}(M) &= ab + c\big(d(1-a^2) - a\big) + 3c'(a-1) \\
e(M) &= \bar{e}(M) + \frac{3}{2}\lambda(c)(a^2-1) \\
\varepsilon(M) &= \left(\frac{a}{c'}\right)\zeta_{24}^{e(M)}
\end{aligned}$$

with $\zeta_{24} = e^{2\pi i/24}$. Notice that $e(M) - \bar{e}(M)$ is divisible by 12, since a and c cannot be even simultaneously. By [Sch10, Th. 1.10.1],

$$\eta(Mz) = \varepsilon(M)\sqrt{cz+d}\,\eta(z).$$

So for $M \in \Gamma^0(N)$ with $b = Nb_0$ we have, cf. [ES05, Th. 3],

$$\begin{aligned}
\mathfrak{w}_N(Mz) &= \varepsilon\begin{pmatrix} a & b_0 \\ Nc & d \end{pmatrix} \varepsilon\begin{pmatrix} a & Nb_0 \\ c & d \end{pmatrix}^{-1} \mathfrak{w}_N(z) \qquad (4)\\
&= \left(\frac{a}{N'}\right)\zeta_{24}^{(N-1)\left(-ab_0 + c(d(1-a^2)-a)\right) + 3(N'-1)c'(a-1) + \frac{3}{2}(\lambda(Nc)-\lambda(c))(a^2-1)} \mathfrak{w}_N(z),
\end{aligned}$$

where $\lambda(Nc) - \lambda(c)$ equals 0 for $c = 0$, and $\lambda(N)$ otherwise. With $s = \frac{24}{\gcd(24, N-1)}$ and $e \mid s$, we have $\mathfrak{w}_N^e \in \mathcal{F}_{\frac{s}{e}N}$ by [EM09, Th. 6].

For the double η-quotients $\mathfrak{w}_{p_1,p_2}$ of level $N = p_1p_2$ and $M \in \Gamma^0(N)$ with $b = Nb_0$ we compute

$$\begin{aligned}
\mathfrak{w}_{p_1,p_2}(Mz) &= \varepsilon\begin{pmatrix} a & p_2b_0 \\ p_1c & d \end{pmatrix} \varepsilon\begin{pmatrix} a & p_1b_0 \\ p_2c & d \end{pmatrix} \varepsilon\begin{pmatrix} a & b_0 \\ Nc & d \end{pmatrix}^{-1} \varepsilon\begin{pmatrix} a & Nb_0 \\ c & d \end{pmatrix}^{-1} \mathfrak{w}_{p_1,p_2}(z) \qquad (5)\\
&= \zeta_{24}^{-(p_1-1)(p_2-1)\left(ab_0 + c(d(1-a^2)-a)\right) - 3(p_1'-1)(p_2'-1)c'(a-1)} \mathfrak{w}_{p_1,p_2}(z).
\end{aligned}$$

Let $s = \frac{24}{\gcd(24, (p_1-1)(p_2-1))}$ and $e \mid s$. Then $\mathfrak{w}_{p_1,p_2}^e \in \mathcal{F}_{\frac{s}{e}N}$, cf. [ES05, Th. 7] and (5).

For η-quotients of order $k \geqslant 2$, where $N = p_1 \cdots p_k$, the formula generalises as

$$\begin{aligned}
&\mathfrak{w}_{p_1,\ldots,p_k}(Mz) = \\
&\zeta_{24}^{-(p_1-1)\cdots(p_k-1)\left(ab_0 + (-1)^k c(d(1-a^2)-a)\right) - 3(-1)^k(p_1'-1)\cdots(p_k'-1)c'(a-1)} \mathfrak{w}_{p_1,\ldots,p_k}(z).
\end{aligned} \qquad (6)$$

If $s = \frac{24}{\gcd(24, (p_1-1)\cdots(p_k-1))}$ and $e \mid s$, then $\mathfrak{w}_{p_1,\ldots,p_k}^e \in \mathcal{F}_{\frac{s}{e}N}$.

For later reference, we also recall the transformation behaviour of $\gamma_2 = \sqrt[3]{j}$ and $\gamma_3 = \sqrt{j - 1728}$, see [Sch10, §2.4.3]:

$$\gamma_2(Mz) = \zeta_3^{-e(M)}\gamma_2(z), \gamma_3(Mz) = (-1)^{e(M)}\gamma_3(z), (\gamma_2\gamma_3)(Mz) = \zeta_6^{e(M)}(\gamma_2\gamma_3)(z). \qquad (7)$$

Since η has a rational q-expansion, so does $\mathfrak{w}_{p_1,\dots,p_k}$. For $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we have $\eta\left(\frac{Sz}{N}\right) = \varepsilon(S)\sqrt{Nz}\,\eta(Nz)$ by [ES05, Th. 3], so that

$$\mathfrak{w}_N(Sz) = \sqrt{N}\,\frac{\eta(Nz)}{\eta(z)} = \sqrt{N}\,\mathfrak{w}_N(Nz)^{-1}$$

has a rational q-expansion up to a factor $\sqrt{N}$. For $k \geqslant 2$ and $N = p_1 \cdots p_k$, this implies $\mathfrak{w}_{p_1,\dots,p_k}(Sz) = \mathfrak{w}_{p_1,\dots,p_k}(Nz)^{(-1)^k}$, which has a rational q-expansion.

Denote by $|_N$ the Fricke-Atkin-Lehner involution associated to $\Gamma^0(N)$, so that $f|_N(z) = f\left(\frac{-N}{z}\right)$. The previous equation can be rewritten as

$$\mathfrak{w}_{p_1,\dots,p_k}|_N(z) = \mathfrak{w}_{p_1,\dots,p_k}(z)^{(-1)^k}; \tag{8}$$

in particular, $\mathfrak{w}_{p_1,\dots,p_k}$ is invariant under the involution for even k.

2 Singular values of multiple η-quotients

2.1 Class invariants

A very general result on class invariants is obtained in [Sch02, Th. 4]: Let f be modular for $\Gamma^0(N)$ such that f and $f \circ S$ have rational q-expansions. Assume that there are A and B such that $\mathfrak{a} = A\mathbb{Z} + \frac{-B+\sqrt{D}}{2}\mathbb{Z}$ is a proper ideal of $\mathcal{O}_D$, $N \mid \frac{B^2-D}{4A}$ and N is coprime to the conductor c. Let $\tau = \frac{-B+\sqrt{D}}{2A}$ be the basis quotient of $\mathfrak{a}$ with $\Im\tau > 0$. Then $f(\tau) \in \Omega_c$. We use this theorem to determine when singular values of powers of multiple η-quotients are class invariants.

Theorem 1 *Let $p_1 < p_2$ be primes and e an integer such that one of the following conditions is satisfied:*

1) $\{p_1, p_2\} \cap \{2, 3\} = \emptyset$
$e(p_1-1)(p_2-1) \equiv 0 \pmod 3$ *or* $3 \nmid D$, *and*
$e(p_1-1)(p_2-1) \equiv 0 \pmod 8$ *or* $2 \nmid D$.

2) $p_1 = 3$, $p_2 \geqslant 5$
$e(p_2-1) \equiv 0 \pmod 3$, *and*
$e(p_2-1) \equiv 0 \pmod 4$ *or* $2 \nmid D$.

3) $p_1 = 2$
$e(p_2-1) \equiv 0 \pmod{24}$.

