T. Hiramatsu and Y. Mimura
Nagoya Math. J.
Vol. 100 (1985), 145-162

THE MODULAR EQUATION AND MODULAR FORMS OF WEIGHT ONE

TOYOKAZU HIRAMATSU AND YOSHIO MIMURA

Dedicated to Martin Eichler

§ 1. Introduction

This is a continuation of the previous paper [8] concerning the relation between the arithmetic of imaginary quadratic fields and cusp forms of weight one on a certain congruence subgroup. Let K be an imaginary quadratic field, say $K = \boldsymbol{Q}(\sqrt{-q})$ with a prime number $q \equiv -1 \bmod 8$, and let h be the class number of K. By the classical theory of complex multiplication, the Hilbert class field L of K can be generated by any one of the class invariants over K, which is necessarily an algebraic integer, and a defining equation of which is denoted by

$$\Phi(x) = 0\,.$$

The purpose of this note is to establish the following theorem concerning the arithmetic congruence relation for $\Phi(x)$:

THEOREM I. *Let p be any prime not dividing the discriminant D_Φ of $\Phi(x)$, and $\boldsymbol{F}_p$ the p-element field. Suppose that the ideal class group of K is cyclic. Then we have*

$$\#\{x \in \boldsymbol{F}_p \colon \Phi(x) = 0\} = \frac{h}{6}a(p)^2 + \frac{h}{6}a(p) - \frac{1}{2}\left(\frac{-q}{p}\right) + \frac{1}{2}\,,$$

where $a(p)$ denotes the pth Fourier coefficient of a cusp form which will be defined by (1) *in Section* 2.3 *below. One notes that in case $p = 2$, we have $(-q/p) = 1$.*

§ 2. Proof of Theorem I

2.1. Let Λ be a lattice in the complex plane $\boldsymbol{C}$, and define

Received August 22, 1984.

$$G_k(\Lambda) = \sum_{\omega \neq 0} \omega^{-k}, \quad (k \in \mathbf{Z}^+),$$
$$g_2(\Lambda) = 60\, G_4(\Lambda), \qquad g_3(\Lambda) = 140\, G_6(\Lambda),$$

where the sum is taken over all non-zero ω in Λ. The torus $\mathbf{C}/\Lambda$ is analytically isomorphic to the elliptic curve E defined by

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

via the Weierstrass parametrization

$$\mathbf{C}/\Lambda \ni z \longrightarrow (\wp(z), \wp'(z)) \in E,$$

where

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}, \qquad \wp'(z) = \sum_{\omega} \frac{-2}{(z-\omega)^3}.$$

Let Λ and M be two lattices in $\mathbf{C}$. Then the two tori $\mathbf{C}/\Lambda$ and $\mathbf{C}/M$ are isomorphic if and only if there exists a complex number α such that $\Lambda = \alpha M$. If this condition is satisfied, then the two lattices Λ and M are said to be linearly equivalent, and we write $\Lambda \sim M$. If so, we have a bijection between the set of lattices in $\mathbf{C}$ modulo $\sim$ and the set of isomorphism classes of elliptic curves. Let us define an invariant j depending only on the isomorphism classes of elliptic curves:

$$j(\Lambda) = \frac{1728\, g_2^3(\Lambda)}{g_2^3(\Lambda) - 27 g_3^2(\Lambda)}.$$

In fact, $j(\alpha\Lambda) = j(\Lambda)$ for all $\alpha \in \mathbf{C}$. Take a basis $\{\omega_1, \omega_2\}$ of Λ over $\mathbf{Z}$ such that $\mathrm{Im}(\omega_1/\omega_2) > 0$ and write $\Lambda = [\omega_1, \omega_2]$. Since $[\omega_1, \omega_2] \sim [\omega_1/\omega_2, 1]$, the invariant $j(\Lambda)$ is determined by $\tau = \omega_1/\omega_2$ which is called the moduli of E. Therefore we can write the following:

$$j(\Lambda) = j(\tau).$$

The lattice Λ has many different pairs of generators, the most general pair $\{\omega_1', \omega_2'\}$ with τ' in the upper half plane having the form

$$\begin{cases} \omega_1' = a\omega_1 + b\omega_2 \\ \omega_2' = c\omega_1 + d\omega_2 \end{cases}$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})$. Thus the function $j(\tau)$ is a modular function of level one. It is well known that

$$j(\sqrt{-1}) = 1728, \quad j(e^{2\pi\sqrt{-1}/3}) = 0, \quad j(\infty) = \infty .$$

The modular function $j(\tau)$ can be characterized by the above properties.

2.2. The classical theory of complex multiplication (M. Eichler [2], H. Hasse [4], and [13]). Let there be given a lattice Λ and the elliptic curve E as described in Section 2.1. If for some $\alpha \in \boldsymbol{C} - \boldsymbol{Z}$, $\wp(\alpha z)$ is a function on $\boldsymbol{C}/\Lambda$, then we say that E admits multiplication by α; and then α and ω_1/ω_2 are in the same quadratic field. If E admits multiplication by α_1 and α_2, then E admits multiplication by $\alpha_1 \pm \alpha_2$ and $\alpha_1\alpha_2$. Thus the set of all such α is an order in an imaginary quadratic field K. Consider the case when E admits multiplication by the maximal order $\mathfrak{o}_K$ in K. Then the invariant j defines a function on the ideal classes $k_0, k_1, \cdots, k_{h-1}$ of K (h being the class number of K) and the numbers $j(k_i)$ are called "singular values" of j. Put

$$A = \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n > 0,\ 0 \leqq b < d,\ (a, b, d) = 1,\ a, b, d \in \boldsymbol{Z}\right\},$$

