MODULARITY OF GALOIS TRACES OF CLASS INVARIANTS

DAEYEOL JEON, SOON-YI KANG AND CHANG HEON KIM

Abstract. Zagier showed that the Galois traces of the values of j-invariant at CM points are Fourier coefficients of a weakly holomorphic modular form of weight 3/2 and Bruinier-Funke expanded his result to the sums of the values of arbitrary modular functions at Heegner points. In this paper, we identify the Galois traces of real-valued class invariants with modular traces of the values of certain modular functions at Heegner points so that they are Fourier coefficients of weight 3/2 weakly holomorphic modular forms.

1. Introduction and the statement of results

Let τ be a value in the complex upper half plane $\mathbb{H}$ and $q = e^{2\pi i\tau}$. Then the classical modular j-invariant on $SL_2(\mathbb{Z})$ is defined by

$$j(\tau) = \frac{\left(1 + 240\sum_{n=1}^{\infty}\sum_{m|n} m^3 q^n\right)^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}} = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$$

and its value at an imaginary quadratic generates an abelian extension of an imaginary quadratic number field. For positive integer D satisfying $D \equiv 0,\ 3 \pmod 4$, we let

$$\tau_D := \begin{cases} \frac{\sqrt{-D}}{2}, & \text{if } D \equiv 0 \pmod 4, \\ \frac{-1+\sqrt{-D}}{2}, & \text{if } D \equiv 3 \pmod 4. \end{cases} \tag{1.1}$$

Then $j(\tau_D)$ generates the *ring class field* H_D over the imaginary quadratic field $K = \mathbb{Q}(\tau_D)$ with degree $[H_D : K] = h(-D)$, the class number of the order $\mathcal{O}_D = \mathbb{Z}[\tau_D]$ of K. The Galois conjugates of $j(\tau_D)$ under the action of $Gal(H_D/K)$ are *singular moduli* $j(\tau_Q)$, where

$$\tau_Q := \frac{-b+\sqrt{-D}}{2a} \tag{1.2}$$

is a CM point that is a unique root of $Q(x,1) = 0$ in $\mathbb{H}$, where

$$Q(x,y) = [a,b,c] = ax^2 + bxy + cy^2$$

is a positive definite integral primitive binary quadratic form with discriminant $-D = b^2 - 4ac$ and the sum of these conjugates is an ordinary integer.

In order to give a nice analytic property to the sum of singular moduli $j(\tau_Q)$, we allow imprimitive quadratic forms and count them with multiplicities $1/|\Gamma(1)_Q|$, where $\Gamma(1)_Q$ is the stabilizer of Q by $\Gamma(1) := PSL_2(\mathbb{Z})$. Let $\mathcal{Q}_D$ denote the set of positive definite integral binary quadratic forms of discriminant $-D$ with the usual action of the modular group $\Gamma(1)$. Following

D. Zagier, we define the modified trace of the Hauptmodul $J(\tau) = j(\tau) - 744$ for index D as

$$\mathbf{t}_J(D) := \sum_{Q \in \mathcal{Q}_D/\Gamma(1)} \frac{J(\tau_Q)}{|\Gamma(1)_Q|}. \tag{1.3}$$

In general, this modified trace is not a Galois trace but a sum of traces that we may write ([17, Section 2]) as

$$\mathbf{t}_J(D) = \sum_{\mathcal{O} \supseteq \mathcal{O}_D} \frac{2}{\omega_{\mathcal{O}}} \sum_{[\mathfrak{a}_{\mathcal{O}}]} J(\mathfrak{a}_{\mathcal{O}}), \tag{1.4}$$

where the first sum runs over all imaginary quadratic orders $\mathcal{O}$ that contain the order $\mathcal{O}_D$ of discriminant $-D$, $\omega_{\mathcal{O}}$ is the number of units in $\mathcal{O}$, and the second sum runs over representatives of the proper $\mathcal{O}$-ideal class. The corresponding generalized class polynomial is then given by [28],

$$\mathcal{H}_D(X) := \prod_{Q \in \mathcal{Q}_D/\Gamma(1)} (X - j(\tau_Q))^{1/|\Gamma(1)_Q|} \tag{1.5}$$

and its q-expansion at $j(\tau)$ is ([28, Eq. (11)])

$$\mathcal{H}_D(j(\tau)) = q^{-H(D)}(1 - \mathbf{t}_J(D)q + O(q^2)), \tag{1.6}$$

where $H(D)$ is the *Hurwitz-Kronecker class number.* If $-D < -4$ is a fundamental discriminant, then $\mathbf{t}_J(D)$ and $\mathcal{H}_D(X)$ are indeed the Galois trace and Hilbert class polynomial, respectively. For example,

$$\mathcal{H}_{23}(X) = X^3 + 3491750X^2 - 5151296875X + 12771880859375 \in \mathbb{Z}[X] \tag{1.7}$$

and $\mathbf{t}_J(23) = -3491750$, the Galois trace of $J(\tau_{23})$.

One of the significant properties of the modified trace is that they are Fourier coefficients of a certain weakly holomorphic modular form of weight 3/2 on $\Gamma_0(4)$ [28]. This discovery of Zagier inspired a great number of works on traces of singular values (see [20, Section 13.1] for references). In particular, J. H. Bruinier and J. Funke [5] showed that the modular traces of the values of an arbitrary modular function at Heegner points are Fourier coefficients of the holomorphic part of a harmonic weak Maass form of weight 3/2 and Bruinier, P. Jenkins, and K. Ono [6] and W. Duke [10] derived exact formulas of traces of $J_m(z) := mJ(z)|T_m$, where T_m is the weight zero m-th Hecke operator, which lead to exact formulas for Hilbert class polynomials.

It is known that the value of every modular function for any congruence subgroup at an imaginary quadratic lies in a finite abelian extension of an imaginary quadratic field, the so called *ray class field.* While the Zagier-Bruinier-Funke modular trace of the value of a modular function at a Heegner point is naturally its Galois trace, it is not trivial to see whether the Galois trace of a given algebraic integer is a modular trace and hence a Fourier coefficient of a certain automorphic form. However, if we restrict our attention to a modular function whose value at a CM point generates a ring class field of an imaginary quadratic field, we can make use of Shimura's reciprocity law to relate the Galois trace with the modular trace. Following H. Weber [26], we call the value of a modular function $f(\tau_D)$ a *class invariant* if we have

$$K(f(\tau_D)) = K(j(\tau_D)).$$

The Shimura reciprocity law [24] provides a method of systematically determining whether $f(\tau_D)$ is a class invariant as well as a description of the Galois conjugates of $f(\tau_D)$ under the action of $Gal(H_D/K)$ in terms of the action of the form class group. This tool is well-illustrated in several works by R. M. Bröker, A. Gee, and P. Stevenhagen in [4], [11], [12], [13], [25].

In this paper, we identify the Galois traces of several class invariants whose minimal polynomials have integer coefficients with modular traces of the values of certain modular functions at Heegner points so that they are Fourier coefficients of weight 3/2 weakly holomorphic modular forms. We begin with the holomorphic cube root $\gamma_2 : \mathbb{H} \to \mathbb{C}$ of the j-function and a modular function $\mathfrak{f}_2 : \mathbb{H} \to \mathbb{C}$ of level 48. The function values $\zeta_3\gamma_2(\tau_{23})$ and $\zeta_{48}\mathfrak{f}_2(\tau_{23})$ are both class invariants and these values have minimal polynomials

$$\mathcal{H}_{23}^{\zeta_3\gamma_2}(X) = X^3 + 155X^2 + 650X + 23375 \in \mathbb{Z}[X]$$

and

$$\mathcal{H}_{23}^{\zeta_{48}\mathfrak{f}_2}(X) = X^3 - X - 1 \in \mathbb{Z}[X].$$

Compared with the Hilbert class polynomial in (1.7), the minimal polynomials of class invariants above produce much smaller coefficients.

The holomorphic cube root γ_2 of j is a modular function of level 3. It is well known that if $D > 4$ and $3 \nmid D$ and if $B = 0$ for D even and $B = 1$ otherwise, then $\zeta_3^B\gamma_2(\tau_D)$ is a class invariant. Using the Shimura reciprocity, we deduce the following theorem.

Theorem 1.1. *Suppose $-D$ is an imaginary quadratic discriminant such that $3 \nmid D$. We let $\tau_D = \frac{-B+\sqrt{-D}}{2}$ as defined in (1.1) and let $\tau_Q = \frac{-b+\sqrt{-D}}{2a}$ be the CM point associated with a primitive quadratic form $Q = [a, b, c]$ of discriminant $-D$. The action of the form class group on $\zeta_3^B\gamma_2(\tau_D)$ is given by the formula*

$$(\zeta_3^B\gamma_2(\tau_D))^{[a,-b,c]} = \begin{cases} \zeta_3^{ab}\gamma_2(\tau_Q), & \text{if } 3 \nmid a, \\ \zeta_3^{-bc}\gamma_2(\tau_Q), & \text{if } 3 \mid a \text{ and } 3 \nmid c, \\ \gamma_2(\tau_Q), & \text{if } 3 \mid a \text{ and } 3 \mid c. \end{cases} \tag{1.8}$$

Of the three cases in (1.8), we are particularly interested in the last, where both a and c are multiples of 3, and discriminant $-D$ is congruent to a square modulo 36. In general, for $-D$ that is congruent to a square modulo $4N^2$ and β modulo $2N^2$, we let

$$\mathcal{Q}_{D,(N),\beta} = \{[Na, b, Nc] \in \mathcal{Q}_D \mid b \equiv \beta \pmod{2N^2}\} \tag{1.9}$$

on which $\Gamma_0^0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \mid b \equiv c \equiv 0 \pmod N\}$ acts. Then the associated Heegner points are of the form $\tau_Q = \dfrac{-b+\sqrt{-D}}{2aN}$ and τ_D is not a Heegner point unless $N = 1$. If $p^2 \nmid -D$ for any prime divisor p of N, then there is a canonical bijection between $\mathcal{Q}_D/\Gamma(1)$ and $\mathcal{Q}_{D,(N),\beta}/\Gamma_0^0(N)$, as to be shown later in Lemma 5.1. Let $\mathrm{GT}_f(D)$ denote the modified Galois trace of a class invariant $f(\tau_D)$. By means of Theorem 1.1, the modified Galois trace of $\zeta_3^B\gamma_2(\tau_D)$ for discriminant $-D$ which is congruent to a square modulo 36 but not divisible by 3 is given by

$$\mathrm{GT}_{\zeta_3^B\gamma_2}(D) = \sum_{Q \in \mathcal{Q}_{D,(3),\beta}/\Gamma_0^0(3)} \gamma_2(\tau_Q). \tag{1.10}$$

The sum of the traces given on the right-hand side of equation (1.10) is a constant multiple of the Bruinier-Funke modular trace of γ_2 at a Heegner point. To state the relation more precisely, we introduce some notations. For a weakly holomorphic modular function f on a level N congruence subgroup Γ, we consider a lattice L such that the group Γ acts with finitely many orbits on $L_{h,m} := \{X \in L + h \,|\, q(X) = m\}$, where h is in the dual lattice of L, $m \in \mathbb{Q}_{>0}$, and $q(X) := \det(X)$. We denote the modular trace function of f for positive index m with respect to L by $\mathrm{MT}_f^L(h, m)$. If we use the lattice

$$L_1 = \left\{ X = \begin{pmatrix} b & 2Nc \\ 2Na & -b \end{pmatrix} \middle| a, b, c \in \mathbb{Z} \right\} \tag{1.11}$$

with $q(X) = \det(X)$ and the associated bilinear form $(X, Y) := -\mathrm{tr}(XY)$ in the construction of the Bruinier-Funke modular trace and apply some properties of the function γ_2, we obtain the following theorem.