Let p_1, p_2 be non-inert in K and not dividing the conductor c, and let $\tau = \frac{-B+\sqrt{D}}{2A}$ be such that $p_1p_2 \mid C = \frac{B^2-D}{4A}$. Then $\mathfrak{w}_{p_1,p_2}^e(\tau) \in \Omega_c$.

Proof: The result is well-known in the case $e(p_1-1)(p_2-1) \equiv 0 \pmod{24}$, cf. [ES04, Th. 3.2], since then $\mathfrak{w}^e_{p_1,p_2}$ is modular for $\Gamma^0(p_1p_2)$. In all other cases, p_1 and p_2 are odd, and (5) becomes

$$\mathfrak{w}_{p_1,p_2}(Mz) = \zeta_6^{-\frac{(p_1-1)(p_2-1)}{4}(e(M)+ab_0(1-p_1p_2))}\mathfrak{w}_{p_1,p_2}(z). \tag{9}$$

Consider first the case that $p_1, p_2 \neq 3$, and let $h = (\gamma_2\gamma_3)^{\frac{(p_1-1)(p_2-1)}{4}}\mathfrak{w}_{p_1,p_2}$. From (7), (9) and the fact that at least one of p_1-1, p_2-1 and $1-p_1p_2$ is divisible by 3, we deduce that h is modular for $\Gamma^0(p_1p_2)$, cf. [Sch10, §2.4.3], so that $h(\tau) \in \Omega_c$. Since $\gamma_2(\tau) \in \Omega_c$ for $3 \nmid D$ and $\gamma_3(\tau) \in \Omega_c$ for $2 \nmid D$ by [Sch02, Th. 2 and 3], and $j(\tau) = \gamma_2(\tau)^3 = \gamma_3(\tau)^2+1728 \in \Omega_c$, we have $(\gamma_2\gamma_3)^{e\frac{(p_1-1)(p_2-1)}{4}}(\tau) \in \Omega_c$ under the assumptions of the theorem, which proves the result.

If $p_1 = 3$, the function h^e is modular for $\Gamma^0(p_1p_2)$ under the conditions of the theorem, and we conclude analogously. $\square$

Similar results hold for higher order η-quotients; in fact, adding odd primes makes it easier to satisfy the restrictions modulo 8.

Theorem 2 *For $k \geqslant 3$, let e be an integer and $p_1, \ldots, p_k$ distinct primes such that one of the following conditions is satisfied:*

1) $e(p_1-1)\cdots(p_k-1) \equiv 0 \pmod{24}$.

2) All p_i are odd and congruent to -1 modulo 3, and $3 \nmid D$.

Let $p_1, \ldots, p_k$ be non-inert in K and not dividing the conductor c, and let $\tau = \frac{-B+\sqrt{D}}{2A}$ be such that $N = p_1\cdots p_k \mid C = \frac{B^2-D}{4A}$. Then $\mathfrak{w}^e_{p_1,\ldots,p_k}(\tau) \in \Omega_c$.

Proof: The first case is trivial. In the second case, we use the auxiliary function $h = \gamma_2^{(-1)^k}\mathfrak{w}_{p_1,\ldots,p_k}$, which is modular for $\Gamma^0(N)$ by (6), (7), where $N \equiv (-1)^k \pmod 3$, and we conclude as in the proof of Theorem 1. $\square$

2.2 n-systems and reality of class polynomials

In order to compute the *class polynomial* $H^f_D(X)$, the characteristic polynomial of a class invariant $f(\tau)$ under the action of $\mathrm{Cl}(\mathcal{O}_D)$, we need to explicitly determine the conjugates of $f(\tau)$ under the Galois group $\mathrm{Cl}(\mathcal{O}_D)$. Classically, this is done using Shimura reciprocity. The concept of n-systems was introduced in [Sch02]; it encapsulates Shimura reciprocity and provides a simple way of expressing the conjugates as singular values of the *same* function f in basis quotients of suitably normalised quadratic ideals.

An n-system for $\mathrm{Cl}(\mathcal{O}_D)$ is defined as a set of quadratic forms $[A_i, B_i, C_i] = A_iX^2 + B_iX + C_i$, $C_i = \frac{B_i^2-D}{4A_i}$, $\gcd(A_i, B_i, C_i) = 1$ for $1 \leqslant i \leqslant h(\mathcal{O}_D)$, such that the ideals $\mathfrak{a}_i = \begin{pmatrix} \frac{-B_i+\sqrt{D}}{2} \\ A_i \end{pmatrix}_{\mathbb{Z}}$ form a system of representatives of $\mathrm{Cl}(\mathcal{O}_D)$, and furthermore

$$\gcd(A_i, n) = 1 \text{ and } B_i \equiv B_1 \pmod{2n}.$$

(Here and in the following, we write $\mathbb{Z}$-bases of ideals as column vectors such that the *basis quotient* of its two entries is the root of the quadratic form with positive imaginary part.)

Notice that if $n \mid C_1$, then $n \mid C_i$ for all i. For any n, an initial $[A_1, B_1, C_1]$ with $\gcd(A_1, n) = 1$ is easily extended to an n-system using the algorithm of [Sch02, Prop. 3]. It is shown in [Sch02, Th. 7] that if $f \in \mathcal{F}_n$ is such that $f \circ S$ has a rational q-expansion, $\tau_i = \frac{-B_i+\sqrt{D}}{2A_i}$ are basis quotients coming from an n-system and $f(\tau_1) \in \Omega_c$, then its algebraic conjugates are the $f(\tau_i)$. More precisely, if $\sigma : \mathrm{Cl}(\mathcal{O}_D) \xrightarrow{\simeq} \mathrm{Gal}(\Omega_c/K)$ is the Artin map, then

$$H_D^f(X) = \prod_{\mathfrak{k} \in \mathrm{Cl}(\mathcal{O}_D)} \left(X - f(\tau_1)^{\sigma(\mathfrak{k})}\right) = \prod_{i=1}^{h(\mathcal{O}_D)} \left(X - f(\tau_i)\right) \in K[X].$$

This characterisation can also be used to identify pairs of complex conjugate roots of the class polynomial whenever the latter is real. We recall that $|_N$ denotes the Fricke–Atkin–Lehner involution such that $f|_N(z) = f\left(\frac{-N}{z}\right)$.

Theorem 3 *Let N and n be integers such that $N \mid n$, let $f \in \mathcal{F}_n$ be such that f and $f \circ S$ have rational q-expansions, and assume that there is an ideal $\mathfrak{n} = \begin{pmatrix} \frac{-B_1+\sqrt{D}}{2} \\ A_1 \end{pmatrix}$ of basis quotient $\tau_1 = \frac{-B_1+\sqrt{D}}{2A_1}$ and cofactor $C_1 = \frac{B_1^2-D}{4A_1}$ such that $C_1 = N$ and $f(\tau_1) \in \Omega_c$.*

Write $\tau_0 = A_1\tau_1$. Then $f(\tau_0) = f(\tau_1)^{\sigma(\mathfrak{n})} \in \Omega_c$.

Assume that there is a proper ideal $\mathfrak{c}$ of $\mathcal{O}_D$ such that $f|_N(\tau_0) = f(\tau_0)^{\sigma(\mathfrak{c})}$. Then $H_D^f(X) \in \mathbb{Q}[X]$. More precisely, if the $\mathfrak{a}_i$ are given by an n-system $[A_i, B_i, C_i]$ for $\mathrm{Cl}(\mathcal{O}_D)$ with basis quotients τ_i and $\sim$ denotes equivalence in the class group, then $f(\tau_i)$ and $f(\tau_j)$ are complex conjugates if $\mathfrak{a}_i\mathfrak{a}_j \sim \mathfrak{n}\mathfrak{c}^{-1}$. In particular, $f(\tau_i) \in \mathbb{R}$ if $\mathfrak{a}_i^2 \sim \mathfrak{n}\mathfrak{c}^{-1}$.