and consider the polynomial

$$F_n(t) = \prod_{\alpha \in A} (t - j(\alpha z)) .$$

We may view $F_n(t)$ as a polynomial in two independent variables t and j over $\boldsymbol{Z}$, and write it as

$$F_n(t) = F_n(t, j) \in \boldsymbol{Z}[t, j] .$$

Let us put

$$H_n(j) = F_n(j, j) .$$

Then $H_n(j)$ is a polynomial in j with coefficients in $\boldsymbol{Z}$, and if n is not a square, then the leading coefficient of $H_n(j)$ is ± 1. This equation

$$H_n(j) = 0$$

is called the modular equation of order n. Now we can find an element w in $\mathfrak{o}_K$ such that the norm of w is square-free:

$$w = \begin{cases} 1 + \sqrt{-1}, \text{ if } K = \boldsymbol{Q}(\sqrt{-1}), \\ \sqrt{-m}, \text{ if } K = \boldsymbol{Q}(\sqrt{-m}) \text{ with } m > 1 \text{ square-free.} \end{cases}$$

Let $\{\omega_1, \omega_2\}$ be a basis of an ideal in an ideal class k_i such that $\operatorname{Im}(\omega_1/\omega_2) > 0$. Then

$$\begin{cases} w\omega_1 = a\omega_1 + b\omega_2 \\ w\omega_2 = c\omega_1 + d\omega_2 \end{cases}$$

with integers a, b, c, d and the norm of w is equal to $ad - bc$. Thus $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is primitive and $\alpha\omega = \omega$. Hence $j(\omega) = j(k_i)$ is a root of the modular equation $H_n(j) = 0$. Therefore we have the following

(i) $j(k_i)$ is an algebraic integer.

Furthermore we know

(ii) $K(j(k_i))$ is the Hilbert class field of K.

By the class field theory, there exists a canonical isomorphism between the ideal class group C_K of K and the Galois group G of $K(j(k_i))/K$, and we have the following formulas which describe how it operates on the generator $j(k_i)$:

(iii) Let σ_k be the element of G corresponding to an ideal class k by the canonical isomorphism. Then

$$\sigma_k(j(k')) = j(k^{-1}k')$$

for any $k' \in C_K$.

(iv) For each prime ideal $\mathfrak{p}$ of K of degree 1, we have

$$j(\mathfrak{p}^{-1}k) \equiv j(k)^{N\mathfrak{p}} \bmod \mathfrak{p}\,, \quad k \in C_K\,,$$

where $N\mathfrak{p}$ denotes the norm of $\mathfrak{p}$.

(v) The invariants $j(k_i)$, $i = 0, 1, \cdots, h-1$, of K form a complete set of conjugates over $\boldsymbol{Q}$.

2.3. Let q be a prime number such that $q \equiv -1 \bmod 8$, $K = \boldsymbol{Q}(\sqrt{-q})$ and let h be the class number of K, which is necessarily odd. For $0 \leqq i \leqq h-1$, we denote by $Q_{k_i}(x, y)$ the binary quadratic form corresponding to the ideal class k_i (k_0: principal class) in K and put

$$\theta_i(\tau) = \frac{1}{2} \sum_{n=0}^{\infty} A_{k_i}(n)\, e^{2\pi\sqrt{-1}\,n\tau} \quad (\mathrm{Im}\,(\tau) > 0)\,,$$

where $A_{k_i}(n)$ is the number of integral representations of n by the form Q_{k_i}. Then the following lemma is classical:

LEMMA 1. 1) *If p is any odd prime, except q, then we have*

$$\frac{1}{2} A_{k_0}(p) + \sum_{i=1}^{h-1} A_{k_i}(p) = 1 + \left(\frac{-q}{p}\right).$$

2) *If we identify opposite ideal classes by each other, there remain only* $A_{k_0}(p)$, $A_{k_1}(p), \cdots, A_{k_{(h-1)/2}}(p)$, *among which there is at most one non-zero element.*

Moreover, for each ideal class k in K, we have

LEMMA 2. 1) $A_k(n) = 2\#\{\mathfrak{a}\subset\mathfrak{o}_K\colon \mathfrak{a}\in k^{-1},\ N\mathfrak{a} = n\}$,
2) $2A_k(mn) = \sum_{\substack{k_1k_2=k \\ k_1,k_2\in C_K}} A_{k_1}(m)A_{k_2}(n)$ *if* $(m, n) = 1$.

Proof. 1) If $\mathfrak{b}\in k$ and $\mathfrak{b}\subset\mathfrak{o}_K$, then

$$\begin{aligned} A_k(n) &= \#\{\alpha\in\mathfrak{b}\colon N(\alpha) = nN\mathfrak{b}\} \\ &= \#\{\alpha\in\mathfrak{b}\colon (\alpha) = \mathfrak{a}\mathfrak{b},\ N\mathfrak{a} = n\} \\ &= 2\#\{\mathfrak{a}\subset\mathfrak{o}_K\colon \mathfrak{a}\in k^{-1},\ N\mathfrak{a} = n\}. \end{aligned}$$

2) For m, n coprime, take an ideal $\mathfrak{a}$ such that $\mathfrak{a}\in k^{-1}$, $\mathfrak{a}\subset\mathfrak{o}_K$ and $N\mathfrak{a} = mn$. Then we have the following unique decomposition of $\mathfrak{a}$:

$$\mathfrak{a} = \mathfrak{m}\mathfrak{n}, \quad N\mathfrak{m} = m, \quad N\mathfrak{n} = n.$$

If $\mathfrak{m}\in k_1^{-1}$, then $\mathfrak{n}\in k_2^{-1}$ $(= k_1k^{-1})$, and $\mathfrak{m}$ and $\mathfrak{n}$ are both integral. Therefore

$$\frac{1}{2}A_k(mn) = \sum_{k_1k_2=k}\left(\frac{1}{2}A_{k_1}(m)\right)\left(\frac{1}{2}A_{k_2}(n)\right). \qquad \text{Q.E.D.}$$

Let χ be any character $(\neq 1)$ on the group C_K of ideal classes and put

$$A(n) = \frac{1}{2}\sum_{k_i\in C_K}\chi(k_i)A_{k_i}(n).$$

Then we have the following multiplicative formulas.