Theorem 1.2. *For imaginary quadratic discriminant $-D$ which is congruent to a square modulo 36 and not divisible by 3,*

$$\mathrm{GT}_{\zeta_3^B \gamma_2}(D) = \frac{1}{4}\mathrm{MT}_{\gamma_2}^{L_1}(0, D). \tag{1.12}$$

Moreover, the generating series of $\mathrm{GT}_{\zeta_3^B \gamma_2}(D)$,

$$q^{-1} + \sum_{\substack{D>0 \\ -D \equiv \square \pmod{36}}} \mathrm{GT}_{\zeta_3^B \gamma_2}(D) q^D$$

is a weakly holomorphic modular form of weight $3/2$ on $\Gamma_0(36)$.

Example 1. *Let $-D = -23 \equiv 7^2 \pmod{36}$ and $\beta = 7$. Then $\mathcal{Q}_{23}/\Gamma(1)$ is given by*

$$\mathcal{Q}_{23}/\Gamma(1) = \{[1, 1, 6], [2, 1, 3], [2, -1, 3]\}$$

and thus the Galois trace of $j(\tau_{23})$ is $j(\tau_{[1,1,6]}) + j(\tau_{[2,1,3]}) + j(\tau_{[2,-1,3]})$. By Theorem 1.1, we find that the Galois trace of $\zeta_3\gamma_2(\tau_{23})$ is equal to

$$\zeta_3\gamma_2(\tau_{[1,1,6]}) + \zeta_3^2\gamma_2(\tau_{[2,1,3]}) + \zeta_3^{-2}\gamma_2(\tau_{[2,-1,3]}).$$

However, by the discussion above and the fact

$$\mathcal{Q}_{23,(3),7}/\Gamma_0^0(3) = \{[6, 25, 27], [9, 25, 18], [3, 7, 6]\},$$

we may also write the Galois trace of $\zeta_3\gamma_2(\tau_{23})$ as

$$\gamma_2(\tau_{[6,25,27]}) + \gamma_2(\tau_{[9,25,18]}) + \gamma_2(\tau_{[3,7,6]})$$

so that the corresponding minimal polynomial has Heegner divisors:

$$\mathcal{H}_{23}^{\zeta_3\gamma_2}(X) = \prod_{Q \in \mathcal{Q}_{23,(3),7}/\Gamma_0^0(3)} (X - \gamma_2(\tau_Q)) \tag{1.13}$$

Likewise as above, we discover similar results for the Weber functions $\mathfrak{f}$ and $\mathfrak{f}_2$ of level 48.

Theorem 1.3. *For imaginary quadratic discriminant $-D$ which is congruent to a square modulo* 9216 *but not divisible by* 2 *or* 3*,*

$$\mathrm{GT}_{\zeta_{48}\mathfrak{f}_2}(D) = \frac{1}{8}\mathrm{MT}_{\mathfrak{f}}^{L_1}(0, D).$$

Moreover, there is a finite principal part $A(\tau) = \sum_{n\leq 0} a(n)q^n$ for which

$$A(\tau) + \sum_{\substack{D>0 \\ -D\equiv\square \pmod{9216}}} \mathrm{GT}_{\zeta_{48}\mathfrak{f}_2}(D)q^D$$

is a weakly holomorphic modular form of weight $3/2$ *on* $\Gamma_0(9216)$.

There are generalized Weber functions $\mathfrak{g}_0$, $\mathfrak{g}_1$, $\mathfrak{g}_2$ and $\mathfrak{g}_3$ of level 72. For these functions, we choose the lattice

$$L_2 = \left\{ X = \begin{pmatrix} Nb & c \\ a & -Nb \end{pmatrix} \Big| a, b, c \in \mathbb{Z} \right\} \tag{1.14}$$

with $q(X) = \det(X)$ and $(X, Y) = -\mathrm{tr}(XY)$ that yields

Theorem 1.4. *If the imaginary quadratic discriminant $-D$ is congruent to a square modulo* 20736 *and $-D \equiv 1 \pmod{12}$, then $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_D)$ is a real-valued class invariant. And for a fixed value $\beta \pmod{10368}$ such that $\beta^2 \equiv -D \pmod{20736}$, we have*

$$\mathrm{GT}_{\mathfrak{g}_0^6+\mathfrak{g}_1^6}(D) = \begin{cases} \mathrm{MT}_{\mathfrak{g}_0^6}^{L_2}(\beta, D/20736), & \text{if } \beta \equiv 7 \pmod{12}, \\ \mathrm{MT}_{\mathfrak{g}_3^6}^{L_2}(\beta, D/20736), & \text{if } \beta \equiv 5 \pmod{12}. \end{cases}$$

Moreover, there is a finite principal part $B(\tau) = \sum_{n\leq 0} b(n)q^n$ for which

$$B(\tau) + \sum_{\substack{D>0 \\ -D\equiv\square \pmod{20736}}} GT_{\mathfrak{g}_0^6+\mathfrak{g}_1^6}(D)q^{D/20736}$$

is a weakly holomorphic modular form of weight $3/2$ *on* $\Gamma(20736)$.

The organization of this paper is as follows. In Section 2, we summarize Bruinier-Funke's construction of a modular trace and illustrate with examples of two lattices that it is a sum of Zagier type modified traces that depends on the choice of a lattice. In Section 3, we introduce several class invariants whose minimal polynomials have integral coefficients, then in Section 4, we compute the Galois conjugates of the class invariants presented in Section 3. With the material presented up to this point, we provide proofs for our results on a cube root of j-function and the Weber functions of level 48 in Section 5 and in Section 6, we do the same for a new class invariant of level 72 whose minimal polynomial also has integral coefficients. Finally, we give a conjectural statement on relation between Galois traces and modular traces in Section 7.

2. Modular trace of a weakly holomorphic modular function

In this section, we state Bruinier and Funke's generalization of Zagier's traces of singular moduli to the traces of the values at CM points of modular functions on groups of arbitrary genus. The main tool of their proof for modularity of their traces of singular moduli is the Kudla-Milson theta lift [5]. But we do not discuss anything on theta-lift but briefly recall the definition of their modular traces for positive index and prove a couple of lemmas that will be used later.

We consider the quadratic space (V, q) over $\mathbb{Q}$ of signature $(1, 2)$ given by the trace zero 2×2 matrices with the quadratic form $q(X) = \det(X)$ and the associated bilinear form $(X, Y) = -\mathrm{tr}(XY)$. We assume the discriminant of (V, q) is 1. The group $SL_2(\mathbb{Q})$ acts on V by conjugation $g \cdot X := gXg^{-1}$ for $X \in V$ and $g \in SL_2(\mathbb{Q})$. By assigning each point $z = x + iy \in \mathbb{H}$ the positive line spanned by

$$X(z) := \frac{1}{y}\begin{pmatrix} -\frac{1}{2}(z+\bar{z}) & z\bar{z} \\ -1 & \frac{1}{2}(z+\bar{z}) \end{pmatrix},$$

we identify the complex upper half-plane $\mathbb{H}$ with the space of lines in $V(\mathbb{R})$ on which the quadratic form q is positive definite. Note that $q(X(z)) = 1$ and $g \cdot X(z) = X(gz)$ for $g \in SL_2(\mathbb{R})$. Then the CM points can be defined as $D_X = \mathrm{span}(X)$ for $X \in V(\mathbb{Q})$ of positive norm so that the corresponding point in $\mathbb{H}$ satisfies a quadratic equation over $\mathbb{Q}$.

Let $L \subset V(\mathbb{Q})$ be an even lattice of full rank and write $L^{\#}$ for the dual lattice of L. If Γ denotes a congruence subgroup of $\mathrm{Spin}(L)$ which preserves L and acts trivially on the discriminant group $L^{\#}/L$.

We now define the modular trace function of a weakly holomorphic modular form of weight 0 with respect to Γ. Since the stabilizer S_X of X in $SL_2(\mathbb{R})$ is isomorphic to $SO(2)$ which is compact, $\Gamma_X = S_X \cap \Gamma$ is finite. For $m \in \mathbb{Q}_{>0}$ and $h \in L^{\#}$, the group Γ acts on

$$L_{h,m} = \{X \in L + h \mid q(X) = m\}$$

with finitely many orbits. We define the *Heegner divisor* of discriminant m on the modular curve $\Gamma\backslash\mathbb{H}$ by

$$Z(h, m) = \sum_{X \in \Gamma\backslash L_{h,m}} \frac{1}{|\overline{\Gamma}_X|} D_X$$

and define the modular trace of f for positive index m by

$$\mathrm{MT}_f^L(h, m) = \sum_{X \in \Gamma\backslash L_{h,m}} \frac{1}{|\overline{\Gamma}_X|} f(D_X). \tag{2.1}$$

The modular trace of f for zero index is given by a regularized integral [5, Definition 4.3] and the modular trace of f for negative index is defined in terms of an infinite geodesic in $\mathbb{H}$ [5, Definition 4.3]. Their explicit computations in terms of Fourier coefficients of f are given in [5, Remark 4.9] and [5, Proposition 4.7], respectively.

The modular trace satisfies the following important analytic property.

Theorem 2.1. [5, Theorem 4.5] *Let f be a weakly holomorphic modular function on a congruence subgroup Γ and assume that the constant coefficients of f at all cusps vanish. Then*

$$\sum_{n \gg -\infty} \mathrm{MT}_f^L(h, n) q^n \tag{2.2}$$

is a weakly holomorphic modular form of weight $3/2$ for $\Gamma(4N)$, where $4N$ is the level of the lattice L.

Remark 1. If $h = 0$, then the modular trace is modular on a bigger congruence subgroup $\Gamma_0(4N)$ [5].

Suppose we use the lattice L_1 in (1.11) and assume that the discriminant $-D$ is congruent to a square modulo $4N^2$. For a function f that is modular on $\Gamma_0^0(N)$, we define

$$\mathbf{t}_f^{(\beta)}(D) := \sum_{Q \in \mathcal{Q}_{D,(N),\beta}/\Gamma_0^0(N)} \frac{1}{|\Gamma_0^0(N)_Q|} f(\tau_Q). \tag{2.3}$$

Then $\mathrm{MT}_f^{L_1}(0, D)$ is the sum of $\mathbf{t}_f^{(\beta)}(D)$ given in the lemma below.