This result generalises [ES04, Th. 3.4], which treats the case that $f|_N = f$ (so that $\mathfrak{c} = \mathcal{O}_D$) and that $N = n$. The latter condition is used in [ES04] only to ensure that $f(\tau_1) \in \Omega_c$, which instead we added to the hypotheses of the theorem. Once the correct assumptions are identified, the proof itself is very similar.

Proof: The proof of [Sch02, Th. 7] shows that

$$f(\tau_i) = f(\tau_0)^{\sigma(\mathfrak{a}_i^{-1})} \tag{10}$$

for all i. (Here we need the rationality of the q-expansion of $f \circ S$, which implies that all g_i equal $g = f$ in the notation of [Sch02].)

Denote by κ the complex conjugation, and recall that $\mathrm{Gal}(\Omega_c/\mathbb{Q})$ is isomorphic to the generalised dihedral group $\mathrm{Cl}(\mathcal{O}_D) \rtimes \langle\kappa\rangle$ with $\kappa\sigma(\mathfrak{a})\kappa = \sigma(\mathfrak{a}^{-1})$ for $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_D)$.

We first consider $i = 1$ and use that $f(z)^\kappa = f(-z^\kappa)$ by the rationality of the q-expansion of f. Then

$$\begin{aligned} f(\tau_1)^\kappa &= f\left(\frac{-B_1+\sqrt{D}}{2A_1}\right)^\kappa = f\left(\frac{B_1+\sqrt{D}}{2A_1}\right) = f\left(\frac{2N}{B_1-\sqrt{D}}\right) \text{ since } C_1 = N \\ &= f|_N(\tau_0) = f(\tau_0)^{\sigma(\mathfrak{c})} \text{ by assumption.} \end{aligned}$$

Let now i and j be such that $\mathfrak{a}_i\mathfrak{a}_j \sim \mathfrak{n}\mathfrak{c}^{-1}$. We compute

$$\begin{aligned} f(\tau_i)^\kappa &= f(\tau_1)^{\sigma(\mathfrak{n}\mathfrak{a}_i^{-1})\kappa} \text{ by (10)} \\ &= f(\tau_1)^{\kappa\sigma(\mathfrak{n}^{-1}\mathfrak{a}_i)} = f(\tau_0)^{\sigma(\mathfrak{c}\mathfrak{n}^{-1}\mathfrak{a}_i)} = f(\tau_j)^{\sigma(\mathfrak{a}_j\mathfrak{c}\mathfrak{n}^{-1}\mathfrak{a}_i)} = f(\tau_j). \end{aligned}$$

$\square$

Corollary 4 *Under the hypotheses of Theorems 1 or 2, let* $N = p_1 \cdots p_k$, $s = \frac{24}{\gcd\left(24,(p_1-1)\cdots(p_k-1)\right)}$, $e \mid s$ *and* $n = \frac{s}{e}N$. *Then there is an* n*-system satisfying* $C_1 = N$, *which yields the roots of the class polynomial* $H_D^{\mathfrak{w}_{p_1,\ldots,p_k}^e}$.

Moreover, the polynomial is real for even k*; its complex conjugate roots may be identified by Theorem 3 with* $\mathfrak{c} = \mathcal{O}_D$.

Proof: Since none of the prime divisors of N is inert, there is an ideal of norm N or, equivalently, a quadratic form $[A_1, B_1, C_1]$ with $C_1 = N$. An application of Theorem 3 using (8) finishes the proof. $\square$

For $f = \mathfrak{w}_{p_1,\ldots,p_k}^e$ with odd k, the class polynomial is in general defined over K. As for simple η-quotients in [EM09, Th. 21], a particular case is easily identified in which the class polynomial is real: If $n \mid B_1$, which implies that $N \mid D$ and that all primes dividing N are ramified, then $-B_i \equiv B_i \pmod{2n}$, and for every ideal class $\mathfrak{a}_i$ represented by an element $[A_i, B_i, C_i]$ of the n-system, the inverse class $\overline{\mathfrak{a}}_i$ is represented by the element $[A_i, -B_i, C_i]$. Together with the rationality of the q-expansion of f, this implies that H_D^f is real and that $f(\tau_j) = \overline{f(\tau_i)}$ if $\mathfrak{a}_j \sim \overline{\mathfrak{a}}_i \sim \mathfrak{a}_i^{-1}$. It is then enough to compute only $\frac{h(\mathcal{O}_D)+h_0}{2}$ values $f(\tau_i)$, where h_0 is the number of real roots of the class polynomial, which is bounded above by the size of the 2-torsion subgroup of $\mathrm{Cl}(\mathcal{O}_D)$. So it is generally small, and the required number of function evaluations boils down to essentially $\frac{h(\mathcal{O}_D)}{2}$.

We show in Corollary 8 that the condition $n \mid B_1$ is in fact too restrictive: H_D^f is real already when only one prime dividing N is ramified in K.

2.3 Examples

Let $D = -215 = -5 \cdot 31$, for which 2, 3, 7 and 11 split and 5 ramifies. The class number of $\mathcal{O}_{-215}$ is 14, and $\mathcal{O}_{-215} = \mathbb{Z} + \omega\mathbb{Z}$ with $\omega = \frac{1+\sqrt{-215}}{2}$.

Using the double η-quotient for the primes 7 and 11, the full exponent s equals 2, but we may use the lower exponent $e = 1$ by Theorem 1:

$$\begin{aligned} H_{-215}^{\mathfrak{w}_{7,11}}(X) =& X^{14} - 10X^{13} + 42X^{12} - 97X^{11} + 144X^{10} - 147X^9 + 89X^8 + 25X^7 \\ & - 124X^6 + 113X^5 - 23X^4 - 28X^3 + 20X^2 - 5X + 1. \end{aligned}$$

The triple η-quotient for 2, 3 and 7 has $s = e = 2$, and

$$\begin{aligned} H_{-215}^{\mathfrak{w}_{2,3,7}^2}(X) =& X^{14} + (17+\omega)X^{13} + (104+16\omega)X^{12} + (211+107\omega)X^{11} \\ & + (-573+379\omega)X^{10} + (-4197+737\omega)X^9 + (-10230+686\omega)X^8 \\ & - 13247X^7 + (-9544-686\omega)X^6 + (-3460-737\omega)X^5 \\ & + (-194-379\omega)X^4 + (318-107\omega)X^3 + (120-16\omega)X^2 \\ & + (18-\omega)X + 1. \end{aligned}$$

With the ramified 5 instead of the split 7, the polynomial becomes real, but one needs the higher exponent $s = e = 3$:

$$\begin{aligned} H_{-215}^{\mathfrak{w}_{2,3,5}^3}(X) =& X^{14} + 22X^{13} + 175X^{12} + 578X^{11} + 819X^{10} + 2190X^9 + 10130X^8 \\ & + 17295X^7 + 10130X^6 + 2190X^5 + 819X^4 + 578X^3 + 175X^2 + 22X + 1. \end{aligned}$$

Examples for η-quotients of order 4 and 5 are given by

$$\begin{aligned} H_{-215}^{\mathfrak{w}_{2,3,5,7}}(X) =& X^{14} - X^{13} - 8X^{12} - 12X^{11} - 7X^{10} - 4X^9 - 17X^8 - 29X^7 - 17X^6 \\ & - 4X^5 - 7X^4 - 12X^3 - 8X^2 - X + 1 \end{aligned}$$

and

$$\begin{aligned} H_{-215}^{\mathfrak{w}_{2,3,5,7,11}}(X) =& X^{14} - 3X^{13} + 6X^{12} + 35X^{11} + 80X^{10} + 130X^9 + 188X^8 + 201X^7 \\ & + 188X^6 + 130X^5 + 80X^4 + 35X^3 + 6X^2 - 3X + 1. \end{aligned}$$

3 Singular values for ramified primes

3.1 Class invariants in subfields

In this section, we show that the singular values of multiple η-quotients lie in subfields of the ring class field when at least two of the involved primes are ramified. We first treat the case of double η-quotients, which is slightly more involved than $k \geqslant 3$.