LEMMA 3. 1) $A(mn) = A(m)A(n)$ *if* $(m, n) = 1$,
2) $A(p)A(p^r) = A(p^{r+1}) + (-q/p)A(p^{r-1})$ *for prime* p $(\neq q)$ and $r \geqq 1$,
3) $A(qn) = A(q)A(n)$.

Proof. These follow immediately from Lemma 2 by the direct computation.

We define here two functions f and F as follows:

$$f(\tau) = \theta_0(\tau) - \theta_1(\tau), \tag{1}$$

and

$$F(\tau) = \sum_{i=0}^{h-1}\chi(k_i)\theta_i(\tau) = \sum_{n=1}^{\infty}A(n)e^{2\pi\sqrt{-1}n\tau}, \tag{2}$$

where $\theta_0(\tau)$ is the theta-function corresponding to the principal class k_0. Then $f(\tau)$ is a normalized cusp form on the congruence subgroup $\Gamma_0(q)$ of weight one and character $(-q/p)$, and moreover, by Lemma 3, $F(\tau)$ is a normalized new form on $\Gamma_0(q)$ of weight one and character $(-q/p)$ (cf. Hecke [7]). From now on, we assume that the ideal class group C_K of K is cyclic. By Lemma 1 we shall calculate the Fourier coefficients of $f(\tau)$ and $F(\tau)$. Let

$$C_K = \langle k_1 \rangle \quad \text{and} \quad \chi(k_1) = e^{2\pi\sqrt{-1}/h}\,.$$

Then we can write the function $F(\tau)$ as

$$F(\tau) = \theta_0(\tau) + 2\sum_{i=1}^{\frac{1}{2}(h-1)} \cos\frac{2\pi i}{h}\,\theta_i(\tau)\,,$$

where $k_i = k_1^i$ $(1 \leqq i \leqq \frac{1}{2}(h-1))$. If $(-q/p) = -1$, then $A_k(p) = 0$ for all $k \in C_K$. If $(-q/p) = 1$, then

$$(p) = \mathfrak{p}\bar{\mathfrak{p}} \quad (\mathfrak{p} \neq \bar{\mathfrak{p}}) \quad \text{in } K\,,$$

where $\mathfrak{p}$ denotes a prime ideal in K and $\bar{\mathfrak{p}}$ a conjugate of $\mathfrak{p}$. We denote by $k_{\mathfrak{p}}$ the ideal class such that $\mathfrak{p} \in k_{\mathfrak{p}}$. If $k_{\mathfrak{p}}$ is ambigous, then

$$A_k(p) = \begin{cases} 4, & \text{for } k = k_{\mathfrak{p}}^{-1}\,, \\ 0, & \text{otherwise.} \end{cases}$$

If k is not ambigous, then

$$A_k(p) = \begin{cases} 2, & \text{for } k = k_{\mathfrak{p}} \text{ or } k = k_{\mathfrak{p}}^{-1}\,, \\ 0, & \text{otherwise}. \end{cases}$$

In the case $p = q$, put

$$(p) = \mathfrak{p}^2 \ (\mathfrak{p} = \bar{\mathfrak{p}}), \quad \mathfrak{p} \in k_{\mathfrak{p}}\,.$$

Then we know

$$A_k(p) = \begin{cases} 2, & \text{if } k = k_{\mathfrak{p}}\,, \\ 0, & \text{otherwise}. \end{cases}$$

Let $a(n)$ be the nth coefficient of the Fourier expansion for $f(\tau)$:

$$f(\tau) = \sum_{n=1}^{\infty} a(n) e^{2\pi\sqrt{-1}n}\,.$$

By the above results, we have the following formulas for $a(p)$ and $A(p)$.

LEMMA 4. *Suppose that the ideal class group C_K of K is cyclic. Then, for each prime p, the Fourier coefficients $a(p)$ and $A(p)$ are given as follows:*

$$a(p)=\begin{cases}0, & \text{if } \left(\frac{-q}{p}\right)=-1\,,\\ 2, & \text{if } \left(\frac{-q}{p}\right)=1 \text{ and } p=x^2+xy+\frac{1+q}{4}y^2 \quad (x, y\in \boldsymbol{Z})\,,\\ 0 \text{ or } 1, & \text{if } \left(\frac{-q}{p}\right)=1 \text{ and } k_{\mathfrak{p}}\neq k_0 \text{ with } (p)=\mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p}\in k_{\mathfrak{p}}\,,\\ 1, & \text{if } p=q\,,\end{cases}$$

and

$$A(p)=\begin{cases}0, & \text{if } \left(\frac{-q}{p}\right)=-1\,,\\ 2, & \text{if } \left(\frac{-q}{p}\right)=1 \text{ and } p=x^2+xy+\frac{1+q}{4}y^2 \quad (x, y\in \boldsymbol{Z})\,,\\ 2\cos\frac{2\pi n}{h}, & \text{if } \left(\frac{-q}{p}\right)=1 \text{ and } k_{\mathfrak{p}}=k_n^{\pm 1}(\neq k_0) \text{ with } (p)=\mathfrak{p}\bar{\mathfrak{p}}\,,\\ & \qquad \mathfrak{p}\in k_{\mathfrak{p}} \quad (1\leqq n\leqq \frac{1}{2}(h-1))\,.\end{cases}$$

2.4. Let

$$\Phi(x)=0$$

be the defining equation of a generating element of the Hilbert class field L over the imaginary quadratic field $K=\boldsymbol{Q}(\sqrt{-q})$. Then the polynomial $\Phi(x)$ is one of the irreducible factors of the modular polynomial $H_q(x)$. We say simply $\Phi(x)$ is a modular polynomial.