Lemma 2.2. *Suppose $-D$ is an imaginary quadratic discriminant such that $-D \equiv \square \pmod{4N^2}$. If f is a weakly holomorphic modular function on $\Gamma_0^0(N)$ and the lattice L_1 is given as (1.11), then the Bruinier-Funke modular trace is given by*

$$\mathrm{MT}_f^{L_1}(0, D) = 2 \sum_{\beta \in \mathbb{Z}/2N^2\mathbb{Z}} \boldsymbol{t}_f^{(\beta)}(D).$$

Proof. This lemma follows from the parallel argument to that in [5, Section 6]. The lattice L_1 given in (1.11) has level $4N^2$ and is stabilized by $\Gamma = \Gamma_0^0(N)$. Each vector $X = \begin{pmatrix} b & 2Nc \\ -2Na & -b \end{pmatrix} \in L_1$ with $q(X) = D > 0$ corresponds to the definite integral binary quadratic form $Q = \begin{pmatrix} Na & b/2 \\ b/2 & Nc \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} X$ with discriminant $-D = b^2 - 4N^2ac = -q(X)$. Here the $\Gamma_0^0(N)$-action on L_1 corresponds to the natural right action on quadratic forms and the cycle D_X coincides with the CM point τ_Q (resp. τ_{-Q}) corresponding to Q (resp. $-Q$) if Q is positive (resp. negative) definite. Consequently, if we set $\mathcal{Q}_{D,(N)} = \{[Na, b, Nc] \in \mathcal{Q}_D\}$ that is stabilized by $\Gamma_0^0(N)$, then the Heegner divisor is given by $Z(0, D) = \sum_{Q \in \mathcal{Q}_{D,(N)}/\Gamma_0^0(N)} \frac{2\tau_Q}{|\Gamma_0^0(N)_Q|}$ and hence we have

$$\mathrm{MT}_f^{L_1}(0, D) = 2 \sum_{Q \in \mathcal{Q}_{D,(N)}/\Gamma_0^0(N)} \frac{f(\tau_Q)}{|\Gamma_0^0(N)_Q|}. \tag{2.4}$$

Now, the lemma follows immediately. □ □

Example 2. *Recall that $\gamma_2(\tau) = q^{-1/3} + O(q)$. Applying* [5, Remark 4.9] *with transformation properties of γ_2 in (3.1), we find that $\mathrm{MT}_{\gamma_2}(0, 0) = 0$. Also, on account of* [5, Proposition 4.7], *we have*

$$\mathrm{MT}_{\gamma_2}(0, -m^2) = -2m \sum_{n \in \frac{m}{3}\mathbb{Z}_{<0}} (a_0(n) + a_\infty(n)),$$

where $a_\ell(n)$ is the n-th Fourier coefficient of γ_2 at cusp ℓ. Hence the only nonzero trace with negative index is $\mathrm{MT}_{\gamma_2}(0, -1) = 4$, and we see that the generating series of modular traces of γ_2 is given by

$$\sum_{n \in \mathbb{Z},\ n \gg -\infty} \mathrm{MT}_{\gamma_2}(0, n) q^n = 4q^{-1} + O(q), \tag{2.5}$$

which is a weakly holomorphic modular form as asserted in Theorem 2.1.

Lemma 2.3. *Suppose $-D$ is an imaginary quadratic discriminant such that $-D \equiv \square \pmod{4N^2}$. If f is a weakly holomorphic modular function on $\Gamma_0^0(N)$ and the lattice L_2 is given as (1.14), then the Bruinier-Funke modular trace is given by*

$$\mathrm{MT}_f^{L_2}(h, D/4N^2) = \boldsymbol{t}_f^{(h)}(D) + \boldsymbol{t}_f^{(-h)}(D).$$

Proof The dual lattice $L_2^{\#}$ of the lattice L_2 in (1.14) is given by

$$L_2^{\#} = \left\{ \begin{pmatrix} Nb & c \\ -a & -Nb \end{pmatrix} \Big| a, c \in \mathbb{Z}, b \in \frac{1}{2N^2}\mathbb{Z} \right\}.$$

Since $L_2^{\#}/L_2 \cong \mathbb{Z}/2N^2\mathbb{Z}$ is cyclic, each coset in $L_2^{\#}/L_2$ is of the form

$$\left\{ \begin{pmatrix} Nb + h/2N & c \\ -a & -Nb - h/2N \end{pmatrix} \Big| a, b, c \in \mathbb{Z} \right\}$$

for $h \in \{0, 1, \cdots, 2N^2 - 1\}$. It is easy to check that $\Gamma = \Gamma_0^0(N)$ acts on L_2 and acts trivially on $L_2^{\#}/L_2$. If

$$X = \begin{pmatrix} Nb + h/2N & c \\ -a & -Nb - h/2N \end{pmatrix} \in L_2 + h$$

is a vector of positive norm $D/4N^2$, then the matrix

$$Q = \begin{pmatrix} Na & N^2b + h/2 \\ N^2b + h/2 & Nc \end{pmatrix} = N \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} X$$

defines a definite integral binary quadratic form of discriminant $-D = (2N^2b + h)^2 - 4N^2ac = -4N^2q(X)$. Again, the $\Gamma_0^0(N)$-action on $L_2 + h$ corresponds to the natural right action on quadratic forms and the cycle D_X coincides with the CM point τ_Q (resp. τ_{-Q}) corresponding to Q (resp. $-Q$) if Q is positive (resp. negative) definite. We then see

$$Z(h, D/N^2) = \sum_{Q \in \mathcal{Q}_{D,(N),h}/\Gamma_0^0(N)} \frac{\tau_Q}{|\Gamma_0^0(N)_Q|} + \sum_{Q \in \mathcal{Q}_{D,(N),-h}/\Gamma_0^0(N)} \frac{\tau_Q}{|\Gamma_0^0(N)_Q|}$$

and this establishes the lemma. □

3. Class invariants with minimal polynomials in $\mathbb{Z}[X]$

Let F_N denote the modular function field of level N defined over $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive N-th root of unity. The second main theorem of complex multiplication tells us that the value of a modular function $f \in F_N$ at τ_D lies in the ray class field of conductor N for the order $\mathcal{O}_D = \mathbb{Z}[\tau_D]$ of an imaginary quadratic number field K and the ray class field is generated by the values $g(\tau_D)$ for the functions $g \in F_N$ with no poles at τ_D. In particular, $j(\tau_D)$ generates the ring class field H_D, the ray class field of conductor 1. One of many advantages of having a ring class field over a ray class field is that there is an isomorphism

$$Gal(H_D/K) \simeq C(D)$$

between Galois group of H_D over K and the form class group of discriminant $-D$ due to class field theory.

If a level N modular function f also generates the ring class field H_D at τ_D, we follow Weber to call the value $f(\tau_D)$ a class invariant. A real-valued class invariant $f(\tau_D)$ is especially convenient because its minimal polynomial has integral coefficients. The holomorphic cube root γ_2 of j on $\mathbb{H}$ is an example of the function that yields such a class invariant. It has an integral Fourier expansion and it takes on real values at purely imaginary numbers in $\mathbb{H}$. The function γ_2 is modular of level 3 and the generating matrices $S, T \in \Gamma(1)$ given by $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ act via

$$\gamma_2 \circ S = \gamma_2 \quad \text{and} \quad \gamma_2 \circ T = \zeta_3^{-1}\gamma_2. \tag{3.1}$$

The following result can be found in quite a lot of places in the literature (for example, [4], [8], [11], [22], [26]).

Proposition 3.1. *Suppose $-D$ is an imaginary quadratic discriminant and $\tau_D = \frac{-B+\sqrt{-D}}{2}$ as in (1.1). If $3 \nmid D$, then $\zeta_3^B\gamma_2(\tau_D)$ is a class invariant and its minimal polynomial has integer coefficients.*

Remark 2. The holomorphic square root γ_3 of $j - 1728$ is a modular function of level 2 and the action of matrices of S and T is given by

$$\gamma_3 \circ S = -\gamma_3, \quad \gamma_3 \circ T = -\gamma_3. \tag{3.2}$$

But its minimal polynomial has imaginary coefficients [23, Theorem 3].

While the coefficients of $\mathcal{H}_{-71}(X)$ are enormously large (its constant term is as large as 7×10^{35}), the minimal polynomial of $\zeta_3\gamma_2(\tau_{71})$ is

$$\begin{aligned} \mathcal{H}_{71}^{\zeta_3\gamma_2}(X) &= X^7 + 6745X^6 - 327467x^5 + 51857115X^4 + 2319299751X^3 \\ &\quad +41264582513X^2 - 307873876442X + 903568991567. \end{aligned} \tag{3.3}$$

As seen in the introduction, however, a Weber function does a better job in producing smaller coefficients for its minimal polynomial. Define the Weber functions

$$\mathfrak{f}(\tau) = \zeta_{48}^{-1}\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)}, \qquad \mathfrak{f}_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)}, \qquad \mathfrak{f}_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}, \tag{3.4}$$

where the Dedekind-eta function $\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ is holomorphic and non-zero on $\mathbb{H}$. These level 48 modular functions, specifically, $\mathfrak{f}, \mathfrak{f}_1, \sqrt{2}\mathfrak{f}_2$, have integral Fourier coefficients and the action of matrices S and T is given by

$$(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ S = (\mathfrak{f}, \mathfrak{f}_2, \mathfrak{f}_1) \qquad \text{and} \qquad (\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ T = (\zeta_{48}^{-1}\mathfrak{f}_1, \zeta_{48}^{-1}\mathfrak{f}, \zeta_{48}^{2}\mathfrak{f}_2). \tag{3.5}$$

They also satisfy

$$\mathfrak{f}\mathfrak{f}_1\mathfrak{f}_2 = \sqrt{2} \quad \text{and} \quad (X + \mathfrak{f}^8)(X - \mathfrak{f}_1^8)(X - \mathfrak{f}_2^8) = X^3 - \gamma_2 X + 16. \tag{3.6}$$

The following has been known for many years as well (see [3], [4], [11], [12], [13], [22], [26] for example).