Theorem 5 *Under the assumptions of Theorem 1, let $p_1 \neq p_2$ be ramified in K. Denoting by $\mathfrak{p}_i$ the ideal of the maximal order $\mathcal{O}_\Delta$ of K above p_i and by $\sigma(\mathfrak{p}_i)$ the associated Frobenius automorphism of Ω_c/K, we have*

1) $\mathfrak{w}_{p_1,p_2}^e(\tau)^{\sigma(\mathfrak{p}_1)} = \left(\frac{p_1}{p_2'}\right)^e \frac{1}{\mathfrak{w}_{p_1,p_2}^e(\tau)}$, *2)* $\mathfrak{w}_{p_1,p_2}^e(\tau)^{\sigma(\mathfrak{p}_2)} = \left(\frac{p_2}{p_1'}\right)^e \frac{1}{\mathfrak{w}_{p_1,p_2}^e(\tau)}$, *and*

3) $\mathfrak{w}_{p_1,p_2}^e(\tau)^{\sigma(\mathfrak{p}_1\mathfrak{p}_2)} = \begin{cases} (-1)^{\frac{e(p_1-1)(p_2-1)}{4}} \mathfrak{w}_{p_1,p_2}^e(\tau) & \text{if } 2 \nmid p_1p_2 \\ (-1)^{\frac{e(p_2^2-1)}{8}} \mathfrak{w}_{p_1,p_2}^e(\tau) & \text{if } p_1 = 2 \end{cases}.$

In particular, if $|D| \notin \{p_1p_2, 4p_1p_2\}$ and one of the following conditions holds:

- *e is even;*
- *p_1 and p_2 are odd and one of them is congruent to 1 modulo 4;*
- *$p_1 = 2$ and $p_2 \equiv \pm 1 \pmod 8$;*

then $\mathfrak{w}_{p_1,p_2}^e(\tau)$ lies in the subfield of index 2 of Ω_c/K with Galois group $\mathrm{Cl}(\mathcal{O}_D)/\langle \mathfrak{p}_1\mathfrak{p}_2\rangle$, and $H_D^{\mathfrak{w}_{p_1,p_2}^e}$ is the square of a polynomial in $K[X]$ (resp. $\mathbb{Q}[X]$ if $H_D^{\mathfrak{w}_{p_1,p_2}^e} \in \mathbb{Q}[X]$).

Proof: We rely on Shimura's reciprocity law in the formulation of [Sch10, Th. 5.1.2]. Since p_1 and p_2 divide the level of $\mathfrak{w}_{p_1,p_2}^e$, we cannot use it directly; instead, we apply it twice for $\mathfrak{p}_1$ on the singular value $\mathfrak{w}_{p_2}^e(\tau)$. Recall from §1 that $\mathfrak{w}_{p_2}^e$ is modular of level $n = \frac{s}{\gcd(e,s)} p_2$ with $s = \frac{24}{\gcd(24,p_2-1)}$; the hypotheses of Theorem 1 imply that e is sufficiently large so that p_1 is coprime to the level of $\mathfrak{w}_1^e$. Since $N = p_1p_2$ divides C and p_1 does not divide c by assumption, τ is the basis quotient of the ideal $\mathfrak{a} = \begin{pmatrix} \frac{-B+\sqrt{D}}{2} \\ A \end{pmatrix}_{\mathbb{Z}}$, and $\frac{\tau}{p_1}$ is the basis quotient of $\mathfrak{a}\bar{\mathfrak{p}}_1 = \mathfrak{a}\mathfrak{p}_1 = \begin{pmatrix} \frac{-B+\sqrt{D}}{2} \\ p_1 A \end{pmatrix}_{\mathbb{Z}}$; the matrix $P_1 = \begin{pmatrix} 1 & 0 \\ 0 & p_1 \end{pmatrix}$ of determinant p_1 sends the former to the latter basis. By Shimura reciprocity, we have

$$\begin{aligned} \mathfrak{w}_{p_2}^e(\tau)^{\sigma(\mathfrak{p}_1)} &= \left(\mathfrak{w}_{p_2}^e \circ \left(p_1 P_1^{-1}\right)\right)(P_1\tau) = \left(\mathfrak{w}_{p_1}^e \circ S \circ P_1 \circ S\right)\left(\frac{\tau}{p_1}\right) \\ &= \left(\left(\sqrt{p_2}\,\frac{\eta(p_2 z)}{\eta(z)}\right)^e \circ P_1 \circ S\right)\left(\frac{\tau}{p_1}\right). \end{aligned}$$

The action of P_1 on $\sqrt{p_2}$ is given by multiplication by $\xi \in \{\pm 1\}$, and it is trivial on the rational q-expansion of $\frac{\eta(p_2 z)}{\eta(z)}$. Thus,

$$\mathfrak{w}_{p_2}^e(\tau)^{\sigma(\mathfrak{p}_1)} = \xi^e \mathfrak{w}_{p_2}^e\left(\frac{\tau}{p_1}\right) = \xi^e \frac{\mathfrak{w}_{p_2}^e(\tau)}{\mathfrak{w}_{p_1,p_2}^e(\tau)}.$$

A second application of $\sigma(\mathfrak{p}_1)$ and using $\mathfrak{p}_1^2 = (p_1)$ and $\xi^2 = 1$ yields

$$\mathfrak{w}_{p_2}^e(\tau)^{\sigma(p_1)} = \frac{\mathfrak{w}_{p_2}^e(\tau)}{\mathfrak{w}_{p_1,p_2}^e(\tau)\mathfrak{w}_{p_1,p_2}^e(\tau)^{\sigma(\mathfrak{p}_1)}}. \tag{11}$$

The action of $\sigma(p_1)$ is again computed by Shimura reciprocity as

$$\mathfrak{w}_{p_2}^e(\tau)^{\sigma(p_1)} = \left(\mathfrak{w}_{p_2}^e \circ \begin{pmatrix} p_1 & 0 \\ 0 & p_1 \end{pmatrix}\right)(\tau).$$

Notice that from the hypotheses of Theorem 1, we have $\gcd(p_1, n) = 1$. Bézout's relation between p_1 and n^2 yields a matrix $M \in \Gamma$ with $M \equiv \begin{pmatrix} p_1 & 0 \\ 0 & p_1^{-1} \end{pmatrix} \pmod n$, so that $\begin{pmatrix} p_1 & 0 \\ 0 & p_1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & p_1^2 \end{pmatrix} M \pmod n$. Then

$$\mathfrak{w}_{p_2}^e \circ \begin{pmatrix} p_1 & 0 \\ 0 & p_1 \end{pmatrix} = \mathfrak{w}_{p_2}^e \circ \begin{pmatrix} 1 & 0 \\ 0 & p_1^2 \end{pmatrix} \circ M = \mathfrak{w}_{p_2}^e \circ M = \left(\frac{p_1}{p_2'}\right)^e \mathfrak{w}_{p_2}^e \text{ by (4).}$$

Plugging this into (11) finishes the proof of the first formula of the theorem. The second formula is shown in the same way by exchanging the roles of p_1 and p_2, and the third one follows from quadratic reciprocity. Under the additional restrictions on e, p_1 and p_2, it immediately follows that $\mathfrak{w}_{p_1,p_2}^e(\tau)$ is invariant under $\sigma(\mathfrak{p}_1\mathfrak{p}_2)$.