Now, in order to prove Theorem I, it is enough to show that if the ideal class group C_K is a cyclic group of order h, then

$$\#\{x\in \boldsymbol{F}_p\colon \Phi(x)=0\}$$
$$=\begin{cases}1, & \text{if } \left(\frac{-q}{p}\right)=-1\,,\\ h, & \text{if } \left(\frac{-q}{p}\right)=1 \text{ and } p=x^2+xy+\frac{1+q}{4}y^2 \quad (x, y\in \boldsymbol{Z}),\\ 0, & \text{if } \left(\frac{-q}{p}\right)=1 \text{ and } k_{\mathfrak{p}}\neq k_0 \text{ with } (p)=\mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p}\in k_{\mathfrak{p}}\,.\end{cases}$$

We denote by H the ideal group corresponding to the Hilbert class field L of K:

$$H=\{(\alpha)\colon \text{principal ideals in } K\}\,.$$

Case 1. $(-q/p) = 1$. Let

$$(p) = \mathfrak{p}\bar{\mathfrak{p}} \quad \text{in } K.$$

Then we have the following relations:

$$\mathfrak{p} \in H \Longleftrightarrow \mathfrak{p} = (\pi),\ \pi = a + b\omega \quad \left(\omega = \frac{1+\sqrt{-q}}{2},\ a,\ b \in \boldsymbol{Z}\right)$$
$$\Longleftrightarrow p = N\mathfrak{p} = a^2 + ab + \frac{1+q}{4} b^2 \quad (a,\ b \in \boldsymbol{Z}),$$

and

$$\mathfrak{p} \text{ splits completely in } L \Longleftrightarrow \Phi(x) \bmod p \text{ has exactly } h \text{ factors.}$$

Therefore

$$p = a^2 + ab + \frac{1+q}{4} b^2 \ (a,\ b \in \boldsymbol{Z}) \Longleftrightarrow \Phi(x) \bmod p \text{ has exactly } h \text{ factors.}$$

On the other hand, it is obvious that

$$\mathfrak{p} \notin H \Longleftrightarrow \mathfrak{p} \text{ is a product of prime ideals of degree} > 1 \text{ in } L$$
$$\Longleftrightarrow \Phi(x) \bmod p \text{ has no linear factors in } \boldsymbol{F}_p[x].$$

Case 2. $(-q/p) = -1$. The polynomial $\Phi(x)$ splits completely modulo p in $\mathfrak{o}_K/(p)$ and the field $\mathfrak{o}_K/(p)$ is a quadratic extension of $\boldsymbol{Z}/p\boldsymbol{Z}$. Therefore

$$\Phi(x) \bmod p = h_1(x) \cdots h_t(x)$$

and

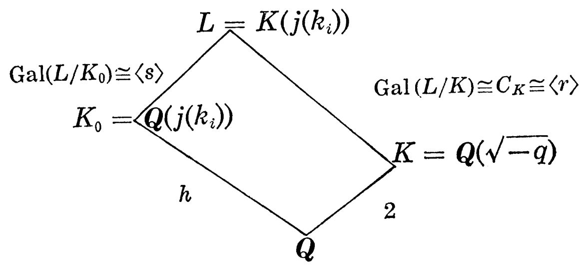
$$\deg h_i \leqq 2 \quad (i = 1, \cdots, t),$$

where each $h_i(x)$ is irreducible in $\boldsymbol{F}_p[x]$. Since the class number h of K is odd, there exist odd numbers of i such that $\deg h_i = 1$. In the following, we shall show that there exists one and only one of such i.

The dihedral group D_h has $2h$ elements and is generated by r, s with the defining relations:

$$r^h = s^2 = 1, \qquad srs = r^{-1}.$$

Let K_0 be the maximal real subfield of L. We have the following diagram:



Let $\mathfrak{o}_{K_0}$ be the ring of algebraic integers in K_0. Then the ideal $p\mathfrak{o}_{K_0}$ decomposes into a product of distinct prime ideals in K_0:

$$p\mathfrak{o}_{K_0} = \mathfrak{p}_1 \cdots \mathfrak{p}_m \mathfrak{q}_1 \cdots \mathfrak{q}_n ,$$

where

$$N_{K_0/\boldsymbol{Q}}\mathfrak{p}_l = p \quad (1 \leqq l \leqq m) \quad \text{and} \quad N_{K_0/\boldsymbol{Q}}\mathfrak{q}_l = p^2 \quad (1 \leqq l \leqq n) .$$

Moreover, if $\mathfrak{o}_L$ is the ring of algebraic integers in L, then

$$\mathfrak{p}_l \mathfrak{o}_L = \mathfrak{P}_l \quad (1 \leqq l \leqq m) ,$$

where each $\mathfrak{P}_l$ is a prime ideal in $\mathfrak{o}_L$. On the other hand, the ideal $p\mathfrak{o}_L$ has the following decomposition via the field K:

$$p\mathfrak{o}_L = \mathfrak{P}_1 \mathfrak{P}_1^r \cdots \mathfrak{P}_1^{r^{h-1}} .$$

Since $\mathfrak{p}_1^s = \mathfrak{p}_1$, we have also

$$\mathfrak{P}_1^s = \mathfrak{P}_1 .$$

Similarly,

$$\mathfrak{P}_l^s = \mathfrak{P}_l , \quad (2 \leqq l \leqq m) .$$

However, since h is odd and $srs = r^{-1}$, we deduce

$$\mathfrak{P}_1^{r^i s} = \mathfrak{P}_1^{r^{-i}} \neq \mathfrak{P}_1^{r^i} , \quad (1 \leqq i \leqq h-1) .$$

Since $\mathfrak{P}_l = \mathfrak{P}_1^{r^i}$ for some i, we have $m = 1$. Q.E.D.