Proposition 3.2. *Suppose $-D$ is an imaginary quadratic discriminant such that $-D \equiv 1 \pmod 8$ and $\tau_D = \frac{-1+\sqrt{-D}}{2}$. If $3 \nmid D$, then $\zeta_{48}\mathfrak{f}_2(\tau_D)$ is a class invariant and its minimal polynomial has integer coefficients.*

The minimal polynomial of $\zeta_{48}\mathfrak{f}_2(\tau_{71})$ is

$$\mathcal{H}_{71}^{\zeta_{48}\mathfrak{f}_2}(X) = X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X - 1.$$

One can generalize Weber functions by taking the holomorphic 24-th root of the Siegel function

$$\phi = n^{12}\frac{\Delta(A\tau)}{\Delta(\tau)},$$

where $\Delta(\tau) = \eta^{24}(\tau)$ is the modular form of weight 12 with no poles or zeros on $\mathbb{H}$ and $A = \left(\begin{smallmatrix} 1 & k \\ 0 & n \end{smallmatrix}\right)$ for $k \in \mathbb{Z}$ and a positive integer n. If $n = 2$, we have Weber functions and if $n = 3$, we consider

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)}, \quad \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)}, \quad \mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)}, \quad \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)}. \tag{3.7}$$

The Siegel function has a long history [9], [18] and the study on its 24-th root of unity for arbitrary n can be found in [12], [15], [16]. The functions in (3.7) are modular of level 72 and the action of S and T again permutes them up to multiplication by some roots of unity:

$$(\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3) \circ S = (\mathfrak{g}_3, \zeta_{24}^{-2}\mathfrak{g}_2, \zeta_{24}^{2}\mathfrak{g}_1, \mathfrak{g}_0), \qquad (\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3) \circ T = (\mathfrak{g}_1, \zeta_{24}^{-2}\mathfrak{g}_2, \mathfrak{g}_0, \zeta_{24}^{2}\mathfrak{g}_3) \tag{3.8}$$

The relations $\mathfrak{g}_0\mathfrak{g}_1\mathfrak{g}_2\mathfrak{g}_3 = \sqrt{3}$ and

$$(X + \mathfrak{g}_0^6)(X - \mathfrak{g}_1^6)(X - \mathfrak{g}_2^6)(X - \mathfrak{g}_3^6) = X^4 + 18X^2 + \gamma_3 X - 27$$

are analogous to Weber's identities in (3.6).

The values of these functions at an imaginary quadratic were first evaluated by S. Ramanujan [21] and further studied in [2], [7]. Gee and Stevenhagen [12], [13] found congruence conditions that imaginary quadratic discriminant $-D$ should satisfy for which $\mathfrak{g}_i(\tau_D)$ $(i = 0, 1, 2, 3)$ is a class invariant. In particular, they [13] showed that $\zeta_3\mathfrak{g}_0^2(\tau)$ when $\tau = \tau_{71}$ is a class invariant with the minimal polynomial

$$\mathcal{H}_{71}^{\zeta_3\mathfrak{g}_0^2}(X) = X^7 + (2 + 2\tau)X^5 - (30 + 3\tau)X^4 + (51 - 3\tau)X^3 - (8 - 10\tau)X^2 - (47 + 2\tau) \notin \mathbb{Z}[X].$$

We, however, will show that $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_D)$ is a real-valued class invariant for $-D \equiv 1 \pmod{12}$ so that its minimal polynomial has integer coefficients. The minimal polynomial of $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_{71})$ is

$$\mathcal{H}_{71}^{\mathfrak{g}_0^6+\mathfrak{g}_1^6}(X) = X^7 - 171X^6 + 4535X^5 - 73947X^4 + 606693X^3 - 4397075X^2 + 17581554X - 25839143.$$

We may reduce the size of coefficients of the minimal polynomial by considering $(\zeta_3\mathfrak{g}_0^2 + \zeta_3^2\mathfrak{g}_1^2)(\tau_{71})$. But for discriminants $-D$ satisfying $-D \equiv 1 \pmod{12}$ in general, $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_D)$ is the optimal choice.

Computing Hilbert class polynomials is very important in number theory and its application to cryptography [1], [8]. Despite a long history of the problem (see [6, p. 378] for the list of a few of references), one began to treat class invariants in a systemic and algorithmic way only after Shimura's reciprocity law became available. We discuss the reciprocity theorem in the next section.

4. Shimura reciprocity law and Galois conjugates of class invariants

Let K^{ab} denote the maximal abelian extension of K. For $f \in F_N$, if $f(\tau_D)$ lies in H_D, then all automorphisms in $\mathrm{Gal}(K^{\mathrm{ab}}/H_D)$ act trivially on $f(\tau_D)$. Then Shimura reciprocity law states that the image of $f(\tau_D)$ under the inverse image of the Artin map of $\mathrm{Gal}(K^{\mathrm{ab}}/H_D)$ can be obtained as the value at τ_D of a modular function that is conjugate to f over $\mathbb{Q}(j)$.

We follow the exposition in [7] that we can easily employ to prove our results. Let $\mathcal{Q}_D^0 \subseteq \mathcal{Q}_D$ be the subset of primitive quadratic forms and $C(D) = \mathcal{Q}_D^0/\Gamma(1)$ denote the form class group of discriminant $-D$. One obtains a complete set of representatives in $C(D)$ by choosing the reduced forms $[a, b, c]$ such that

$$|b| \le a \le c \quad \text{and} \quad b \ge 0 \text{ if either } |b| = a \text{ or } a = c. \tag{4.1}$$

The class of $[a, -b, c]$ is the inverse of $[a, b, c]$ in $C(D)$.

Given $f \in F_N$ with $f(\tau_D) \in H_D$, Shimura reciprocity enables one to determine the Galois action of the class of $[a, -b, c]$ in $C(D)$ with respect to the Artin map as follows ([13], [11, Theorem 20], [7, Lemma 3.1]):

$$f(\tau_D)^{[a,-b,c]} = f^M(\tau_Q), \tag{4.2}$$

where f^M denotes the image of f under the action of M and $M = M_{[a,b,c]} \in GL_2(\mathbb{Z}/N\mathbb{Z})$ is the matrix given by

$$M \equiv \begin{cases} \begin{pmatrix} a & \frac{b-u}{2} \\ 0 & 1 \end{pmatrix} & \pmod{p^{r_p}}, \text{ if } p \nmid a, \\ \begin{pmatrix} \frac{-b-u}{2} & -c \\ 1 & 0 \end{pmatrix} & \pmod{p^{r_p}}, \text{ if } p \mid a \text{ and } p \nmid c, \\ \begin{pmatrix} \frac{-b-u}{2} - a & \frac{-b+u}{2} - c \\ 1 & -1 \end{pmatrix} & \pmod{p^{r_p}}, \text{ if } p \mid a \text{ and } p \mid c, \end{cases} \tag{4.3}$$

where p runs over all prime factors of N and $p^{r_p} \| N$. Here $u = 0$ when D is even and $u = 1$ when D is odd.

The action of M depends only on M_{p^r} for all primes $p|N$ where $M_m \in GL_2(\mathbb{Z}/m\mathbb{Z})$ is the reduction modulo m of M. Every M_m with determinant x decomposes as $M_m = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}_m \begin{pmatrix} a & b \\ c & d \end{pmatrix}_m$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix}_m \in SL_2(\mathbb{Z}/m\mathbb{Z})$. Since $SL_2(\mathbb{Z}/m\mathbb{Z})$ is generated by S_m and T_m, it suffices to find the action of $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}_{p^{r_p}}$, $S_{p^{r_p}}$ and $T_{p^{r_p}}$ on f for all $p|N$. For $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}_{p^{r_p}}$, the action on F_N is given by lifting the automorphism of $\mathbb{Q}(\zeta_N)$ determined by

$$\zeta_{p^{r_p}} \mapsto \zeta_{p^{r_p}}^x \quad \text{and} \quad \zeta_{q^{r_q}} \mapsto \zeta_{q^{r_q}}$$

for all prime factors $q|N$ such that $q \neq p$. In order that the actions of the matrices at different primes commute with each other, we lift $S_{p^{r_p}}$ and $T_{p^{r_p}}$ to matrices in $SL_2(\mathbb{Z}/N\mathbb{Z})$ such that they reduce to the identity matrix in $SL_2(\mathbb{Z}/q^{r_p}\mathbb{Z})$ for all $q \neq p$.

Now, we are ready to prove Theorem 1.1. Recall from Proposition 3.1 that $\zeta_3^B \gamma_2(\tau_D)$ is a class invariant if the discriminant $-D$ is not divisible by 3.

Proof of Theorem 1.1. Using (4.3), we may write the matrix $M \in GL_2(\mathbb{Z}/3\mathbb{Z})$ that satisfies

$$(\zeta_3^B \gamma_2(\tau_D))^{[a,-b,c]} = (\zeta_3^B \gamma_2)^M(\tau_Q)$$

as, if D is even,

$$M_3 = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} ST^{-a}ST^{-a}ST^{-a(b+1)}, & \text{if } 3 \nmid a; \\ \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} T^{(b+1)c}ST^{c}ST^{c}, & \text{if } 3 \mid a \text{ and } 3 \nmid c; \\ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} T^{b+1}ST^{b}ST^{b-1}, & \text{if } 3 \mid a \text{ and } 3 \mid c \end{cases} \tag{4.4}$$

and, if D is odd,

$$M_3 = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} ST^{-a}ST^{-a}ST^{-ba}, & \text{if } 3 \nmid a; \\ \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} T^{(b-1)c}ST^{c}ST^{c}, & \text{if } 3 \mid a \text{ and } 3 \nmid c; \\ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} T^{1-b}ST^{b}ST^{b-1}, & \text{if } 3 \mid a \text{ and } 3 \mid c. \end{cases} \tag{4.5}$$

By applying (3.1) in (4.4) and (4.5), we can easily see that (1.8) holds for both cases. □

For appropriate discriminants $-D$, $\gamma_3(\tau_D)$ and $\zeta_{48}\mathfrak{f}_2(\tau_D)$ are also class invariants by Remark 2 and Proposition 3.2, respectively. Earlier, using the same method with the proof of Theorem 1.1, Gee [11] computed Galois conjugates of them so that she could prove conjectural formulas made by Morain [19] and Zagier and Yui [27], respectively.

Theorem 4.1. [11, Proposition 21] *Suppose $-D$ is an odd imaginary quadratic discriminant. We let $\tau_D = \frac{-1+\sqrt{-D}}{2}$ and let $\tau_Q = \frac{-b+\sqrt{-D}}{2a}$ be the associated CM point to a primitive quadratic form $Q = [a, b, c]$ of discriminant $-D$. The action of the form class group on $\gamma_3(\tau_D)$ is given by the formula*

$$(\gamma_3(\tau_D))^{[a,-b,c]} = (-1)^{\frac{b+1}{2}+ac+a+c}\gamma_3(\tau_Q).$$

Theorem 4.2. [11, Proposition 22] *Suppose* $-D \equiv 1 \pmod 8$ *is an imaginary quadratic discriminant such that $3 \nmid D$. We let $\tau_D = \frac{-1+\sqrt{-D}}{2}$ and let $\tau_Q = \frac{-b+\sqrt{-D}}{2a}$ be the associated CM point to a primitive quadratic form $Q = [a, b, c]$ of discriminant $-D$. The action of the form class group on $\zeta_{48}\mathfrak{f}_2(\tau_D)$ is given by the formula*

$$(\zeta_{48}\mathfrak{f}_2(\tau_D))^{[a,-b,c]} = \begin{cases} \zeta_{48}^{b(a-c+a^2c)}\mathfrak{f}_2(\tau_Q), & \text{if } 2 \nmid a, \\ \zeta_{48}^{b(a-c-ac^2)}\mathfrak{f}_1(\tau_Q), & \text{if } 2 \mid a \text{ and } 2 \nmid c, \\ (-1)^{\frac{-D-1}{8}}\zeta_{48}^{b(a-c+ac^2)}\mathfrak{f}(\tau_Q), & \text{if } 2 \mid a \text{ and } 2 \mid c. \end{cases}$$

Lastly, we consider the cubic analogues $\mathfrak{g}_0$, $\mathfrak{g}_1$, $\mathfrak{g}_2$, $\mathfrak{g}_3 \in F_{72}$ of the Weber functions, which are given in (3.7). H. H. Chan, Gee, and V. Tan [7, Theorem 3.2] showed that $\mathfrak{g}_0^{12}(\tau_D)$ is a class invariant when $-D \equiv 0 \pmod{12}$ and Gee [12, p.73, Theorem 1] completely determined the values of τ_D at which $\mathfrak{g}_i(\tau_D)$ $(i = 0, 1, 2)$ is a class invariant for the case when $-D$ is a fundamental discriminant of K. For example, if $-D \equiv 1 \pmod 4$ and square-free, she showed that the value at τ_D of each function in the table below generates the Hilbert class field over K:

$-D \equiv 1 \pmod 9$	$-D \equiv 4 \pmod 9$	$-D \equiv 7 \pmod 9$
$\zeta_3\mathfrak{g}_0^2,\ \zeta_3^2\mathfrak{g}_1^2$	$\mathfrak{g}_0^2,\ \mathfrak{g}_1^2$	$\zeta_3^2\mathfrak{g}_0^2,\ \zeta_3\mathfrak{g}_1^2$

In fact, for any discriminant $-D$ such that $-D \equiv 1 \pmod 4$, one can easily verify that the value at τ_D of each function in the table above generates the ring class field, as the conductor of $\mathcal{O}_D$ is prime to 2 and 3. Therefore, we can conclude that $\mathfrak{g}_0^6(\tau_D)$ and $\mathfrak{g}_1^6(\tau_D)$ are class invariants if $-D \equiv 1 \pmod{12}$.

