On Hilbert modular forms modulo $p$: explicit ring structure

Shoyu Nagaoka

Abstract

H. P. F. Swinnerton-Dyer determined the structure of the ring of modular forms modulo $p$ in the elliptic modular case. In this paper, the structure of the ring of Hilbert modular forms modulo $p$ is studied. In the case where the discriminant of corresponding quadratic field is 8 (or 5), the explicit structure is determined.

1. Introduction

In [9] Swinnerton-Dyer determined the structure of the ring of modular forms modulo $p$ in the elliptic modular case. The result has been applied in several fields in the theory of modular forms, for example, the $p$–adic theory of modular forms (e.g. cf. Serre [8]). In this note, we try to generalize the result to the case of symmetric Hilbert modular forms for real quadratic fields of small discriminant. We have already developed a generalization in the Siegel modular case of degree 2, which is important in our proof (cf. Theorem 4.1). A geometric approach has been developed in recent studies by E. Goren (for example, [3] and [4]).

2. Hilbert modular forms for a real quadratic field

Let $K$ be a real quadratic field with the discriminant $d_{K}$ and the ring of integers $O_{K}$. We denote by $\mathbb{H}$ the upper-half plane in $\mathbb{C}$. The Hilbert modular group $\Gamma_{K} := SL(2, O_{K})$ acts on $\mathbb{H}^{2} = \mathbb{H} \times \mathbb{H}$ by

$$
\begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix} \circ (z_1, z_2) := \left( \frac{az_1 + b}{cz_1 + d}, \frac{\bar{a}z_2 + \bar{b}}{\bar{c}z_2 + d} \right),
$$

where $\bar{x}$ denotes the conjugation of $x \in K$ over $\mathbb{Q}$.

2000 Mathematics Subject Classification: 11F41.

Keywords: Hilbert modular forms, modular forms mod $p$. 
Let $A_{\mathbb{C}}(\Gamma_K)_k$ be the complex vector space of symmetric Hilbert modular forms of parallel weight $k$ for $\Gamma_K$. Each element $f(\tau)$ of $A_{\mathbb{C}}(\Gamma_K)_k$ admits a Fourier expansion of the form

$$f(\tau) = \sum_{0 < \nu \in \mathfrak{d}_K^{-1}} a_f(\tau) \exp \left[ 2\pi \sqrt{-1} \text{tr}(\nu \tau) \right],$$

where $\tau = (z_1, z_2) \in \mathbb{H}^2$, $\text{tr}(\nu \tau) = \nu z_1 + \bar{\nu} z_2$ and the summation is extended over the elements $\nu$ in the inverse different $\mathfrak{d}_K^{-1}$ which are semi-totally positive.

From now on, we restrict ourselves to the case $K = \mathbb{Q}(\sqrt{2})$.

(There is another case $K = \mathbb{Q}(\sqrt{5})$ where our discussion leads to similar results: cf. section 5, Remark (2)).

In this case, we have $d_K = 8$ and $d_K = 2\sqrt{2} \mathcal{O}_K$. We fix an integral basis $\{1, \sqrt{2}\}$ and introduce new variables:

$$x =: \exp \left[ \pi \sqrt{-1}(z_1 - z_2)/\sqrt{2} \right], \quad q = \exp \left[ \pi \sqrt{-1}(z_1 + z_2) \right].$$

Then, the above Fourier expansion is rewritten as

$$f(\tau) = \sum_{\nu = (\alpha + \beta \sqrt{2})/2\sqrt{2}} a_f(\nu) x^\alpha q^\beta$$

$$= a_f(0) + a_f((-1 + \sqrt{2})/2\sqrt{2}) x^{-1} q + a_f(1/2) q + a_f((1 + \sqrt{2})/2\sqrt{2}) x q$$

$$+ a_f((-2 + 2\sqrt{2})/2\sqrt{2}) x^{-2} q^2 + a_f((-1 + 2\sqrt{2})/2\sqrt{2}) x^{-1} q^2 + a_f(1) q^2$$

$$+ a_f((1 + 2\sqrt{2})/2\sqrt{2}) x q^2 + a_f((2 + 2\sqrt{2})/2\sqrt{2}) x^2 q^2 + \cdots.$$