Let $\operatorname{Spl}\{\Phi(x)\}$ be the set of all primes p such that $\Phi(x) \bmod p$ factors into a product of distinct linear polynomials over the field $\boldsymbol{F}_p$. Then the following Corollary holds:

COROLLARY (Higher Reciprocity Law).

$$\operatorname{Spl}\{\Phi(x)\} = \left\{ p : p \nmid D_\Phi, \left(\frac{-q}{p}\right) = 1 \quad \textit{and} \quad a(p) = 2 \right\} .$$

2.5. The Schläfli modular equation. The problem of determining the modular polynomial $F_n(t, j)$ explicitly for an arbitrary order n was treated by N. Yui [11]. But, even for $n = 2$, $F_2(t, j)$ has an astronomically long form. We shall use here the Schläfli modular function $h_0(\tau)$ in place of $j(\tau)$:

$$h_0(\tau) = e^{-(\pi\sqrt{-1})/24} \frac{\eta((\tau+1)/2)}{\eta(\tau)} = e^{-(\pi\sqrt{-1}\tau)/24} \prod_{n=1}^{\infty} (1 + e^{(2n-1)\pi\sqrt{-1}\tau}) ,$$

where η is Dedekind's eta function. This function $h_0(\tau)$ is the modular function for the principal congruence subgroup of level 48 and has the following properties:

$$j(\tau) = \frac{\{h_0(\tau)^{24} - 16\}^3}{h_0(\tau)^{24}} \quad \text{and} \quad h_0\left(-\frac{1}{\tau}\right) = h_0(\tau).$$

LEMMA 5 (H. Weber [10]). *Let q be any prime number such that $q \equiv -1 \bmod 8$. Then*

1) $\sqrt{2}\, h_0(\sqrt{-q}) \in \boldsymbol{Q}(j(\sqrt{-q}))$,

2) $\sqrt{1/2}\, h_0(\sqrt{-q})$ *is a unit of an algebraic number field.*

Put

$$x = \frac{1}{\sqrt{2}} h_0(\sqrt{-q}).$$

Then, by Lemma 5. 1), we have

$$\boldsymbol{Q}(x) = \boldsymbol{Q}(j(\sqrt{-q})).$$

The defining equation of x is called the Schläfli modular equation. It will be useful to recall Weber's method for an explicit expression of this equation (H. Weber [10], §§ 73–75 and § 131). We shall explain its outline in brief. Put

$$h_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)}, \quad h_2(\tau) = \frac{\sqrt{2}\,\eta(2\tau)}{\eta(\tau)};$$
$$u = h_0(\tau), \quad u_1 = h_1(\tau), \quad u_2 = h_2(\tau);$$

and

$$v = h_0\left(\frac{c+d\tau}{a}\right), \quad v_1 = \left(\frac{2}{a}\right) h_1\left(\frac{c+d\tau}{a}\right), \quad v_2 = \left(\frac{2}{d}\right) h_2\left(\frac{c+d\tau}{a}\right),$$

where $(2/\ )$ is a Jacobi symbol and $ad = n$ is a positive integer such that $n \equiv -1 \bmod 8$. Put

$$\begin{cases} 2A = uv + (-1)^{(n+1)/8}(u_1 v_1 + u_2 v_2), \\ B = \dfrac{2}{u_1 v_1} + \dfrac{2}{u_2 v_2} + (-1)^{(n+1)/8} \dfrac{2}{uv}. \end{cases}$$

Then there is a polynomial relation between A and B with integer coefficients, which depend on n but not on a, c, d. If we put

$$\tau = \frac{-1}{\sqrt{-n}},$$

then

$$h_0(n\tau) = h_0(\tau) = h_0(\sqrt{-n}).$$

Therefore, putting $h_0(\sqrt{-n}) = \sqrt{2}\,x$, we have

$$\text{(3)} \qquad \begin{cases} A = x^2 + (-1)^{(n+1)/8}\dfrac{1}{x}, \\ B = 4x + (-1)^{(n+1)/8}\dfrac{1}{x^2}. \end{cases}$$

Substitute (3) in the above polynomial relation. Then we obtain an equation of x with integer coefficients, which is known as Schläfli's modular equation of order n.

EXAMPLE. $n = 47$ (H, Weber [10], § 75 and § 131). A relation between A and B is given by

$$A^2 - A - B = 2,$$

and we have the following Schläfli's modular equation of order 47:

$$x^5 - x^3 - 2x^2 - 2x - 1 = 0.$$

§ 3. The case of $q = 47$

3.1. Let $\mathfrak{o}_K$ be the principal order of the imaginary quadratic field $K = \boldsymbol{Q}(\sqrt{-47})$ and put

$$\mathfrak{o}_K = [1, \omega], \qquad \omega = \frac{1 + \sqrt{-47}}{2}.$$

The field K has class number 5. Let

$$Q_0(x, y) = x^2 + xy + 12y^2,$$
$$Q_1(x, y) = 7x^2 + 3xy + 2y^2,$$
$$Q_2(x, y) = 3x^2 - xy + 4y^2,$$

be the binary quadratic forms corresponding to the ideals $\mathfrak{o}_K$, $[7, 1 + \omega]$, $[3, \omega]$, respectively, and let

$$\theta_i(\tau) = \frac{1}{2}\sum_{n=0}^{\infty} A_{Q_i}(n) e^{2\pi\sqrt{-1}n\tau} \quad (i = 0, 1, 2)$$

be the theta-functions belonging to the above binary quadratic forms, respectively, where $A_{Q_i}(n)$ denotes the number of integral representations of n by the form Q_i. By Lemma 1, we have easily the following table:

		$A_{Q_0}(p)$	$A_{Q_1}(p)$	$A_{Q_2}(p)$
$\left(\frac{-47}{p}\right) = -1$		0	0	0
$\left(\frac{-47}{p}\right) = 1$	$p = x^2 + 47y^2$	4	0	0
	$7p = x^2 + 47y^2$	0	2	0
	$3p = x^2 + 47y^2$	0	0	2

For $p = 2, 47$, we know

$$A_{Q_0}(2) = A_{Q_2}(2) = 0\,, \quad A_{Q_1}(2) = 2\,;$$
$$A_{Q_0}(47) = 2\,, \quad A_{Q_1}(47) = A_{Q_2}(47) = 0\,.$$

Now we define two functions as follows:

$$F_1(\tau) = \theta_0(\tau) - \theta_1(\tau) = \sum_{n=1}^{\infty} a(n) e^{2\pi\sqrt{-1}n\tau}\,,$$
$$F_2(\tau) = \theta_0(\tau) - \theta_2(\tau)\,.$$

Then $F_1(\tau)$ and $F_2(\tau)$ are normalized cusp forms on the group $\Gamma_0(47)$ of weight one and character $(-47/p)$ (cf., Hecke [7]). Put $\varepsilon_0 = \frac{1}{2}(1 + \sqrt{5})$, and define

$$F_3(\tau) = \bar{\varepsilon}_0 F_1 + \varepsilon_0 F_2(\tau) = F_1(\tau) + \varepsilon_0 \eta(\tau)\eta(47\tau) = \sum_{n=1}^{\infty} A(n) e^{2\pi\sqrt{-1}n\tau}\,.$$

Then the function $F_3(\tau)$ is also a normalized cusp form of weight one and character $(-47/p)$ on the group $\Gamma_0(47)$, and the Fourier coefficient $A(n)$ is multiplicative. The Fourier coefficients of $F_1(\tau)$ and $F_3(\tau)$ are obtained by the above table as follows, respectively. For each prime p ($\neq 2, 47$), we have

$$(4) \qquad a(p) = \begin{cases} 0 & \text{if } \left(\frac{-47}{p}\right) = -1\,, \\ 2 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad p = x^2 + 47y^2 \quad (x, y \in \boldsymbol{Z})\,, \\ 0 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad 3p = x^2 + 47y^2 \quad (x, y \in \boldsymbol{Z})\,, \\ -1 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad 7p = x^2 + 47y^2 \quad (x, y \in \boldsymbol{Z})\,, \end{cases}$$

and

$$(5)\qquad A(p)=\begin{cases} 0 & \text{if } \left(\dfrac{-47}{p}\right)=-1,\\ 2 & \text{if } \left(\dfrac{-47}{p}\right)=1 \quad\text{and}\quad p=x^2+47y^2 \quad (x,y\in \boldsymbol{Z}),\\ -\varepsilon_0 & \text{if } \left(\dfrac{-47}{p}\right)=1 \quad\text{and}\quad 3p=x^2+47y^2 \quad (x,y\in \boldsymbol{Z}),\\ -\bar{\varepsilon}_0 & \text{if } \left(\dfrac{-47}{p}\right)=1 \quad\text{and}\quad 7p=x^2+47y^2 \quad (x,y\in \boldsymbol{Z}).\end{cases}$$

Futhermore we know that $a(2)=-1$, $a(47)=A(47)=1$ and $A(2)=-\bar{\varepsilon}_0$.

3.2. An arithmetic congruence relation for the Fricke polynomial. Put

$$h_0(\tau)=\frac{e^{-(\pi\sqrt{-1})/24}\eta((\tau+1)/2)}{\eta(\tau)}$$

and

$$h_0(\sqrt{-47})=\sqrt{2}\,x\,.$$

Then the class invariant x satisfies the following Schläfli's modular equation of order 47 (cf. § 2.5):

$$(6)\qquad f_W(x)=x^5-x^3-2x^2-2x-1=0 \quad (D_{f_W}=47^2)\,.$$

Let L be the Hilbert class field over K. Then the field L is a splitting field for the polynomial

$$(7)\qquad f_H(x)=x^5-2x^4+2x^3-3x^2+6x-5 \quad (D_{f_H}=11^2\cdot 47^2)\,,$$

and the Galois group $G(L/\boldsymbol{Q})$ is equal to the dihedral group D_5 (Hasse [5], Hasse and Liang [6]). Put

$$\eta_0=\frac{1}{2}\left(\frac{47-5\sqrt{5}}{2}+\frac{-5+\sqrt{5}}{2}\sqrt{47\sqrt{5}\,\varepsilon_0}\right)$$

and

$$\omega_0=\frac{9353+422\sqrt{5}}{4}-\frac{715+325\sqrt{5}}{4}\sqrt{47\sqrt{5}\,\varepsilon_0}\,,$$

then from Hasse [5] we deduce that

$$\theta_H=\frac{1}{5}\left(\sqrt[5]{\omega_0}-\frac{1}{\sqrt[5]{\omega_0}}-\frac{\sqrt[5]{\omega_0^2}}{\eta_0}+\frac{\eta_0}{\sqrt[5]{\omega_0^2}}+2\right)$$

generates L/K. Consider the following equation (Fricke [3], p. 492):

$$f_F(x) = x^5 - x^4 + x^3 + x^2 - 2x + 1 = 0. \tag{8}$$

It is known that there are two relations

$$\begin{cases} \theta_H = 5\theta_W^2 - 5\theta_W - 2, \\ \theta_W = \ -\theta_F^4 - 2\theta_F + 1 \end{cases} \tag{9}$$