The Galois automorphism $\sigma(\mathfrak{p}_1\mathfrak{p}_2)$ is non-trivial unless $(\mathfrak{p}_1\mathfrak{p}_2) \cap \mathcal{O}_D$ is principal. This can be checked using genus theory of non-maximal orders, or in an elementary fashion as follows: Write $|D| = p_1 p_2 r$ with $r \geqslant 1$. Then $(\mathfrak{p}_1\mathfrak{p}_2) \cap \mathcal{O}_D = \frac{t+v\sqrt{D}}{2}\mathcal{O}_D$ if and only if

$$p_1 p_2 = \frac{t^2 + v^2|D|}{4} = \frac{t^2 + v^2 p_1 p_2 r}{4} = p_1 p_2 \frac{s^2 p_1 p_2 + v^2 r}{4}$$

with $t = s p_1 p_2$. This happens exactly for $s = 0$, $v = 2$, $r = 1$, $|D| = p_1 p_2$; or $s = 0$, $v = 1$, $r = 4$, $|D| = 4p_1 p_2$. So excluding these cases, $\mathfrak{w}_{p_1,p_2}^e$ lies in the subfield of Ω_c of index 2 and of Galois group $\mathrm{Cl}(\mathcal{O}_D)/\langle \mathfrak{p}_1\mathfrak{p}_2 \rangle$ over K. □

For $k \geqslant 3$, the values of $\mathfrak{w}_{p_1,\ldots,p_{i-1},p_{i+1},\ldots,p_k}^e(\tau)^{\sigma(\mathfrak{p}_i)}$ and $\mathfrak{w}_{p_1,\ldots,p_k}(\tau)^{\sigma(\mathfrak{p}_i)}$ are computed in essentially the same way as in the proof of Theorem 5, but with ξ and the Legendre symbols dropped. This simplifies the argument and leads to fewer restrictions on e and the p_i:

Theorem 6 *Under the assumptions of Theorem 2, in particular $k \geqslant 3$, let $p_1, \ldots, p_k'$ for $2 \leqslant k' \leqslant k$ be ramified in K. Denoting by $\mathfrak{p}_i$ the ideal of the maximal order $\mathcal{O}_\Delta$ of K above p_i and by $\sigma(\mathfrak{p}_i)$ the associated Frobenius automorphism of Ω_c/K, we have*

$$\mathfrak{w}_{p_1,\ldots,p_k}^e(\tau)^{\sigma(\mathfrak{p}_i)} = \frac{1}{\mathfrak{w}_{p_1,\ldots,p_k}^e(\tau)} \text{ for } 1 \leqslant i \leqslant k'.$$

If k' is odd, or $|D| \notin \{p_1 \cdots p_{k'}, 4p_1 \cdots p_{k'}\}$, then $\mathfrak{w}_{p_1,\ldots,p_k}^e(\tau)$ lies in the subfield of index $2^{k'-1}$ of Ω_c which has Galois group $\mathrm{Cl}(\mathcal{O}_D)/\langle \{\mathfrak{p}_1\mathfrak{p}_j : 2 \leqslant j \leqslant k'\} \rangle$ over K. In particular, $H_D^{\mathfrak{w}_{p_1,\ldots,p_k}^e}$ is the $2^{k'-1}$-th root of a polynomial in $K[X]$ (resp. $\mathbb{Q}[X]$ if $H_D^{\mathfrak{w}_{p_1,\ldots,p_k}^e} \in \mathbb{Q}[X]$).

Proof: The action of $\sigma(\mathfrak{p}_i)$ is computed as above and implies that the singular value is invariant under all the $\sigma(\mathfrak{p}_1\mathfrak{p}_j)$ for $2 \leqslant j \leqslant k'$. The classes of these ideals generate a subgroup of the 2-torsion subgroup of $\mathrm{Cl}(\mathcal{O}_D)$. By the same argument as in the proof of Theorem 5, a product $\mathfrak{n}$ of several $\mathfrak{p}_1\mathfrak{p}_j$ is principal if and only if $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_{k'}$, which can only happen for even k', and $|D| \in \{\mathfrak{p}_1 \cdots \mathfrak{p}_{k'}, 4\mathfrak{p}_1 \cdots \mathfrak{p}_{k'}\}$. □

Corollary 7 *Under the assumptions of Corollary 4, let $k' \geqslant 1$ of the primes be ramified in $\mathcal{O}_D$. Then $\mathfrak{w}^e_{p_1,\ldots,p_k}(\tau_1)$ is a unit. For $k = 2$, if p_i is ramified (and p_{3-i} potentially not), then the constant coefficient of $H_D^{\mathfrak{w}_{p_1,p_2}}$ is $\left(\frac{p_i}{p'_{3-i}}\right)^{\frac{eh(\mathcal{O}_D)}{2}}$. Under the assumptions of Theorem 5, the constant coefficient of $\sqrt{H_D^{\mathfrak{w}_{p_1,p_2}}}$ is $\left(\frac{p_1}{p'_2}\right)^{\frac{eh(\mathcal{O}_D)}{4}}$. For $k \geqslant 3$, the constant coefficient of $H_D^{\mathfrak{w}^e_{p_1,\ldots,p_k}}$ is $+1$. Under the assumptions of Theorem 6 and $|D| \notin \{p_1 \cdots p_{k'}, 4p_1 \cdots p_{k'}\}$, the constant coefficient of $\sqrt[2^{k'-1}]{H_D^{\mathfrak{w}^e_{p_1,\ldots,p_k}}}$ is $+1$.*

Proof: Since $\mathfrak{a}_i$ and $\mathfrak{a}_i\mathfrak{p}_1$ are always inequivalent in $\mathrm{Cl}(\mathcal{O}_D)$, each conjugate $\mathfrak{w}^e_{p_1,\ldots,p_k}(\tau_i)$ occurs with its inverse (possibly up to sign if $k = 2$) by Theorems 5 and 6. This shows the unit property and the results on the constant coefficients of $H_D^{\mathfrak{w}_{p_1,p_2}}$ and $H_D^{\mathfrak{w}^e_{p_1,\ldots,p_k}}$. The constant coefficient of the 2-power root has the desired property as long as $\mathfrak{p}_1$ does not lie in the subgroup of $\mathrm{Cl}(\mathcal{O}_D)$ generated by $\mathfrak{p}_1\mathfrak{p}_2$ resp. the $\mathfrak{p}_1\mathfrak{p}_2, \ldots, \mathfrak{p}_1\mathfrak{p}_{k'}$, which holds under the additional assumptions. □

3.2 n-systems and reality of class polynomials, again

In the setting of Theorem 5, the class polynomial is the square of a polynomial with real coefficients, and we would like to identify the elements of an n-system leading to identical values, thus effectively cutting down the number of function evaluations to about $\frac{h(\mathcal{O}_D)}{4}$. We know by Theorem 5 that $\mathfrak{w}^e_{p_1,p_2}(\tau_{i_1}) = \mathfrak{w}^e_{p_1,p_2}(\tau_{i_1})^{\sigma(\mathfrak{p}_1\mathfrak{p}_2)}$. On the other hand, the proof that an n-system yields the algebraic conjugates of $\mathfrak{w}^e_{p_1,p_2}(\tau_{i_1})$ relies on the equation $\mathfrak{w}^e_{p_1,p_2}(\tau_{i_1})^{\sigma(\mathfrak{p}_1\mathfrak{p}_2)} = \mathfrak{w}^e_{p_1,p_2}(\tau_{i_2})$, where τ_{i_2} is the basis quotient of $\mathfrak{a}_{i_2} \sim \mathfrak{a}_{i_1}(\mathfrak{p}_1\mathfrak{p}_2)^{-1} \sim \mathfrak{a}_{i_1}\mathfrak{n}$. So $\mathfrak{a}_{i_1}$ and $\mathfrak{a}_{i_2}$ determine a double root of the class polynomial.

