Trends in Mathematics - New Series
Information Center for Mathematical Sciences
Volume 11, Number 2, 2009, pages 1–8

ASARC Workshop
Daecheon & Muju 2009

TRACES OF CLASS INVARIANTS AND HILBERT CLASS POLYNOMIALS FOR ORDERS

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 modular functions of arbitrary genus at Heegner points. The purpose of this note is to give a survey of the recent work on modularity of Galois traces of class invariants in [8].

1. Introduction

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

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$$

and its value at 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

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

2000 *Mathematics Subject Classification.* 11F37; 11F30; 11G15; 11R27; 11R37.
Key words and phrases. class invariant, Galois trace, modular trace, Hilbert class polynomial, ring class field, Shimura reciprocity law, weakly holomorphic modular form.

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.

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

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

The corresponding generalized class polynomial is then given by [13],

$$\mathcal{H}_D(X):=\prod_{Q\in\mathcal{Q}_D/\Gamma(1)}(X-j(\tau_Q))^{1/|\Gamma(1)_Q|} \tag{1.4}$$

and its q-expansion at $j(\tau)$ is ([13, Eq. (11)])

$$\mathcal{H}_D(j(\tau))=q^{-H(D)}(1-\mathbf{t}_J(D)q+O(q^2)), \tag{1.5}$$

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,

$$\mathcal{H}_{23}(X)=X^3+3491750X^2-5151296875X+12771880859375\in\mathbb{Z}[X] \tag{1.6}$$

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 $\Gamma_0(4)$ [13]. This discovery of Zagier inspired a great number of works on traces of singular values (see [9, Section 13.1] for references). In particular, J. H. Bruinier and J. Funke [3] 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 $3/2$.

The Zagier-Bruinier-Funke modular trace of the value of a modular function at a Heegner point is naturally a Galois trace at the value. However, it is not trivial to see whether the Galois trace of a given algebraic integer is a Fourier coefficient of a certain automorphic form. But 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, then we can relate the Galois trace with the modular trace as there is an explicit description of its Galois conjugates under the action of the corresponding Galois group in terms of the action of a form class group. In his Lehrbuch der Algebra [12], H. Weber calls the value of a modular function $f(\tau_D)$ a *class invariant*

if we have

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

and gives several examples such as a holomorphic cube root $\gamma_2 : \mathbb{H} \to \mathbb{C}$ of 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 (1.6), the minimal polynomials of class invariants above produce much smaller coefficients. Computing Hilbert class polynomials is very important in number theory and its application to cryptography [1], [4]. The Shimura reciprocity law [10] provides a method of systematically determining whether $f(\tau_D)$ is a class invariant and also 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 [2], [5], [6], [7], [11].

2. Modularity of Galois traces of class invariants

In this section, 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.

The holomorphic cube root γ_2 of j is a modular function of level 3 and 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 2.1. *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*

$$(\zeta_3^B\gamma_2(\tau_D))^{[a,-b,c]} = \begin{cases} \zeta_3^{ab}\gamma_2(\tau_Q), & \text{if } 3 \nmid a, \\ \zeta_3^{-bc}\gamma_2(\tau_Q), & \text{if } 3 \mid a \text{ and } 3 \nmid c, \\ \gamma_2(\tau_Q), & \text{if } 3 \mid a \text{ and } 3 \mid c. \end{cases} \tag{2.1}$$

Of the three cases in (2.1), we consider 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

$$\mathcal{Q}_{D,(N),\beta} = \{[Na, b, Nc] \in \mathcal{Q}_D \mid b \equiv \beta \pmod{2N^2}\} \tag{2.2}$$

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. 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 $\mathcal{Q}_{D,(N),\beta}/\Gamma_0^0(N)$. Let $\mathrm{GT}_f(D)$ denote the modified Galois trace of a class invariant $f(\tau_D)$. By means of Theorem 2.1, 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

$$\mathrm{GT}_{\zeta_3^B\gamma_2}(D) = \sum_{Q \in \mathcal{Q}_{D,(3),\beta}/\Gamma_0^0(3)} \gamma_2(\tau_Q). \tag{2.3}$$

The Bruinier-Funke modular trace of γ_2 at a Heegner point is a sum of the traces given on the right-hand side of equation (2.3). For a weakly holomorphic modular function f on a 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 $\mathrm{MT}_f^L(h, m)$ that satisfies the following analytic property.

Theorem 2.2. [3, 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*

$$\sum_{n \gg -\infty} \mathrm{MT}_f^L(h, n) q^n \tag{2.4}$$

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 $\Gamma_0(4N)$ [3].