Now we compute the action of a primitive quadratic form $Q = [a, b, c]$ on $\mathfrak{g}_0^6(\tau_D)$ and $\mathfrak{g}_1^6(\tau_D)$ using (4.2) and (4.3). In either case of $m = 8$ or 9, the matrix has the following decomposition due to [11, Lemma 6]:

$$M_m = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}_m S_m T_m^{-a^{-1}} S_m T_m^{-a^{-1}} S_m T_m^{\frac{b-3}{2a}}, & \text{if } 3 \nmid a, \\ \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}_m T_m^{\frac{1-b}{2}c} S_m T_m^{c^{-1}} S_m T_m^{c}, & \text{if } 3|a \text{ and } 3 \nmid c, \\ \begin{pmatrix} 1 & 0 \\ 0 & a+b+c \end{pmatrix}_m T_m^{(\frac{1-b-2a}{2})(a+b+c)} S_m T_m^{(a+b+c)^{-1}} S_m T_m^{(a+b+c-1)}, & \text{if } 3|a \text{ and } 3|c \end{cases}$$

Also, by means of transformation formulas for $\mathfrak{g}_i$ $(i = 0, 1, 2, 3)$ in (3.8), we derive the following actions:

	$\mathfrak{g}_0^6$	$\mathfrak{g}_1^6$	$\mathfrak{g}_2^6$	$\mathfrak{g}_3^6$
$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}_8$	$\mathfrak{g}_0^6$	$\mathfrak{g}_1^6$	$\mathfrak{g}_2^6$	$\mathfrak{g}_3^6$
S_8	$-\mathfrak{g}_0^6$	$-\mathfrak{g}_1^6$	$-\mathfrak{g}_2^6$	$-\mathfrak{g}_3^6$
T_8	$-\mathfrak{g}_0^6$	$-\mathfrak{g}_1^6$	$-\mathfrak{g}_2^6$	$-\mathfrak{g}_3^6$
$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}_9$, $3\|(x-1)$	$\mathfrak{g}_0^6$	$\mathfrak{g}_1^6$	$\mathfrak{g}_2^6$	$\mathfrak{g}_3^6$
$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}_9$, $3\|(x-2)$	$\mathfrak{g}_0^6$	$\mathfrak{g}_2^6$	$\mathfrak{g}_1^6$	$\mathfrak{g}_3^6$
S_9	$-\mathfrak{g}_3^6$	$\mathfrak{g}_2^6$	$\mathfrak{g}_1^6$	$-\mathfrak{g}_0^6$
T_9	$-\mathfrak{g}_1^6$	$\mathfrak{g}_2^6$	$-\mathfrak{g}_0^6$	$\mathfrak{g}_3^6$

Accordingly, the action of M_8 on $\mathfrak{g}_i^6$ (for $i = 0, 1$) is given by

$$(\mathfrak{g}_i^6)^{M_8} = (-1)^{\frac{b+1}{2}+ac+a+c}\mathfrak{g}_i^6$$

and the action of M_9 on $\mathfrak{g}_i^6$ depends on the values of a, b, c modulo 3. For example, consider the case when $3|a$ and $3|c$. Then b should be congruent to 1 or 2 modulo 3 and we obtain

$$(\mathfrak{g}_0^6)^{M_9} = \begin{cases} \mathfrak{g}_0^6, & b \equiv 1 \pmod 3), \\ -\mathfrak{g}_3^6, & b \equiv 2 \pmod 3). \end{cases}$$

We finally establish the following theorem.

Theorem 4.3. *Suppose $-D \equiv 1 \pmod{12}$ is an imaginary quadratic discriminant. Let $\tau_D = \frac{-1+\sqrt{-D}}{2}$ and let $\tau_Q = \frac{-b+\sqrt{-D}}{2a}$ be the associated CM point to a primitive quadratic form $Q =$*

$[a,b,c]$ of discriminant $-D$. The actions of the form class group on $\mathfrak{g}_0^6(\tau_D)$ and $\mathfrak{g}_1^6(\tau_D)$ are given by the formulas below:

(1) *The cases $3 \nmid a$.*

$$\mathfrak{g}_0^6(\tau_D)^{[a,-b,c]} = \begin{cases} (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_0^6(\tau_Q), & \text{if } b \equiv 1 \pmod 3, \\ (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_1^6(\tau_Q), & \text{if } a(b-1) \equiv -1 \pmod 3, \\ (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_2^6(\tau_Q), & \text{if } a(b-1) \equiv 1 \pmod 3, \end{cases}$$

$$\mathfrak{g}_1^6(\tau_D)^{[a,-b,c]} = \begin{cases} (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_0^6(\tau_Q), & \text{if } b \equiv -1 \pmod 3, \\ (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_1^6(\tau_Q), & \text{if } a+b \equiv -1 \pmod 3, \\ (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_2^6(\tau_Q), & \text{if } a-b \equiv 1 \pmod 3. \end{cases}$$

(2) *The cases $3|a$ and $3 \nmid c$.*

$$\mathfrak{g}_0^6(\tau_D)^{[a,-b,c]} = \begin{cases} (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_1^6(\tau_Q), & \text{if } (b+1)c \equiv -1 \pmod 3, \\ (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_2^6(\tau_Q), & \text{if } (b+1)c \equiv 1 \pmod 3, \\ (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_3^6(\tau_Q), & \text{if } b \equiv -1 \pmod 3, \end{cases}$$

$$\mathfrak{g}_1^6(\tau_D)^{[a,-b,c]} = \begin{cases} (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_1^6(\tau_Q), & \text{if } b+c \equiv 1 \pmod 3, \\ (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_2^6(\tau_Q), & \text{if } b-c \equiv 1 \pmod 3, \\ (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_3^6(\tau_Q), & \text{if } b \equiv 1 \pmod 3. \end{cases}$$

(3) *The cases $3|a$ and $3|c$.*

$$\mathfrak{g}_0^6(\tau_D)^{[a,-b,c]} = \begin{cases} (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_0^6(\tau_Q), & \text{if } b \equiv 1 \pmod 3, \\ (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_3^6(\tau_Q), & \text{if } b \equiv -1 \pmod 3, \end{cases}$$

$$\mathfrak{g}_1^6(\tau_D)^{[a,-b,c]} = \begin{cases} (-1)^{\frac{b+1}{2}+ac+a+c}\,\mathfrak{g}_3^6(\tau_Q), & \text{if } b \equiv 1 \pmod 3, \\ (-1)^{\frac{b-1}{2}+ac+a+c}\,\mathfrak{g}_0^6(\tau_Q), & \text{if } b \equiv -1 \pmod 3. \end{cases}$$

It follows from the Galois action given in Theorem 4.3 (3) that if $3|a$ and $3|c$, then

$$\mathfrak{g}_0^6(\tau_D)^{[a,-b,c]} = \overline{\mathfrak{g}_1^6(\tau_D)^{[a,b,c]}}.$$

In particular, $\mathfrak{g}_0^6(\tau_D)$ is the complex conjugation of $\mathfrak{g}_1^6(\tau_D)$ and

$$\mathfrak{g}_0^6(\tau_D) + \mathfrak{g}_1^6(\tau_D) = 2\mathrm{Re}(\mathfrak{g}_0^6(\tau_D)). \tag{4.6}$$

We save proving that $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_D)$ is a class invariant using Theorem 4.3 and (4.6) until Section 6.

5. Modularity of Galois traces of the Weber class invariants

We start this section with a proof of $\mathcal{Q}_D/\Gamma(1) \cong \mathcal{Q}_{D,(N),\beta}/\Gamma_0^0(N)$.

Lemma 5.1. *Assume that D is not divisible as a discriminant by the square of any prime dividing N. Then there is a canonical bijection between $\mathcal{Q}_D/\Gamma(1)$ and $\mathcal{Q}_{D,(N),\beta}/\Gamma_0^0(N)$ if $\mathcal{Q}_{D,(N),\beta}$ is not empty.*

Proof. For $-D$ which is congruent to a square modulo $4N$ and β modulo $2N$, we define

$$\mathcal{Q}_{D,N,\beta} = \{[Na, b, c] \in \mathcal{Q}_D \mid b \equiv \beta \pmod{2N}\} \tag{5.1}$$

on which $\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \mid c \equiv 0 \pmod N\}$ acts. It is known from [14] that there is a canonical bijection between $\mathcal{Q}_{D,N,\beta}/\Gamma_0(N)$ and $\mathcal{Q}_D/\Gamma(1)$ for D that is not divisible by any prime divisors of N. Hence, for the discriminant satisfying the condition in the hypothesis, $\mathcal{Q}_{D,N^2,\beta}/\Gamma_0(N^2) \cong \mathcal{Q}_D/\Gamma(1)$. Also, the map from $\mathcal{Q}_{D,(N),\beta}/\Gamma_0^0(N)$ to $\mathcal{Q}_{D,N^2,\beta}/\Gamma_0(N^2)$ that sends Q to $Q \circ \begin{pmatrix} \sqrt{N} & 0 \\ 0 & 1/\sqrt{N} \end{pmatrix}$ is bijective, and therefore the lemma follows. □ □

Lemma 5.1 enables one to define modular traces of class invariants that we presented in Section 3. In order to discuss the modularity of Galois traces of the class invariants using Theorem 2.1, we prove the constant coefficients at all cusps of all functions that produce our class invariants are zero.