By semi-positivity of $\nu$, we may regard $f$ as an element of formal power series ring $\mathbb{C} [x^{-1}, x] \llbracket q \rrbracket$. For a subring $R$ in $\mathbb{C}$,

$$A_R(\Gamma_K)_k := \{ f \in A_{\mathbb{C}}(\Gamma_K)_k \mid a_f(\nu) \in R \text{ for all } \nu \} \subset R [x^{-1}, x] \llbracket q \rrbracket$$

and

$$A_R^{(m)}(\Gamma_K) := \bigoplus_{k \geq 0} A_R(\Gamma_K)_k \llbracket q \rrbracket.$$

For an even positive integer $k$, we can define the normalized Eisenstein series of weight $k$ for $\Gamma_K$ whose Fourier expansion is

$$G_k(\tau) = 1 + \kappa_k \sum_{\nu \in \mathfrak{d}_K^{-1}} \sigma_{k-1}(\nu) \exp \left[ 2\pi \sqrt{-1} \text{tr}(\nu \tau) \right]$$

where $\sigma_{k-1}(\nu)$ is the $(k-1)$th elementary symmetric polynomial in the $\nu$'s.
where
\[ \kappa_k := \zeta_K(k)^{-1} \cdot (2\pi)^{2k} \cdot [(k - 1)!]^{-2} \cdot d_K^{1/2-k}, \]
\[ \sigma_{k-1}(\nu) := \sum_{\nu \in \mathbb{Z}^d \subset b} |N(b)|^{k-1}. \]

Since \( \kappa_k \in \mathbb{Q} \), we have \( G_k \in A_Q(\Gamma_K) \).

Let \( E_k(z) \) be the normalized Eisenstein series of weight \( k \) for \( SL(2, \mathbb{Z}) \), and let \( \Delta(z) \) be a cusp form defined by
\[ \Delta(z) = 2^{-6} \cdot 3^{-3} (E^3_4(z) - E^2_6(z)). \]

It is well-known that \( E_k \in A_Q(SL(2, \mathbb{Z}))_k \) and \( \Delta \in A_Z(SL(2, \mathbb{Z}))_{12} \).

For a function \( f((z_1, z_2)) \) on \( \mathbb{H}^2 \), we define a function on \( \mathbb{H} \) by
\[ \mathbb{D}(f)(z) := f((z, z)). \]

By the definition of Hilbert modular form, we see that the map \( \mathbb{D} \) induces an \( R \)-linear map
\[ \mathbb{D} : A_R(\Gamma_K) \to A_R(SL(2, \mathbb{Z}))_{2k}. \]

In fact, if
\[ f(\tau) = \sum a_f(\nu) \exp \left[ 2\pi \sqrt{-1} \text{tr}(\nu \tau) \right] \]
in \( A_R(\Gamma_K) \), then the Fourier expansion of \( \mathbb{D}(f) \) is
\[ \mathbb{D}(f)(z) = \sum_{n=0}^{\infty} c_f(n) \exp \left[ 2\pi \sqrt{-1} nz \right], \quad c_f(n) = \sum_{\text{tr}(\nu)=n} a_f(\nu). \]