for the real roots θ_W, θ_H and θ_F of (6), (7) and (8), respectively (Zassenhaus and Liang [12]). Put

$$f_M(x) = x^5 - 2x^4 + 3x^3 + x^2 - x - 1.$$

The discriminant of $f_M(x)$ is $5^2 \cdot 47^2$. By a simple calculation, we verify

$$x^2 - ax + b \mid f_F(x) \Longleftrightarrow f_H(a) f_M(a) = 0, \tag{10}$$

where a and b denote any constants. If θ is the real root of the equation $f_M(x) = 0$, then we obtain the following relations by making use of a handy computer:

$$\begin{cases} \theta_H = 2\theta_F^4 - \theta_F^3 + \theta_F^2 + 2\theta_F - 2, \quad \text{(by (9))} \\ \theta = -2\theta_F^4 + \theta_F^3 - \theta_F^2 - 3\theta_F + 3, \\ \theta_F = \dfrac{-1}{11}(\theta_H^4 + \theta_H^3 + 5\theta_H^2 + \theta_H - 2), \\ \theta = \dfrac{1}{11}(\theta_H^4 + \theta_H^3 + 5\theta_H^2 - \theta_H + 9), \\ \theta_F = \dfrac{1}{5}(\theta^4 - 5\theta^3 + 8\theta^2 - 8\theta - 2), \\ \theta_H = \dfrac{1}{5}(-\theta^4 + 5\theta^3 - 8\theta^2 + 3\theta + 7). \end{cases} \tag{11}$$

Now we consider $f_F(x) \bmod p$ for any odd prime number p ($\neq 47$). Because of (10) and (11), the reduced polynomial $f_F \bmod p$ ($p \neq 5, 11$) can factor over the p-element field F_p in one of three ways:

(i) Five linear factors,

(ii) (Linear) (Quadratic) (Quadratic),

(iii) (Quintic).

The reduced polynomials $f_F \bmod 5$ and $f_F \bmod 11$ have the above type (ii). When we combine this with the results of Section 4.1, we are led to the following which is a special case of Theorem I:

THEOREM II. *Let p be any prime, except 47, and F_p the field of p-elements. Let $a(n)$ be the nth coefficient of the expansion*

$$F_1(\tau) = \sum_{n=1}^{\infty} a(n) e^{2\pi\sqrt{-1}n\tau}.$$

Then the following arithmetic congruence relation holds:

$$\#\{x \in F_p : f_F(x) = 0\} = \frac{5}{6}a(p)^2 + \frac{5}{6}a(p)^2 - \frac{1}{2}\left(\frac{-47}{p}\right) + \frac{1}{2},$$

where for $p = 2$, we understand $(-47/2) = 1$.

Proof. In order to prove this, it is enough to show the following fact. Let L_p be a splitting field of $f_F(x) \bmod p$ over the field F_p. Then it can easily be seen that

$$\begin{aligned}\left(\frac{-47}{p}\right) = -1 &\Longleftrightarrow [L_p : F_p] = 2 \\ &\Longleftrightarrow f_F \bmod p \text{ has exactly one linear factor over } F_p \\ &\Longleftrightarrow f_F \bmod p \text{ can factor in type (ii).}\end{aligned}$$

Remark 1. Let p be a prime, except 5, 11 and 47. Then, by the relation (11), $f_F \bmod p$, $f_H \bmod p$, $f_W \bmod p$ and $f_M \bmod p$ can factor over F_p in the same way. Using Fourier coefficients of $F_2(\tau)$, we have also the same arithmetic congruence relation for $f_F(x)$. On the other hand, using Fourier coefficients of $F_3(\tau)$, we have the following relation:

$$\#\{x \in F_p : f_F(x) = 0\} = A(p)^2 + A(p) - \left(\frac{-47}{p}\right).$$

Finally the following higher reciprocity law for the Fricke polynomial $f_F(x)$ holds:

COROLLARY. $\mathrm{Spl}\{f_F(x)\} = \{p : (-47/p) = 1$ *and* $a(p) = 2\}$.

Remark 2. A similar result was obtained for some other cases (cf. T. Hiramatsu [8] and J.-P. Serre [9]).

§ 4. Remark

4.1. The dihedral group D_h has $(h+3)/2$ conjugate classes:

$$\{1\},\quad \{sr^i : 1 \leqq i \leqq h\},\quad \{r^j, r^{-j}\},\quad j = 1, 2, \cdots, \frac{h-1}{2}.$$

Thus we have $(h-1)/2$ irreducible representations of degree 2. Among them, here we consider the representation ρ given by the following

$$\rho(r)=\begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^{-1}\end{pmatrix}, \qquad \rho(s)=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$

where $\varepsilon=e^{2\pi i/h}$. The corresponding character is given by the following table:

	$\{1\}$	$\{r^j, r^{-j}\}$	$\{sr^i\colon 1\leqq i\leqq h\}$
ρ	2	$2\cos\dfrac{2\pi j}{h}$	0

$$j=1,\cdots,\frac{h-1}{2}.$$

Let $\phi(s)$ be the Dirichlet series associated to the new form $F(\tau)$ (cf. (2) in § 2.3) via the Mellin transform. Since the function $F(\tau)$ is an eigen-function of all the Hecke operators T_p, U_p, the Dirichlet series $\phi(s)$ has the following Euler product:

$$\begin{aligned}\phi(s)&=\sum_{n=1}^{\infty}A(n)n^{-s}=(1-A(q)q^{-s})^{-1}\prod_{p\neq q}\left(1-A(p)p^{-s}+\left(\frac{-q}{p}\right)p^{-2s}\right)\\&=(1-q^{-s})^{-1}\prod_{(-q/p)=-1}(1-p^{-2s})^{-1}\prod_{p\in P_1}(1-2p^{-s}+p^{-2s})^{-1}\\&\qquad\times\prod_{p\in P_2}\left(1+2\cos\frac{2\pi n}{h}p^{-s}+p^{-2s}\right)^{-1},\end{aligned}$$

where

$$P_1=\left\{p\colon\left(\frac{-q}{p}\right)=1,\ p=x^2+xy+\frac{1+q}{4}y^2\right\},$$

and

$$P_2=\left\{p\colon\left(\frac{-q}{p}\right)=1,\ p=\mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p}\neq\text{principal},\ \mathfrak{p}\in k_n\right\}\cup\{2\}.$$