Using also Theorem 3, we see that if $\mathfrak{a}_{i_1}$, $\mathfrak{a}_{i_2} \sim \mathfrak{a}_{i_1}\mathfrak{n}$, $\mathfrak{a}_{i_3} \sim \mathfrak{a}_{i_1}^{-1}$ and $\mathfrak{a}_{i_4} \sim \mathfrak{a}_{i_1}^{-1}\mathfrak{n}$ correspond to four different elements of the n-system, that is, if they are pairwise inequivalent, then they yield twice the same pair of complex conjugate values. If $\mathfrak{a}_{i_1} \sim \mathfrak{a}_{i_3}$, that is, $\mathfrak{a}_{i_1}^2 \sim \mathcal{O}_D$, then $\mathfrak{a}_{i_1}$ and $\mathfrak{a}_{i_2} \sim \mathfrak{a}_{i_1}^{-1}\mathfrak{n}$ yield the same real value. If $\mathfrak{a}_{i_1} \sim \mathfrak{a}_{i_4}$, that is, $\mathfrak{a}_{i_1}^2 \sim \mathfrak{n}$, then again $\mathfrak{a}_{i_1}$ yields a real value by Theorem 3, and $\mathfrak{a}_{i_2}$ yields the same real value.

This argumentation carries over immediately to Theorem 6: For a given $\mathfrak{a}_{i_1}$, the $2^{k'-1}$ ideals of the n-system that are equivalent to one of $\mathfrak{a}_{i_1}(\mathfrak{p}_1\mathfrak{p}_2)^{e_2} \cdots (\mathfrak{p}_1\mathfrak{p}_{k'})^{e_{k'}}$ with $e_2, \ldots, e_{k'} \in \{0, 1\}$ lead to the same value of $\mathfrak{w}^e_{p_1,\ldots,p_k}$, so that the function needs to be evaluated essentially only $\frac{h(\mathcal{O}_D)}{2^{k'-1}}$ times. If k is even, complex conjugate values may again by identified using Theorem 3, and the number of function evaluations drops to about $\frac{h(\mathcal{O}_D)}{2^{k'}}$.

Yet another factor of 2 may be saved by exploiting the action of $\sigma(\mathfrak{p}_1)$. According to Theorems 5 and 6, if $\mathfrak{a}_{i_2} \sim \mathfrak{a}_{i_1}\mathfrak{p}_1$, then $\mathfrak{w}^e_{p_1,\ldots,p_k}(\tau_2) = \xi \frac{1}{\mathfrak{w}^e_{p_1,\ldots,p_k}(\tau_1)}$ with $\xi = 1$ for

$k \geqslant 3$ and $\xi = \left(\frac{p_1}{p_2'}\right)^e$ for $k = 2$. This cuts down the number of function evaluations to about $\frac{h(\mathcal{O}_D)}{2^{k'}}$, or even $\frac{h(\mathcal{O}_D)}{2^{k'+1}}$ when k is even and thus the class polynomial is real. In this optimal case, the $2^{k'+1}$ ideals of the n-system equivalent to $\mathfrak{a}_{i_1}^{e_0}\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_{k'}^{e_{k'}}$ with $e_0 \in \{\pm 1\}$ and $e_1, \ldots, e_{k'} \in \{0, 1\}$ lead to $2^{k'-1}$ times the same quadruple of two complex conjugate values and their (possibly negative) inverses, assuming that the ideals are pairwise inequivalent, which happens generically.

Even if only one of the primes is ramified, its explicit action gives useful information.

Corollary 8 *Under the assumptions of Corollary 4, let k be odd and p_1 ramified in $\mathcal{O}_D$. Then the class polynomial is real, and its complex conjugate roots may be identified by Theorem 3 with $\mathfrak{c} = \mathfrak{p}_1$.*

Proof: Let $\tau_0 = A_1\tau_1$ as in Theorem 3. By (8) and the action of $\sigma(\mathfrak{p}_1)$ according to Theorem 6 we have

$$\mathfrak{w}^e_{p_1,\ldots,p_k}|_N(\tau_0) = \frac{1}{\mathfrak{w}^e_{p_1,\ldots,p_k}(\tau_0)} = \mathfrak{w}^e_{p_1,\ldots,p_k}(\tau_0)^{\sigma(\mathfrak{p}_1)}.$$

□

3.3 Examples

Consider first $D = -455 = -5\cdot 7\cdot 13$. To simplify the presentation, we use in the following the notation of quadratic forms, identifying the ideal $\left(\begin{smallmatrix}\frac{-B+\sqrt{D}}{2}\\ A\end{smallmatrix}\right)_{\mathbb{Z}}$ with the quadratic form $[A, B, C]$, where $C = \frac{B^2-D}{4A}$. Let $\mathfrak{p}_1 = [5, 5, 24]$, $\mathfrak{p}_2 = [7, 7, 18]$ and $\mathfrak{z} = [2, 1, 57]$. Then $\mathrm{Cl}(\mathcal{O}_D) = \langle \mathfrak{p}_1, \mathfrak{z}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ with $\mathfrak{z}$ of order 10 and $\mathfrak{p}_2 \sim \mathfrak{z}^5$.

The function $\mathfrak{w}_{5,7}$ satisfies the conditions of Theorem 5 and is of level $n = 35$. A first element of a 35-system with C divisible by 35 is given by $\mathfrak{a}_1 = [1, 35, 420] \sim \mathcal{O}_D$. Then $\tau_1 = -17.5 + 10.66\ldots i$, and $z_1 = \mathfrak{w}_{5,7}(\tau_1) = -6.02\ldots$ is real. Since $\left(\frac{5}{7}\right) = -1$, we have another real conjugate $\frac{-1}{z_1}$ corresponding to $\mathfrak{p}_1$, and the same two values reoccur for $\mathfrak{p}_1\mathfrak{p}_2 \sim \mathfrak{p}_1\mathfrak{z}^5$ and $\mathfrak{p}_1(\mathfrak{p}_1\mathfrak{p}_2) \sim \mathfrak{z}^5$.