Lemma 5.2. *The constant coefficients of* γ_2, γ_3, $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, $\mathfrak{g}_0$, $\mathfrak{g}_1$, $\mathfrak{g}_2$, *and* $\mathfrak{g}_3$ *at all cusps vanish.*

Proof. Let $f \in \{\gamma_2, \gamma_3, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2, \mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3\}$. From the definition of f given in Section 3, we find that f has a zero constant coefficient at infinity. For other cusp s, we take $\gamma \in \Gamma(1)$ such that $\gamma \cdot \infty = s$. As $\Gamma(1)$ is generated by S and T, it follows from (3.1), (3.2), (3.5) and (3.8) that the Fourier expansion of $f \circ \gamma$ at infinity has also the zero coefficient. □ □

Proof of Theorem 1.2 Now, we begin to prove the modularity of the generating series of the Galois traces of $\zeta_3^B \gamma_2(\tau_D)$ in Theorem 1.2. Firstly, since γ_2 is $\Gamma_0^0(3)$-invariant by (3.1), it follows from Lemma 2.2 that, for discriminant $-D$ that is congruent to a square modulo 36, the modular trace of γ_2 is given by

$$\mathrm{MT}_{\gamma_2}^{L_1}(0, D) = 2 \sum_{\beta \in \mathbb{Z}/18\mathbb{Z}} \mathbf{t}_{\gamma_2}^{(\beta)}(D),$$

where $\mathbf{t}_f^{(\beta)}(D)$ is defined in (2.3). But if we assume the discriminant $-D$ is not divisible by the square of any prime dividing N, then there are exactly $2^{t(N)}$ choices of β, where $t(N)$ is the number of distinct prime divisors of N. Considering (1.10), we note that the value $\mathbf{t}_{\gamma_2}^{(\beta)}(D)$ is independent of the choice of β. Thus for the discriminant $-D$ which is not divisible by 3, we see that

$$\mathrm{MT}_{\gamma_2}^{L_1}(0, D) = 4 \sum_{Q \in \mathcal{Q}_{D,(3),\beta}/\Gamma_0^0(3)} \gamma_2(\tau_Q).$$

This together with (1.10) gives Equation (1.12) in Theorem 1.2.

For a discriminant that is a multiple of 3, the modified Galois trace of $\zeta_3^B \gamma_2(\tau_D)$ is not defined, while the modular trace of γ_2 vanishes as shown in the following lemma.

Lemma 5.3. *For imaginary quadratic discriminant* $-D$ *which is congruent to a square modulo* 36 *and divisible by* 3, $\mathrm{MT}_{\gamma_2}^{L_1}(0, D) = 0$

Proof. Denote $\mathcal{Q}_{D,N} = \{[Na, b, c] \in \mathcal{Q}_D\}$ that is stabilized by $\Gamma_0(N)$. If D is a multiple of 3, then the canonical map

$$\phi_3 : \mathcal{Q}_{D,(3)}/\Gamma_0^0(3) \to \mathcal{Q}_{D,3}/\Gamma_0(3)$$

may not be bijective. We recall that $\Gamma_0(N) = \bigcup_{k=0}^{N-1} T^k\Gamma_0^0(N)$. For each quadratic form $Q' = [a', b', c']$ in the range of ϕ_3, we may assume $3|a'$ and $3|c'$. And for any i, $Q' \circ T^i \in \mathcal{Q}_{D,(3)}$ and $\phi_3(Q' \circ T^i) = Q'$. Since $\tau_{Q\circ\gamma} = \gamma^{-1}\tau_Q$ for arbitrary $\gamma \in \Gamma(1)$, we obtain from (2.4) that

$$\mathrm{MT}_{\gamma_2}^{L_1}(0, D) = 2 \sum_{Q'\in \mathrm{Im}\phi_3} \sum_{0\le \ell<3} \gamma_2(T^{-\ell}\tau_{Q'}) = 2 \sum_{Q'\in \mathrm{Im}\phi_3} \sum_{\ell=0}^{2} \zeta_3^{\ell}\gamma_2(\tau_{Q'}) = 0,$$

where the penultimate equality above follows from (3.1). □ □

Finally, it follows from (1.12), Lemma 5.3, (2.5), Lemma 5.2, and Theorem 2.1 that the generating series of $\mathrm{GT}_{\zeta_3^B\gamma_2}(D)$ is a weakly holomorphic modular form of weight 3/2 on $\Gamma_0(36)$.
□*Remark 3.* Similarly, we can show that if D is an even discriminant, then $MT_{\gamma_3}^{L_1}(0, D) = 0$.

Proof of Theorem 1.3 From now, we prove Theorem 1.3 following the steps of the proof of Theorem 1.2.

Lemma 5.4. *$\mathfrak{f}$, $\mathfrak{f}_1^2$, and $\mathfrak{f}_2^2$ are $\Gamma_0^0(48)$-invariant.*

Proof. We know that $\mathfrak{f}$, $\mathfrak{f}_1$, and $\mathfrak{f}_2$ are $\Gamma(48)$-invariant from (3.5). But

$$\Gamma_0^0(48) = \bigcup_{a\in(\mathbb{Z}/48)^*} \sigma_a\Gamma(48),$$

where $\sigma_a \in SL_2(\mathbb{Z})$ such that $\sigma_a \equiv \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right) \pmod{48}$. Using [11, Lemma 6], we can write $\sigma_a = ST^{-a^{-1}}ST^{-a}ST^{-a^{-1}}$, which implies $\mathfrak{f}|_{\sigma_a} = \zeta_{48}^{2(a^{-1}-a)}\mathfrak{f} = \mathfrak{f}$ and $\mathfrak{f}_i^2|_{\sigma_a} = \zeta_{48}^{2(-a^{-1}+a)}\mathfrak{f}_i^2 = \mathfrak{f}_i^2$ for $i = 1, 2$. Therefore, $\mathfrak{f}$, $\mathfrak{f}_1^2$, and $\mathfrak{f}_2^2$ are $\Gamma_0^0(48)$-invariant. □ □

It follows from Lemma 2.2 and Lemma 5.4 that, for discriminant $-D$ that is congruent to a square modulo 9216, the modular trace of $\mathfrak{f}$ is given by

$$\mathrm{MT}_{\mathfrak{f}}^{L_1}(0, D) = 2 \sum_{\beta\in\mathbb{Z}/4608\mathbb{Z}} \mathbf{t}_{\mathfrak{f}}^{(\beta)}(D). \tag{5.2}$$

Moreover, if the discriminant satisfies $-D \equiv 1 \pmod 8$ as well, then by Theorem 4.2, $\zeta_{48}\mathfrak{f}_2(\tau_D)$ is a class invariant and its Galois trace is equal to the modular trace in (5.2) up to a constant multiple. More precisely, as there are 4 choices of β since $t(48) = 2$, we have

$$8\mathrm{GT}_{\zeta_{48}\mathfrak{f}_2}(D) = \mathrm{MT}_{\mathfrak{f}}^{L_1}(0, D). \tag{5.3}$$

We now show that the modular trace become zero whenever $-D$ that is congruent to a square modulo 9216 fails to satisfy $-D \equiv 1 \pmod 8$. It occurs when D is a multiple of 2 or 3. This is an analogous result to Lemma 5.3.

Lemma 5.5. *Assume that imaginary quadratic discriminant $-D$ is congruent to a square modulo 9216. If D is divisible by 2 or 3. Then $MT_{\mathfrak{f}}^{L_1}(0, D) = 0$.*

Proof. The proof is similar to that of Lemma 5.3. Consider the canonical map

$$\phi : \mathcal{Q}_{D,(48)}/\Gamma_0^0(48) \to \mathcal{Q}_{D,48}/\Gamma_0(48).$$

Let $Q'=[a',b',c']\in \mathrm{Im}\phi$ and $g=\gcd(b',48)>1$. Then for any i which is a multiple of $48/g$, $Q'\circ T^i\in \mathcal{Q}_{D,(48)}$ and $\phi(Q'\circ T^i)=Q'$, and hence we may write

$$\mathrm{MT}_{\mathfrak{f}}^{L_1}(0,D)=2\sum_{Q'\in\mathrm{Im}\phi}\sum_{\substack{\frac{48}{g}|i\\0\le i<48}}\mathfrak{f}(T^{-i}\tau_{Q'})=\sum_{Q'\in\mathrm{Im}\phi}\sum_{\ell=0}^{g-1}(\mathfrak{f}\circ T^{-\frac{48\ell}{g}})(\tau_{Q'}). \tag{5.4}$$

But it follows from (3.5) that for each Q', if $48/g$ is even, then

$$\sum_{\ell=0}^{g-1}\mathfrak{f}(\tau_{Q'}-\frac{48\ell}{g})=\sum_{\ell=0}^{g-1}\zeta_{48}^{\frac{48\ell}{g}}\mathfrak{f}(\tau_{Q'})=\sum_{\ell=0}^{g-1}\zeta_g^{\ell}\mathfrak{f}(\tau_{Q'})=0, \tag{5.5}$$

and if $48/g$ is odd, then
(5.6)
$$\sum_{\ell=0}^{g-1}(\mathfrak{f}\circ T^{-\frac{48\ell}{g}})(\tau_{Q'})=\sum_{\ell=0}^{g/2-1}\zeta_{48}^{\frac{48(2\ell)}{g}}\mathfrak{f}(\tau_{Q'})+\sum_{\ell=0}^{g/2-1}\zeta_{48}^{\frac{48(2\ell+1)}{g}}\mathfrak{f}_1(\tau_{Q'})=\sum_{\ell=0}^{g/2-1}\zeta_{g/2}^{\ell}(\mathfrak{f}(\tau_{Q'})+\zeta_g\mathfrak{f}_1(\tau_{Q'}))=0.$$

Therefore, $\mathrm{MT}_{\mathfrak{f}}^{L_1}(0,D)=0$. □ □

We now have Theorem 1.3 as a consequence of (5.3), Lemma 5.5, Lemma 5.2, and Theorem 2.1. □

6. Proof of Theorem 1.4

By the exactly same argument in the proof of Lemma 5.4, we find that $\mathfrak{g}_0^6$ and $\mathfrak{g}_3^6$ are $\Gamma_0^0(72)$-invariant. It thus follows from Lemma 2.3 that for discriminant $-D$ that is congruent to a square modulo 20736, the modular trace of $\mathfrak{g}_i^6$ $(i=0,3)$ is given by

$$\mathrm{MT}_{\mathfrak{g}_i^6}^{L_2}(\beta,D/20736)=\mathbf{t}_{\mathfrak{g}_i^6}^{(\beta)}(D)+\mathbf{t}_{\mathfrak{g}_i^6}^{(-\beta)}(D) \tag{6.1}$$

for a fixed value $\beta\in\mathbb{Z}/10368\mathbb{Z}$. On the other hand, both $\mathfrak{g}_0^6(\tau_D)$ and $\mathfrak{g}_1^6(\tau_D)$ are class invariants if $-D\equiv 1 \pmod{12}$ as discussed in Section 5. Hence for discriminant $-D$ that is congruent to a square modular 20736 and congruent to 1 modular 12, we see from Theorem 4.3 (3) that

$$\mathrm{GT}_{\mathfrak{g}_0^6}(D)=\begin{cases}\mathbf{t}_{\mathfrak{g}_0^6}^{(\beta)}(D), & \text{if } \beta\equiv 7 \pmod{12},\\ \mathbf{t}_{\mathfrak{g}_3^6}^{(\beta)}(D), & \text{if } \beta\equiv 5 \pmod{12}\end{cases} \tag{6.2}$$

and

$$\mathrm{GT}_{\mathfrak{g}_1^6}(D)=\begin{cases}\mathbf{t}_{\mathfrak{g}_3^6}^{(\beta)}(D), & \text{if } \beta\equiv 7 \pmod{12},\\ \mathbf{t}_{\mathfrak{g}_0^6}^{(\beta)}(D), & \text{if } \beta\equiv 5 \pmod{12}.\end{cases} \tag{6.3}$$