4.2. Let L be the Hilbert class field of the imaginary quadratic field K, and assume that the Galois group $G(L/K)$ is a cyclic group of order h. Then $L/\boldsymbol{Q}$ is a non-abelian Galois extension with D_h as Galois group. Let p be any prime number and σ_p a Frobenius map of p in L, and put

$$A_p=\frac{1}{e}\sum_{\tau\in T}\rho(\sigma_p\tau),$$

where T is the inertia group of p and $\sharp T=e$. Then, for the Galois extension $L/\boldsymbol{Q}$, the Artin L-function is defined by

$$L(s, \rho, L/\boldsymbol{Q}) = \prod_p \det\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - A_p N(p)^{-s}\right)^{-1}, \quad \mathrm{Re}\,(s) > 1\,.$$

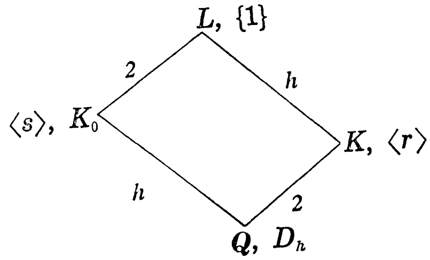
A prime p factorizes in L in one of the following ways:

Case 1. $(-q/p) = -1$. Decomposition field K_0, $\sigma_p = s$, $A_p = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

Case 2. $p \in P_1$. Decomposition field $= L$, $\sigma_p = 1$, $A_p = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$.

Case 3. $p \in P_2$. Decomposition field $= K$. If $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \in k_n^{-1}$, then $\sigma_p = r^n$ and $A_p = \begin{pmatrix}\varepsilon^n & 0\\ 0 & \varepsilon^{-n}\end{pmatrix}$.

Case 4. $p = q$. Ramification exponent $= 2$. $\sigma_q = 1$. $A_q = \frac{1}{2}(\rho(1) + \rho(s)) = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$.



In order to have the explicit form of $L(s, \rho, L/\boldsymbol{Q})$, we use the above results and obtain

$$\begin{aligned} L(s, \rho, L/\boldsymbol{Q}) &= \prod_p \det\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - A_p N(p)^{-s}\right)^{-1} \\ &= \det\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - q^{-s}\cdot\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\right)^{-1} \prod_{(-q/p)=-1} \det\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - p^{-s}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right)^{-1} \\ &\quad \times \prod_{p\in P_1} \det\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - p^{-s}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)^{-1} \prod_{p\in P_2} \det\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - p^{-s}\begin{pmatrix}\varepsilon^n & 0\\ 0 & \varepsilon^n\end{pmatrix}\right)^{-1}. \end{aligned}$$

It is clear that the above Euler product, compared with the Euler product of $\phi(s)$, proves the following:

$$L(s, \rho, L/\boldsymbol{Q}) = \phi(s)\,.$$

This is a constructive version for the dihedral case of the Weil-Langlands-Deligne-Serre theorem (P. Deligne et J.-P. Serre [1]).

References

[1] P. Deligne et J.-P. Serre, Formes modulaires de poids 1, Ann. Sci. École Norm. Sup., **4** (1974), 507–530.
[2] M. Eichler, Der Hilbertsche Klassenkörper eines imaginärquadratischen Zahlkörper, Math. Z., **64** (1956), 229–242.
[3] R. Fricke, Lehrbuch der Algebra III, Braunschweig 1928.
[4] H. Hasse, Neue Begründung der komplexen Multiplikation, I: J. Reine Angew. Math., **157** (1927), 115–139, II: Ibid., **165** (1931), 64–88.
[5] ——, Uber den Klassenkorper zum quadratischen Zahlkorper mit der Diskriminate -47, Acta Arith., **9** (1964), 419–434.
[6] H. Hasse and J. Liang, Uber den Klassenkorper zum quadratischen Zahlkorper mit der Diskriminate -47 (Fortsetzung), Acta Arith., **16** (1969), 89–97.
[7] E. Hecke, Zur Theorie der elliptischen Modulfunktionen, Math. Ann., **97** (1926), 210–242 (= Math. Werke, 461–486).
[8] T. Hiramatsu, Higher reciprocity laws and modular forms of weight one, Comm. Math. Univ. St. Paul, **31** (1982), 75–85.
[9] J.-P. Serre, Modular forms of weight one and Galois representations, Proc. Symposium on Algebraic Number Field, Academic Press, London, 1977, pp. 193–268.
[10] H. Weber, Lehrbuch der Algebra III, Braunschweig 1908.
[11] N. Yui, Explicit form of the modular equation, J. Reine Angew. Math., **299/300** (1978), 185–200.
[12] H. Zassenhaus and J. Liang, On a problem of Hasse, Math. Comp., **23** (1969), 515–519.
[13] Seminar on Complex Multiplication, Lecture Notes in Math. No. 21, Springer-Verlag, Berlin, Heidelberg, New York 1966 (from the Institute Seminar by Borel, Chowla, Herz, Iwasawa, Serre, held in 1957–58).

Department of Mathematics
Kobe University
Rokko, Kobe, 657
Japan