The not yet covered ideal $\mathfrak{z}$ is equivalent to $\mathfrak{a}_2 = [2, 105, 1435]$ in the same 35-system, yielding $\tau_2 = -26.25 + 5.33\ldots i$ and $z_2 = \mathfrak{w}_{5,7}(\tau_2) = 0.65\ldots - 2.05\ldots i$. We then obtain twice the values z_2, $\bar{z}_2$, $\frac{-1}{z_2}$ and $\frac{-1}{\bar{z}_2}$, corresponding to the ideals $\mathfrak{z}$, $\mathfrak{p}_1\mathfrak{z}^4$, $\mathfrak{p}_1\mathfrak{z}$, $\mathfrak{z}^4$, and the second time to $\mathfrak{p}_1\mathfrak{z}^6$, $\mathfrak{z}^9$, $\mathfrak{z}^6$, $\mathfrak{p}_1\mathfrak{z}^9$, respectively.

Finally, $\mathfrak{p}_1\mathfrak{z}^2$ has not occurred yet; it is equivalent to $\mathfrak{a}_3 = [3, 175, 2590]$ in the 35-system with $\tau_3 = -29.16\ldots + 3.55\ldots i$ and yields twice the conjugates $z_3 = \mathfrak{w}_{5,7}(\tau_3) = 1.50\ldots - 0.53\ldots i$, $\bar{z}_3$, $\frac{-1}{z_3}$ and $\frac{-1}{\bar{z}_3}$.

Let $x_i = \Re(z_i)$ and $n_i = z_i\bar{z}_i$, and define g_i to be the polynomial with coefficients in $\mathbb{R}$ whose roots are the conjugates related to z_i. Then $g_1 = X^2 - \left(z_1 - \frac{1}{z_1}\right)X - 1$ and

$g_i = X^4 + 2x_i \left(\frac{1}{n_i} - 1\right)(X^3 - X) + \left(n_i + \frac{1-4x_i^2}{n_i}\right) + 1$ for $i \in \{2, 3\}$. Multiplying g_1, g_2 and g_3 and rounding the resulting coefficients to integers, we obtain

$$\sqrt{H_{-455}^{\mathfrak{w}_{5,7}}} = X^{10} + 3X^9 - 12X^8 + 32X^7 - 38X^6 - 17X^5 + 38X^4 + 32X^3 + 12X^2 + 3X - 1.$$

Notice the constant coefficient -1 as predicted by Corollary 7.

As an example with more ramified primes, let us consider $D = -3795 = -3 \cdot 5 \cdot 11 \cdot 23$, which is divisible by 3, and all other prime factors of which are congruent to -1 modulo 3. Its class group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If we wish to use a multiple η-quotient whose level is composed of only ramified primes, then Theorems 1 and 2 imply that we need to add an exponent of 3. By including three of the four prime factors of D, we may then gain a factor of 4 in the degree. For instance, one computes

$$\sqrt[4]{H_{-3795}^{\mathfrak{w}_{3,5,11}^3}} = X^4 - 200596X^3 - 511194X^2 - 200596X + 1.$$

Alternatively, we may add a split prime congruent to $+1$ modulo 3 to the level of the η-quotient, which enables us to drop the exponent 3. This will generally result in a smaller polynomial:

$$\sqrt[4]{H_{-3795}^{\mathfrak{w}_{3,5,11,19}}} = X^4 - 46X^3 + 2115X^2 - 46X + 1.$$

It should be noted that the singular values of the multiple η-quotients do not necessarily *generate* the subfields indicated in Theorems 5 and 6. Using the split prime 13 instead of 19 above yields

$$\sqrt[4]{H_{-3795}^{\mathfrak{w}_{3,5,11,13}}} = X^4 + 92X^3 + 2118X^2 + 92X + 1 = (X^2 + 46X + 1)^2;$$

apparently, the prime ideals of $\mathcal{O}_D$ above 13 and 19 act differently on the respective η-quotient, although they are all of order 4 in the class group.

4 Other functions on $X_0^+(N)$ in the totally ramified case

Shimura reciprocity relates the Galois action on singular values to actions on modular functions and their arguments. In §3 we used the precise shape of the multiple η-quotients to show invariance results when two or more of the prime factors are ramified. We may consider in more generality functions on $X_0^+(N)$, that is, functions invariant under $\Gamma^0(N)$ and the Fricke–Atkin–Lehner involution $|_N$. Assuming less knowledge about the function, we will make the stronger hypothesis on the imaginary-quadratic field that *all* prime divisors of N are ramified and consider the image under the Artin map of the product of all ramified prime ideals. Under similar technical conditions as before, one can then show that the singular values lie in a subfield of index 2 of the ring class field.

Theorem 9 *Let D be a quadratic discriminant of conductor c and let N be square-free, prime to c and such that $N \mid D$ and $|D| \notin \{N, 4N\}$. Then there is a primitive quadratic form $[A_1, B_1, C_1]$ of discriminant D such that $C_1 = N$ and $N \mid B_1$. Let $\mathfrak{n} = \begin{pmatrix} \frac{-B_1+\sqrt{D}}{2} \\ A_1 \end{pmatrix}$ be the ideal of basis quotient τ_1 associated to this quadratic form. Then $\mathfrak{n}$ is of order 2 in $\mathrm{Cl}(\mathcal{O}_D)$.*

Let f be a modular function for $\Gamma^0(N)$ such that f and $f \circ S$ have a rational q-expansion, and such that $f|_N = f$. Then the singular value $f(\tau_1)$ lies in the subfield of index 2 of Ω_c with Galois group $\mathrm{Cl}(\mathcal{O}_D)/\langle\mathfrak{n}\rangle$. The class polynomial $\sqrt{H_D^f}$ is real and can be computed from an N-system in which $\mathfrak{a}_i$ and $\mathfrak{a}_i\mathfrak{n}$ yield the same root, and $\mathfrak{a}_i^{-1}$ and $\mathfrak{a}_i^{-1}\mathfrak{n}$ yield the complex conjugate root.

Proof: Since all primes dividing N are not inert, there is a quadratic form with $C_1 = N$. As N divides D and is square-free, it follows that $N \mid B_1$ and that all primes dividing N are ramified. The ideal $\mathfrak{n}$ is equivalent to the ideal of norm N; it is non-principal by the same argument as in the proof of Theorem 5.

[Sch02, Th. 4], given in the beginning of §2.1, implies that $f(\tau_1) \in \Omega_c$. Let $[A_i, B_i, C_i]$ be an N-system, associated to the ideals $\mathfrak{a}_i$ of basis quotients τ_i. The class polynomial H_D^f is real by Theorem 3; precisely, the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_i^{-1}\mathfrak{n}$ yield complex conjugate roots. Now,

$$f(\tau_i) = f|_N(\tau_i) = f\left(\frac{-N}{\tau_i}\right) = f\left(\frac{B_i + \sqrt{D}}{2C_i/N}\right) = f(\tau_j),$$

where τ_j is a root of the quadratic form $[C_i/N, -B_i, A_i N]$ of discriminant D. From the N-system condition and $N \mid B_1$ we have $N \mid B_i$ and $-B_i \equiv B_i \pmod{2N}$. Moreover, $\gcd(C_i/N, N) = 1$ since $N \mid B_i$, $N \mid C_i$ and N is coprime with c. So the form is primitive and can be assumed to occur as an element of the N-system, associated to an ideal $\mathfrak{a}_j \sim \mathfrak{a}_i\mathfrak{n}$. Since $\mathfrak{n}$ is not principal, $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are not equivalent and correspond to different elements of the N-system. □

Applied to multiple η-quotients, Theorem 9 is weaker than Theorem 5 (which also considers powers of $\mathfrak{w}_{p_1,p_2}$ of lower exponent $e < s$, for which the function is of level $\frac{s}{e}N$ instead of N) and Theorem 6 (which treats the case that only some primes are ramified). Its interest lies in its application to other functions invariant under the Fricke–Atkin–Lehner involution. In particular, it was suggested in [Mor09] to consider such functions A_p of prime level p and of (conjectured) minimal degree, as are used inside the Schoof–Elkies–Atkin algorithm for point counting on elliptic curves [Elk98, Mor95]. It was observed in [Mor09] that A_{71} yields an asymptotic gain in the logarithmic height of the class polynomial, compared to the polynomial for the j-invariant, by a factor of 36 as $|D| \to \infty$; families of functions with a conjectured asymptotic gain of at least a factor of 30 are given in [ES10]. Using ramified primes has a double advantage: Not only is the degree of the class polynomial divided by 2, but also the coefficients of the polynomial have about half as many digits.