For $\beta \pmod{10368}$ such that $\beta^2\equiv -D \pmod{20736}$ and $\beta\equiv 5,7 \pmod{12}$, the generating series of $\mathrm{MT}_{\mathfrak{g}_i^6}^{L_2}(\beta,D/20736)$ $(i=0,3)$ only allows the terms $q^{D/20736}$ for $D\equiv -1 \pmod{12}$. Therefore, it suffices to prove $(\mathfrak{g}_0^6+\mathfrak{g}_1^6)(\tau_D)$ is a class invariant to complete the proof of Theorem 1.4. We do this by showing that $(\mathfrak{g}_0^6+\mathfrak{g}_1^6)(\tau_D)$ is different from all of its Galois conjugates. For the rest of this section, we assume that the discriminant $-D$ is congruent to a square modular 20736 and congruent to 1 modular 12 unless specified otherwise. This implies $D\ge 23$. Recall from (4.6) that $\mathfrak{g}_0^6(\tau_D) + \mathfrak{g}_1^6(\tau_D) = 2\mathrm{Re}(\mathfrak{g}_0^6(\tau_D))$ and from Theorem 4.3 that for any primitive quadratic form $[a,b,c]$ of discriminant $-D$,

$$\mathfrak{g}_0^6(\tau_D)^{[a,b,c]} = \pm\mathfrak{g}_i^6(\tau_Q) \quad \text{and} \quad \mathfrak{g}_1^6(\tau_D)^{[a,b,c]} = \pm\mathfrak{g}_j^6(\tau_Q)$$

for some $i,j \in \{0,1,2,3\}$. Therefore, if we show that $|\mathrm{Re}(\mathfrak{g}_0^6(\tau_D))|$ is greater than $|g_i^6(\tau_Q)|$ for all $i = 0,1,2,3$ and all the reduced primitive quadratic forms $Q = [a,b,c] \in \mathcal{Q}_D$ in which $a > 1$, then we are done.

For the purpose, we first compute a lower bound of $|\mathrm{Re}(\mathfrak{g}_0^6(\tau_D))|$.

Lemma 6.1. *Let $-D \equiv 1 \pmod{12}$ be a discriminant of an order in an imaginary quadratic field K with $D \geq 23$ and let $\tau_D = \frac{-1+\sqrt{-D}}{2}$. Then*

$$\left|\mathrm{Re}(\mathfrak{g}_0^6(\tau_D))\right| > 0.8e^{\frac{\sqrt{D}\pi}{6}}.$$

Proof. By its definition in (3.7),

$$\mathfrak{g}_0(\tau_D) = \zeta_{72}e^{\frac{\sqrt{D}\pi}{36}}\prod_{n=1}^{\infty}\frac{a_n}{b_n}, \tag{6.4}$$

where

$$a_n = 1 - e^{-\frac{\sqrt{D}n\pi}{3} - \frac{n\pi}{3}i} \qquad \text{and} \qquad b_n = 1 - e^{-\sqrt{D}n\pi - n\pi i}. \tag{6.5}$$

Letting $r = e^{-\sqrt{D}\pi}$, we have

$$1 - r^{\frac{n}{3}} \leq |a_n| \leq 1 + r^{\frac{n}{3}} \qquad \text{and} \qquad 1 - r^n \leq |b_n| \leq 1 + r^n$$

so that

$$\prod_{n=1}^{\infty}(1-r^{\frac{n}{3}})(1-r^n) \leq \prod_{n=1}^{\infty}\frac{1-r^{\frac{n}{3}}}{1+r^n} \leq \prod_{n=1}^{\infty}\left|\frac{a_n}{b_n}\right| \leq \prod_{n=1}^{\infty}\frac{1+r^{\frac{n}{3}}}{1-r^n} \leq \prod_{n=1}^{\infty}(1+r^{\frac{n}{3}})(1+1.1r^n). \tag{6.6}$$

For the far right inequality above, we used the $\dfrac{1}{1-x} \leq 1 + \alpha x$ that holds for $\alpha > 1$ and sufficiently small $x > 0$. In fact, this holds if and only if $\alpha x \leq \alpha - 1$.

As $1 + x \leq e^x$ for all x, we obtain from the far right side of (6.6) that

$$\prod_{n=1}^{\infty}\left|\frac{a_n}{b_n}\right| \leq e^{1.1\sum_{n=1}^{\infty}r^n + \sum_{n=1}^{\infty}r^{\frac{n}{3}} + 1.1\sum_{n=1}^{\infty}r^{\frac{4n}{3}}} = e^{\frac{1.1r}{1-r} + \frac{r^{\frac{1}{3}}}{1-r^{\frac{1}{3}}} + \frac{1.1r^{\frac{4}{3}}}{1-r^{\frac{4}{3}}}} \lessapprox 1.006656214, \tag{6.7}$$

because the middle is an increasing function of r $(0 \leq r < 1)$, and thus it has the maximum at r with $D = 23$.

For the opposite direction, we apply the inequality $1 - x \geq e^{-\alpha x}$ that holds for any positive real number $\alpha > 1$ and sufficiently small $x > 0$ into the far left side of (6.6). By taking $\alpha = 1.1$ and $x = r^n + r^{\frac{n}{3}} - r^{\frac{2n}{3}}$, we find that

$$\prod_{n=1}^{\infty}\left|\frac{a_n}{b_n}\right| \geq e^{-1.1\sum_{n=1}^{\infty}r^n - 1.1\sum_{n=1}^{\infty}r^{\frac{n}{3}} + 1.1\sum_{n=1}^{\infty}r^{\frac{4n}{3}}} = e^{-\frac{1.1r}{1-r} - \frac{1.1r^{\frac{1}{3}}}{1-r^{\frac{1}{3}}} + \frac{1.1r^{\frac{4}{3}}}{1-r^{\frac{4}{3}}}} \gtrapprox 0.9927290230, \tag{6.8}$$

because the middle is now a decreasing function of r $(0 \le r < 1)$, and hence it has the minimum at r with $D = 23$. Therefore, if we put

$$\mathfrak{g}_0^6(\tau_D) = zw = (z_1 + iz_2)(w_1 + iw_2), \tag{6.9}$$

where $z = (\zeta_{72} e^{\frac{\sqrt{D}\pi}{36}})^6 = \zeta_{12} e^{\frac{\sqrt{D}\pi}{6}}$ and $w = \prod_n (a_n/b_n)^6$, then we have

$$z_1 = \frac{\sqrt{3}}{2} e^{\frac{\sqrt{D}\pi}{6}}, \qquad z_2 = \frac{1}{2} e^{\frac{\sqrt{D}\pi}{6}}, \tag{6.10}$$

and

$$0.9571594985 < |w| < 1.040607789. \tag{6.11}$$

Now we compute $|w_1|$ and $|w_2|$ by estimating the argument of w. For $0 \le |\theta|, |\theta_n|, |\varphi_n|, |\psi_n| \le \pi$, set

$$\prod_{n=1}^{\infty} \frac{a_n}{b_n} = \left| \prod_{n=1}^{\infty} \frac{a_n}{b_n} \right| e^{\theta i}, \qquad \frac{a_n}{b_n} = \left| \frac{a_n}{b_n} \right| e^{\theta_n i},$$

and

$$a_n = |a_n| e^{\varphi_n i}, \qquad b_n = |b_n| e^{\psi_n i}.$$

Then from (6.5), we deduce that

$$\begin{aligned} |\tan(\varphi_n)| &= \left| \frac{\sin \frac{n\pi}{3} r^{\frac{n}{3}}}{1 - \cos \frac{n\pi}{3} r^{\frac{n}{3}}} \right| \le \frac{r^{\frac{n}{3}}}{1 - r^{\frac{n}{3}}} \le r^{\frac{n}{3}} (1 + 1.1 r^{\frac{n}{3}}), \\ |\tan(\psi_n)| &= \left| \frac{\sin n\pi r^n}{1 - \cos n\pi r^n} \right| \le \frac{r^n}{1 - r^n} \le r^n (1 + 1.1 r^n), \end{aligned}$$

and further by $x \le \tan x$, we obtain that

$$\begin{aligned} |\theta| &= \left| \sum_{n=1}^{\infty} \theta_n \right| \le \sum_{n=1}^{\infty} (|\tan(\varphi_n)| + |\tan(\psi_n)|) \\ &\le \sum_{n=1}^{\infty} \left(r^{\frac{n}{3}} + 1.1 r^{\frac{2n}{3}} + r^n + 1.1 r^{2n} \right) \\ &\le \frac{r^{\frac{1}{3}}}{1 - r^{\frac{1}{3}}} + 1.1 \frac{r^{\frac{2}{3}}}{1 - r^{\frac{2}{3}}} + \frac{r}{1 - r} + 1.1 \frac{r^2}{1 - r^2}. \end{aligned}$$

Since this is increasing with respect to r, it takes its maximum at r with $D = 23$. Thus we arrive at

$$|\theta| \le 0.006681903424. \tag{6.12}$$

It follows from (6.9), (6.11), and (6.12) that

$$|w_2| = |w||\sin 6\theta| \le |w||6\theta| \le 0.04171944449, \tag{6.13}$$

and then from (6.9), (6.11), and (6.13) that

$$|w_1| = \sqrt{|w|^2 - w_2{}^2} \ge 0.9562498594. \tag{6.14}$$

Finally, using (6.10), (6.13), and (6.14), we establish

$$|\mathrm{Re}(\mathfrak{g}_0^6(\tau_D))| = |z_1 w_1 - z_2 w_2| \ge 0.8072769486 e^{\frac{\sqrt{D}\pi}{6}}.$$

□ □

Next, we compute an upper bound for $|\mathfrak{g}_i^6(\tau_Q)|$ for $i = 0, 1, 2, 3$.