Put
\[ H_2 := G_2 \]
\[ = 1 + 2^4 \cdot 3 \left\{ (x^{-1} + 3 + x)q + (7x^{-2} + 8x^{-1} + 15 + 8x + 7x^2)q^2 + \cdots \right\}, \]
\[ H_4 := 2^{-6} \cdot 3^{-2} \cdot 11(G_2^2 - G_4) \]
\[ = (x^{-1} - 2 + x)q + (-4x^{-2} - 8x^{-1} + 24 - 8x - 4x^2)q^2 \cdots, \]
\[ H_6 := -2^{-8} \cdot 3^{-3} \cdot 13^{-1} \cdot 5 \cdot 7^2G_2^3 - 2^{-7} \cdot 3^{-3} \cdot 5^{-1} \cdot 13^{-1} 19^2G_6 \]
\[ + 2^{-8} \cdot 3^{-2} \cdot 5^{-1} \cdot 13^{-1} \cdot 11 \cdot 59G_2G_4 \]
\[ = q + (-2x^{-2} - 16x^{-1} + 12 - 16x - 2x^2)q^2 + \cdots. \]
Proposition 2.1 Let \( \mathbb{Z}_{(p)} \) be the local ring at \( p \) (\( p \) : prime).

1. \( H_k \in A_{\mathbb{Z}}(\Gamma_K)_k \subset A_{\mathbb{Z}_{(p)}}(\Gamma_K)_k \) (\( k = 2, 4, 6 \)) and
\[
\mathbb{D}(H_2) = E_4, \mathbb{D}(H_4) = 0, \mathbb{D}(H_6) = \Delta.
\]

2. If \( f \in A_{\mathbb{Z}_{(p)}}(\Gamma_K)_k \), (\( k \): even), then there exists a polynomial \( P(X_1, X_2, X_3) \in \mathbb{Z}_{(p)}[X_1, X_2, X_3] \) satisfying
\[
f = P(H_2, H_4, H_6).
\]

Namely,
\[
A_{\mathbb{Z}_{(p)}}(\Gamma_K) = \mathbb{Z}_{(p)}[H_2, H_4, H_6].
\]

Proposition 2.2 ([6, Propositions 3.1, 3.2])

1. There exists an odd weight form \( H_9 \) with integral Fourier coefficients:
\[
H_9 = q - (96^{-1} x + 336 + 96x)q^2 + \cdots \in A_{\mathbb{Z}}(\Gamma_K)_9 \subset A_{\mathbb{Z}_{(p)}}(\Gamma_K)_9.
\]

2. If \( k \) is odd, then \( A_{\mathbb{Z}_{(p)}}(\Gamma_K)_k = H_9 \cdot A_{\mathbb{Z}_{(p)}}(\Gamma_K)_{k-9} \).

3. \( H_9^2 \) has a polynomial expression in \( H_2, H_4, \) and \( H_6 \):
\[
H_9^2 = H_2^3 H_6^2 + 2^2 H_2^2 H_4^2 H_6 - 2^5 \cdot 3^2 H_2 H_4 H_6^2 - 2^{10} H_4^3 H_6 - 2^6 \cdot 3^3 H_6^3.
\]

3. Siegel modular form and modular embedding

Let \( A_{\mathbb{C}}(\Gamma_K)_k \) be the complex vector space of Siegel modular forms of weight \( k \) for \( \Gamma_n := Sp(n, \mathbb{Z}) \). As is well known, each element \( F(Z) \) in \( A_{\mathbb{C}}(\Gamma_n)_k \) admits a Fourier expansion of the form
\[
F(Z) = \sum_{T \geq 0} a_F(T) \exp \left[ 2\pi \sqrt{-1} \text{tr}(TZ) \right], Z \in \mathbb{H}_n,
\]
where \( \mathbb{H}_n \) is the Siegel upper-half space of degree \( n \) and the summation is extended over all half-integral, positive semi-definite, symmetric matrices of degree \( n \). As in the previous case, we can define an \( R \)-module \( A_R(\Gamma_n)_k \).

We now introduce a modular embedding from \( A_{\mathbb{C}}(\Gamma_K)_k (K = \mathbb{Q}(\sqrt{2})) \) to \( A_{\mathbb{C}}(\Gamma_2)_k \).