5 Class field theoretic remarks

The main algorithmic use of class polynomials is the computation of elliptic curves over some finite field $\mathbb{F}$ with a given endomorphism ring $\mathcal{O}_D$. If such curves exist, the class polynomial H_D^f splits completely in $\mathbb{F}[X]$; for each root $\bar{f}$, there is an elliptic curve over $\mathbb{F}$ with complex multiplication by $\mathcal{O}_D$. To compute such a curve, one considers the modular polynomial $\Psi_f(f, j)$, the minimal polynomial of f over $\mathbb{C}(j)$, which is in fact an element of $\mathbb{Z}[f, j]$ for all functions considered in this article. So one may reduce the polynomial to an element of $\mathbb{F}[f, j]$, specialise f as $\bar{f}$ and compute all the roots $\bar{j} \in \mathbb{F}$. For all these roots, of which there may be several, one writes down an elliptic curve over $\mathbb{F}$ with j-invariant $\bar{j}$ and checks whether its endomorphism ring is indeed $\mathcal{O}_D$ as desired. For this application, it is clearly computationally advantageous to compute only $\sqrt[2^{k'-1}]{H_D^f}$.

If one wishes to obtain the full class field Ω_c, one may use the subfield $L = K(x) = K[X]/\left(\sqrt[2^{k'-1}]{H_D^f(X)}\right)$ (assuming the polynomial is irreducible, which need not be the case, see the example in §3.3), as a first step in a tower of field extensions. To this purpose, one may factor the modular polynomial $\Psi_f(x, Y)$ over L. It necessarily has an irreducible factor of degree $2^{k'-1}$, which generates Ω_c/L. In general, this polynomial factorisation step over a number field will be more costly than switching to a different class invariant that directly generates Ω_c. For a few functions of low level, however, the degree d_j of Ψ_f in j is exactly 2^{k-1}, and no factorisation is needed for a discriminant for which all primes dividing N are ramified. For $k = 2$, a degree $d_j = 2$ is obtained if and only if $(p_1 - 1)(p_2 - 1) \mid 24$ by [ES05, Th. 9], that is, for $\{p_1, p_2\} \in \big\{\{2,3\},\{2,5\},\{2,7\},\{2,13\},\{3,5\},\{3,7\},\{3,13\},\{5,7\}\big\}$. Conjecturally, for $k \geqslant 3$ we have $d_j = 2^{k-1}$ if and only if $(p_1 - 1)\cdots(p_k - 1) \mid 24$, that is, for $\{p_1, \ldots, p_k\} \in \big\{\{2,3,5\},\{2,3,7\},\{2,3,13\},\{2,5,7\}\big\}$. Computing the polynomials via the algorithm of [Eng09] shows that the condition is at least sufficient, and that the smallest function with $k = 4$, $\mathfrak{w}_{2,3,5,7}$, has $d_j = 16 > 2^3$. A top-down approach to obtain the class field as a tower of field extensions, starting with a generating element of Ω_c, is described in [HM01, EM03]. The lucky case $d_j = 2^{k-1}$ can be seen as a bottom-up approach, in which moreover the second stage is realised by the universal modular polynomial independently of the concrete class field under consideration.

It may also be possible to construct the missing part of Ω_c classically using genus theory. Suppose that $\sqrt[2^{k'-1}]{H_D^f(X)}$ is irreducible. Let $H = \langle\{\mathfrak{p}_1\mathfrak{p}_j : 2 \leqslant j \leqslant k'\}\rangle$, and assume that $\mathrm{Cl}(\mathcal{O}_D)$ is the direct product of $\mathrm{Cl}(\mathcal{O}_D)/H$ and H, which happens if and only if H contains no element that is a square in $\mathrm{Cl}(\mathcal{O}_D)$. Then Ω_c is the compositum of L and the genus field of K.

For instance, consider the first example of §3.3, where $D = -5 \cdot 7 \cdot 13$ and L/K is generated by $\sqrt{H_{-455}^{\mathfrak{w}_{5,7}}}$. A quick computation with Pari/GP [Bel12] shows that $L \ni \sqrt{13}$, but $L \not\ni \sqrt{5}$, so that $\Omega_c = L(\sqrt{5}) = L(\sqrt{-7})$.

However, the singular values of the multiple η-quotients do not necessarily generate the Hilbert class field of a fundamental discriminant over the genus field. For $D = -3 \cdot 5 \cdot 11 \cdot 23$ and L/K generated by $\sqrt[4]{H_{-3795}^{\mathfrak{w}_{3,5,11,19}}}$, one has $L \ni \sqrt{-3}, \sqrt{-11}$, and $L(\sqrt{5}) = L(\sqrt{-23})$ still has index 2 in Ω_c.

References

[Bel12] Karim Belabas et al. *PARI/GP*. Bordeaux, 2012. Version 2.5.3, `http://pari.math.u-bordeaux.fr/`.

[Elk98] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin*, volume 7 of *Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, 1998.

[EM03] Andreas Enge and François Morain. Fast decomposition of polynomials with known Galois group. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes — AAECC-15*, volume 2643 of *Lecture Notes in Computer Science*, page 254–264, Berlin, 2003. Springer-Verlag.

[EM09] Andreas Enge and François Morain. Generalised Weber functions. I. Technical Report 385608, HAL-INRIA, 2009. `http://hal.inria.fr/inria-00385608`.

[Eng09] Andreas Enge. Computing modular polynomials in quasi-linear time. *Mathematics of Computation*, 78(267):1809–1824, 2009.

[ES04] Andreas Enge and Reinhard Schertz. Constructing elliptic curves over finite fields using double eta-quotients. *Journal de Théorie des Nombres de Bordeaux*, 16:555–568, 2004.

[ES05] Andreas Enge and Reinhard Schertz. Modular curves of composite level. *Acta Arithmetica*, 118(2):129–141, 2005.

[ES10] Andreas Enge and Andrew V. Sutherland. Class invariants by the CRT method. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory — ANTS-IX*, volume 6197 of *Lecture Notes in Computer Science*, page 142–156, Berlin, 2010. Springer-Verlag.

[HM01] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In Bernard Mourrain, editor, *ISSAC 2001 — Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 175–182, New York, 2001. Association for Computing Machinery.

[Mor95] François Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques. *Journal de Théorie des Nombres de Bordeaux*, 7(1):111–138, 1995.

[Mor09] F. Morain. Advances in the CM method for elliptic curves, 2009. Slides of Fields Cryptography Retrospective Meeting, May 11-15, `http://www.lix.polytechnique.fr/~morain/Exposes/fields09.pdf`.

[Sch02] Reinhard Schertz. Weber's class invariants revisited. *Journal de Théorie des Nombres de Bordeaux*, 14(1):325–343, 2002.

[Sch10] Reinhard Schertz. *Complex Multiplication*. Cambridge University Press, 2010.