Lemma 6.2. *Let* $-D \equiv 1 \pmod{12}$ *be a discriminant of an order in an imaginary quadratic field* K *with* $D \geq 23$ *and let* $\tau_Q = \frac{-b+\sqrt{-D}}{2a}$ *be the associated CM point to a primitive quadratic form* $Q = [a, b, c]$ *of discriminant* $-D$*. Then we have*

$$|\mathfrak{g}_i^6(\tau_Q)| \leq 3.4e^{\frac{\sqrt{D}\pi}{6a}} \quad (i = 0, 1, 2) \tag{6.15}$$

and

$$|\mathfrak{g}_3^6(\tau_Q)| \leq 1.1e^{-\frac{\sqrt{D}\pi}{2a}}. \tag{6.16}$$

Proof. Since the same calculation works for all the cases in (6.15) and (6.16), we present the computation for the upper bound for $|\mathfrak{g}_0^6(\tau_Q)|$ only. From the definition in (3.7),

$$\mathfrak{g}_0^6(\tau_Q) = e^{\frac{\sqrt{D}\pi}{6a}} \prod_{n=1}^{\infty} \left(\frac{c_n}{d_n}\right)^6, \quad \text{where } c_n = 1 - e^{\frac{-\sqrt{D}\pi n - bn\pi i}{3a}} \quad \text{and} \quad d_n = 1 - e^{\frac{-\sqrt{D}\pi n - bn\pi i}{a}}.$$

If we put $s = e^{-\frac{\sqrt{D}\pi}{a}}$, then $s \leq e^{-\sqrt{3}\pi}$, because $a \leq \sqrt{\frac{D}{3}}$ by (4.1). By the same argument used in (6.5) through (6.7), we have

$$\prod_{n=1}^{\infty} \left|\frac{c_n}{d_n}\right| \leq e^{\frac{1.1s}{1-s} + \frac{s^{\frac{1}{3}}}{1-s^{\frac{1}{3}}} + \frac{1.1s^{\frac{4}{3}}}{1-s^{\frac{4}{3}}}} \lessapprox 1.2218379. \tag{6.17}$$

Therefore, we obtain the following inequality:

$$|\mathfrak{g}_0^6(\tau_Q)| \lessapprox 3.327220276e^{\frac{\sqrt{D}\pi}{6a}}.$$

□
□

If discriminant $-D$ is a square modulo 20736 and congruent to 1 modulo 12, then $-D = -23, -47, -71, -95$ and so on. For $D \geq 47$, it follows from Lemma 6.1 and Lemma 6.2 that

$$|\mathfrak{g}_i^6(\tau_Q)| \leq 3.4e^{\frac{\sqrt{D}\pi}{6a}} < 0.8e^{\frac{\sqrt{D}\pi}{6}} \leq |\mathrm{Re}(\mathfrak{g}_0^6(\tau_D))|,$$

where $\tau_Q = \frac{-b+\sqrt{-D}}{2a}$ with $a > 1$ for all $i = 0, 1, 2, 3$. This implies that $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_D)$ is different from its Galois conjugates, and hence $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_D)$ generates the ring class field H_D over $K = \mathbb{Q}(\sqrt{-D})$. Hence it remains to prove for the case when $D = 23$. Consider the three reduced primitive quadratic forms of discriminant -23: $[1, 1, 6]$, $[2, 1, 3]$, $[2, -1, 3]$ For each of non principal quadratic forms $[2, 1, 3]$ and $[2, -1, 3]$, we may use the value $e^{\frac{-\sqrt{23}\pi}{4}}$ for the upper bound of s instead of $e^{-\sqrt{3}\pi}$ in inequality (6.17) so that we obtain the following inequality

$$|\mathfrak{g}_i^6(\tau_Q)| \leq 1.2e^{\frac{\sqrt{23}\pi}{12}} < 0.8e^{\frac{\sqrt{23}\pi}{6}} \leq |\mathrm{Re}(\mathfrak{g}_0^6(\tau_{23}))|$$

for all $i = 1, 2, 3$. Therefore, $(\mathfrak{g}_0^6 + \mathfrak{g}_1^6)(\tau_{23})$ is also a class invariant.

7. Concluding remarks

So far, we have investigated several real-valued class invariants and found their Galois traces are equal to the Zagier-Bruinier-Funke modular traces of certain modular functions at Heegner points. Furthermore, the generating series of their Galois traces are weakly holomorphic modular forms of weight 3/2. This may be generalized to arbitrary real-valued class invariants as follows:

Conjecture. *Suppose $-D$ is an imaginary quadratic discriminant and we let $\tau_D = \frac{-B+\sqrt{-D}}{2}$ as defined in (1.1). For a real-valued class invariant $g(\tau_D)$, there exists a modular function f and a suitable lattice L such that for some $h \in L^{\#}/L$ and a positive rational number m,*

$$\mathrm{GT}(g(\tau_D)) = \mathrm{MT}_f^L(h,m).$$

Moreover, the generating series of $\mathrm{GT}(g(\tau_D))$ is a weakly holomorphic modular form of weight 3/2 up to a finite principal form.

For complex-valued class invariants such as $\gamma_3(\tau_D)$ or $\mathfrak{g}_0(\tau_D)$, the conjecture above may not hold. For example, if $-D$ is an odd imaginary quadratic discriminant that is congruent to a square modulo 16, then by Theorem 4.1, the Galois trace of $\gamma_3(\tau_D)$ is given by

$$\mathrm{GT}_{\gamma_3}(\tau_D) = -\sum_{Q\in\mathcal{Q}_{D,(2),1}/\Gamma_0^0(2)} \gamma_3(\tau_Q) = \sum_{Q\in\mathcal{Q}_{D,(2),3}/\Gamma_0^0(2)} \gamma_3(\tau_Q).$$

But the modular trace of γ_3 with respect to the lattices L_1 and L_2 are both given by

$$\mathrm{MT}_{\gamma_3}^{L_1}(0,D) = \mathrm{MT}_{\gamma_3}^{L_2}(1,D/16) = \sum_{Q\in\mathcal{Q}_{D,(2),1}/\Gamma_0^0(2)} \gamma_3(\tau_Q) + \sum_{Q\in\mathcal{Q}_{D,(2),3}/\Gamma_0^0(2)} \gamma_3(\tau_Q) = 0.$$

In fact, as the Bruinier-Funke modular trace always count a positive quadratic form Q with its negative companion $-Q$ together, no lattice can work for this case. If we define a twisted modular trace

$$\mathrm{MT}_{\gamma_3}(\chi(\beta),D) = \sum_{Q\in\mathcal{Q}_{D,(2)}/\Gamma_0^0(2)} \chi(\beta)\gamma_3(\tau_Q),$$

where $\chi(1) = -1$ and $\chi(3) = 1$, then this is equal to $2\mathrm{GT}_{\gamma_3}(\tau_D)$, but we may not determine its modularity at this point as χ is not a genus character.

References

[1] Atkin, O. and Morain, F., 'Elliptic curves and primality proving', *Math. Comp.* 61 29-68 (1993)

[2] Berndt, B. C., Chan, H. H., Kang, S.-Y., and Zhang, L.-C., 'A certain quotient of eta functions found in Ramanujan's lost noptebook', *Pacific J. Math.* 202 267-304 (2002)

[3] Birch, B., 'Weber's class invariants', *Mathematika* 16 283-294 (1969)

[4] Bröker, R. M., Constructing elliptic curves of prescribed order, Ph.D. Thesis, Universiteit Leiden, 2006

[5] Bruinier, J. H. and Funke, J., 'Traces of CM-values of modular functions', *J. Reine Angew. Math.* 594 1–33 (2006)

[6] Bruinier, J. H., Jenkins, P., and Ono, K., 'Hilbert class polynomials and traces of singular moduli', *Math. Ann* 334 373–393 (2006)

[7] Chan, H. H., Gee, A., and Tan, V. 'Cubic singular moduli, Ramanujan's class invariants λ_n and the explicit Shimura reciprocity law', *Pacific J. Math.* 208 23–37 (2003)

[8] Cox, D., Primes of the form $x^2 + ny^2$, John Wiley & Sons, 1989

[9] Deuring, M., 'Die Klassenkörper der komplexen Multiplikation,'*in 'Enz. Math. Wiss. Band I_2'*, Heft 10, Teil II, Stuttgart, 1958

[10] Duke, W., 'Modular functions and the uniform distribution of CM points', *Math. Ann.* 334 241–252 (2006)
[11] Gee, A., 'Class invariants by Shimura's reciprocity law', *J. Théor. Nombre Bordeaux* 11 45–72 (1999)
[12] Gee, A., Class fields by Shimura reciprocity. Ph. D. Thesis, Universiteit van Amsterdam, 2001
[13] Gee, A. and Stevenhagen, P., 'Generating class fields using Shimura reciprocity', *Proceedings of the Third International Symposium on Algorithmic Number Theory,* Lecture Notes in Computer Sciences 1423, Springer-Verlag,, 441-453 1998
[14] Gross, B., Kohnen, W., and Zagier, D., 'Heegner points and derivatives of L-seires, II', *Math. Ann.* 278 497–562 (1987)
[15] Hart, W., 'Schläfli modular equations for generalized Weber functions', *Ramanujan J.* 15 435–468 (2008)
[16] Hajir, F. and Villegas, F. R., 'Explicit elliptic units, I', *Duke Math. J.* 90 (3) 495–521 (1997)
[17] Kaneko, M., 'The fourier coefficients and the singular moduli of the elliptic function $j(\tau)$', *Memoirs of the faculty of engineering and design,* Kyoto Institute of Technology 44, 1996
[18] Lang, S., Elliptic functions, 2nd edition, Springer GTM 112, 1987
[19] Morain, F., 'Primality proving using elliptic curves: An update', in Algorithmic Number Theory, Springer LNCS 1423, 111–130 1988
[20] Ono, K., Unearthing the visions of a master: Harmonic Maass forms and number theory, Harvard-MIT Current Developments in Mathematics, International Press, 2008
[21] Ramanujan, S., The Lost Notebook and other unpublished papers, Narosa, New Delhi, 1988
[22] Shertz, R., 'Die singulären Werte der Weberschen Funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, γ_2, γ_3', *J. Reine Angew. Math.* 286/287 46–74 (1976)
[23] Shertz, R., 'Weber's class invariants revisted', *J. Théor. Nombre Bordeaux* 14 325–343 (2002)
[24] Shimura, G., Introduction to the arithmetic theory of automorphic forms, Princeton University Press, 1971
[25] Stevenhagen, P., 'Hilbert's 12th problem, complex multiplication and Shimura reciprocity', Class field theory-its centenary and prospect, Edited by K. Miyake, *Adv. Studies in pure math.*, 30 161-176 (2001)
[26] Weber, H., Lehrbuch der Algebra, dritter Band, Friedrich Vieweg und Sohn, 1908
[27] Yui, N. and Zagier, D., 'On the singular values of Weber modular functions', *Math. Comp.* 66 no. 220 1645–1662 (1997)
[28] Zagier, D., 'Traces of singular moduli', *Motives, Polylogarithms and Hodge Theory, Part I,* edited by F. Bogomolov, and L. Katzarkov, 211-244, Somerville, MA: International Press, 2002

Kongju National University, Kongju, Chungnam 314-701, Korea
E-mail address: `dyjeon@kongju.ac.kr`

Korea Advanced Institute of Science and Technology, Department of Mathematical Sciences, Daejeon, 305-701 Korea
E-mail address: `s2kang@kaist.ac.kr`

Hanyang University, Seoul 133-791, KOREA
E-mail address: `chhkim@hanyang.ac.kr`