We fix a fundamental unit \( \varepsilon = 1 + \sqrt{2} \) in \( \mathcal{O}_K \) and define a matrix \( A \) by
\[
A = \begin{pmatrix} \alpha & \bar{\alpha} \\ \bar{\alpha} & -\alpha \end{pmatrix}, \quad \alpha = \sqrt{\varepsilon/2\sqrt{2}}, \bar{\alpha} = \sqrt{-\varepsilon/2\sqrt{2}}.
\]
First, we define a mapping \( \Phi : \mathbb{H}^2 = \mathbb{H} \times \mathbb{H} \rightarrow \mathbb{H}_2 \) by

\[
\Phi(\tau) = \Phi((z_1, z_2)) := A \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} A = \begin{pmatrix} \text{tr}((\frac{\epsilon}{2}\sqrt{2})\tau) & \text{tr}((1/2\sqrt{2})\tau) \\ \text{tr}((1/2\sqrt{2})\tau) & \text{tr}((-\frac{\epsilon}{2}\sqrt{2})\tau) \end{pmatrix}.
\]

Secondly, we define a mapping \( \Psi : \Gamma_K = SL(2, \mathcal{O}_K) \rightarrow \Gamma_2 = Sp(2, \mathbb{Z}) \) by

\[
\Psi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = \Psi \left( \begin{pmatrix} a_1 + a_2\sqrt{2} & b_1 + b_2\sqrt{2} \\ c_1 + c_2\sqrt{2} & d_1 + d_2\sqrt{2} \end{pmatrix} \right) = \begin{pmatrix} a_1 + a_2 & a_2 & b_1 + b_2 & b_2 \\ a_2 & a_1 - a_2 & b_2 & b_1 - b_2 \\ c_1 + c_2 & c_2 & d_1 + d_2 & d_2 \\ c_2 & c_1 - c_2 & d_2 & d_1 - d_2 \end{pmatrix}.
\]

**Proposition 3.1** ([6, Proposition 2.1]) If \( F \) is a Siegel modular form in \( A_C(\Gamma_2)_k \), then \( \Phi(F) = F \circ \Phi \) is a symmetric Hilbert modular form in \( A_C(\Gamma_K)_k \).

We calculate the Fourier coefficient of \( \Phi(F) \). Set

\[
F(Z) = \sum_{T \geq 0} a_F(T) \exp \left[ 2\pi \sqrt{-1}\text{tr}(TZ) \right].
\]

We take a half-integral, positive semi-definite matrix

\[
T = \begin{pmatrix} m & l/2 \\ l/2 & n \end{pmatrix}, \quad (m, n, l \in \mathbb{Z}).
\]

Since

\[
\exp \left[ 2\pi \sqrt{-1}\text{tr}(T\Phi(\tau)) \right] = x^{m-n+l}q^{m+n},
\]

we have

\[
\Phi(F)(\tau) = \sum_{(\alpha+\beta\sqrt{2})/2 \geq 0} \sum_{\frac{m-n+l}{m+n} = \alpha} a_F \left( \begin{pmatrix} m & l/2 \\ l/2 & n \end{pmatrix} \right) x^\alpha q^\beta.
\]

**Corollary 3.1** Let \( R \) be a subring of \( \mathbb{C} \). If \( F \in A_R(\Gamma_2)_k \), then

\[
\Phi(F) \in A_R(\Gamma_K)_k.
\]
4. Hilbert modular form modulo $p$

As before, $p$ be a prime number, and let $\mathbb{Z}_{(p)}$ be the local ring at $p$. We set

$$A_{\mathbb{Z}_p}^p(\Gamma_K)_k := \{ \tilde{\mathcal{f}} = \sum a_f(\nu)x^\alpha q^\beta | f \in A_{\mathbb{Z}_p}(\Gamma_K)_k \}$$

$$\subset \mathbb{F}_p[x^{-1}, x][q],$$

where the tilde denotes the reduction modulo $p$. Let $A_{\mathbb{F}_p}^{(m)}(\Gamma_K)$ denote the subring of $\mathbb{F}_p[x^{-1}, x][q]$ generated by $A_{\mathbb{F}_p}(\Gamma_K)_k$ for $k = 0, m, 2m, 3m, \ldots$. The first theorem is as follows.