Suppose we use the lattice

$$L_1 = \left\{ X = \begin{pmatrix} b & 2Nc \\ 2Na & -b \end{pmatrix} \Big| a, b, c \in \mathbb{Z} \right\} \tag{2.5}$$

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 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

$$\mathbf{t}_f^{(\beta)}(D) := \sum_{Q \in \mathcal{Q}_{D,(N),\beta}/\Gamma_0^0(N)} \frac{1}{|\Gamma_0^0(N)_Q|} f(\tau_Q). \tag{2.6}$$

Then the Bruinier-Funke modular trace is given by

$$\mathrm{MT}_f^{L_1}(0, D) = 2 \sum_{\beta \in \mathbb{Z}/2N^2\mathbb{Z}} \mathbf{t}_f^{(\beta)}(D). \tag{2.7}$$

Since γ_2 is $\Gamma_0^0(3)$-invariant, the trace of γ_2 in (2.6) for discriminant $-D$ that is congruent to a square modulo 36 is well defined. Furthermore, from (2.3), (2.6), and (2.7), we find that the Galois trace of $\zeta_3^B \gamma_2(\tau_D)$ is a constant multiple of the modular trace.

Theorem 2.3. *For imaginary quadratic discriminant $-D$ which is congruent to a square modulo* 36 *and not divisible by* 3*,*

$$\mathrm{GT}_{\zeta_3^B \gamma_2}(D) = \frac{1}{4} \mathrm{MT}_{\gamma_2}^{L_1}(0, D). \tag{2.8}$$

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 2.1, 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

$$\gamma_2(\tau_{[6,25,27]}) + \gamma_2(\tau_{[9,25,18]}) + \gamma_2(\tau_{[3,7,6]}) = \mathbf{t}_{\gamma_2}^{(7)}(23)$$

so that the corresponding minimal polynomial has Heegner divisors:

$$\mathcal{H}_{23}^{\zeta_3 \gamma_2}(X) = \prod_{Q \in Q_{23,(3),7}/\Gamma_0^0(3)} (X - \gamma_2(\tau_Q)) \tag{2.9}$$

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. Thus, for any discriminant $-D < 0$ that is congruent to a square modulo 36, the equality in (2.8) holds. As γ_2 has zero constant coefficients at all cusps, we obtain the following result from Theorem 2.2.

Theorem 2.4. *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 2. Recall that $\gamma_2(\tau)=q^{-1/3}+O(q)$. Applying [3, Remark 4.9] with transformation properties of γ_2, we find that $\mathrm{MT}_{\gamma_2}(0,0)=0$. Also, on account of [3, 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

$$\sum_{n\in\mathbb{Z},\ n\gg-\infty}\mathrm{MT}_{\gamma_2}(0,n)q^n=4q^{-1}+O(q), \tag{2.10}$$

which is a weakly holomorphic modular form as asserted in Theorem 2.2.

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

Theorem 2.5. *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 $A(\tau)=\sum_{n\le0}a(n)q^n$ *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

$$L_2=\left\{X=\begin{pmatrix}Nb & c\\ a & -Nb\end{pmatrix}\Big|a,b,c\in\mathbb{Z}\right\} \tag{2.11}$$

with $q(X)=\det(X)$ and $(X,Y)=-\mathrm{tr}(XY)$. Suppose $-D$ is an imaginary quadratic discriminant such that $-D\equiv\square \pmod{4N^2}$. If f is a weakly holomorphic

modular function on $\Gamma_0^0(N)$, then the Bruinier-Funke modular trace is given by

$$\mathrm{MT}_f^{L_2}(h, D/4N^2) = \mathbf{t}_f^{(h)}(D) + \mathbf{t}_f^{(-h)}(D). \tag{2.12}$$

Theorem 2.6. *If 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 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 $B(\tau) = \sum_{n \le 0} b(n) q^n$ *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* $\Gamma(20736)$.

References

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

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

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

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

[5] Gee, A., 'Class invariants by Shimura's reciprocity law', *J. Théor. Nombre Bordeaux* 11 45–72 (1999)

[6] Gee, A., Class fields by Shimura reciprocity. Ph. D. Thesis, Universiteit van Amsterdam, 2001

[7] 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

[8] Jeon, Daeyeol, Kang, Soon-Yi, and Kim, Chang Heon, 'Modularity of Galois traces of class invariants', (submitted for publication)

[9] Ono, K., Unearthing the visions of a master: Harmonic Maass forms and number theory, Harvard-MIT Current Developments in Mathematics, International Press, 2008

[10] Shimura, G., Introduction to the arithmetic theory of automorphic forms, Princeton University Press, 1971

[11] 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)

[12] Weber, H., Lehrbuch der Algebra, dritter Band, Friedrich Vieweg und Sohn, 1908

[13] 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 for Science and Technology, Daejeon 305-701, KOREA
E-mail address: s2kang@kaist.ac.kr

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