**Theorem 4.1 (Existence Theorem)** Assume that $K = \mathbb{Q}(\sqrt{2})$ and $p \geq 3$. Then, there exists a Hilbert modular form $f_{p-1} \in A_{\mathbb{Z}_p}(\Gamma_K)_{p-1}$ satisfying

$$f_{p-1} \equiv 1 \pmod{p},$$

where the congruence is the Fourier coefficientwise congruence.

**Proof.** First assume that $p \geq 5$. By [7, Theorem A] there exists a Siegel modular form $F_{p-1} \in A_{\mathbb{Z}_p}(\Gamma_2)_{p-1}$ satisfying

$$F_{p-1} \equiv 1 \pmod{p}.$$  

If we set

$$f_{p-1} := \Phi(F_{p-1}),$$

then, by (3.3), we see that

$$f_{p-1} \in A_{\mathbb{Z}_p}(\Gamma_K)_{p-1}$$

has the desired property. When $p = 3$, we can take $f_{p-1} = f_2 = G_2$. □

**Remark.** In the original (elliptic modular) case, it is easy to find such modular form: the weight $p - 1$ Eisenstein series $E_{p-1}$ satisfies $E_{p-1} \equiv 1 \pmod{p}$. However, the Hilbert-Eisenstein series $G_{p-1}$ does not satisfy the congruence $G_{p-1} \equiv 1 \pmod{p}$ in general. In fact, $G_2 \not\equiv 1 \pmod{13}$ (for example, [3, p. 373]).

In the following we shall determine the structure of $A_{\mathbb{Z}_p}^{(2)}(\Gamma_K)$ under the condition

$$p \equiv 3 \pmod{4}.$$
Theorem 4.2 Assume that $\mathbb{K} = \mathbb{Q}(\sqrt{2})$.

(1) If $p \geq 5$ is a prime number such that $p \equiv 3 \pmod{4}$, then

$$A_{\mathbb{F}_p}^{(2)}(\Gamma_\mathbb{K}) \cong \mathbb{F}_p [\bar{H}_2, \bar{H}_4, \bar{H}_6] / (\bar{A}_p(\bar{H}_2, \bar{H}_4, \bar{H}_6) - 1)$$

where $H_2, H_4,$ and $H_6$ are generators of $A_{\mathbb{Z}(p)}^{(2)}(\Gamma_\mathbb{K})$ (cf. Proposition 2.1) and $A_p(X_1, X_2, X_3) \in \mathbb{Z}(p)[X_1, X_2, X_3]$ is a polynomial defined by

$$f_{p-1} = A_p(H_2, H_4, H_6).$$

(2) If $p = 2$ or 3, then

$$A_{\mathbb{F}_p}^{(2)}(\Gamma_\mathbb{K}) \cong \mathbb{F}_p [\bar{H}_4, \bar{H}_6].$$

Proof. (1) We recall the identities

$$\mathbb{D}(H_2) = E_4, \quad \mathbb{D}(H_4) = 0, \quad \mathbb{D}(H_6) = \Delta$$

and consider the following diagram:

$$\begin{array}{ccc}
\mathbb{Z}(p)[X_1, X_2, X_3] & \longrightarrow & \mathbb{F}_p[X_1, X_2, X_3] \\
\mathbb{D}' \downarrow & & \mathbb{D}' \downarrow \\
\mathbb{Z}(p)[Y_1, Y_2] & \longrightarrow & \mathbb{F}_p[Y_1, Y_2] \\
\mathbb{D} \downarrow & & \mathbb{D} \downarrow \\
& & \mathbb{F}_p[\bar{H}_4, \bar{H}_6] \\
\end{array}$$

where

$$\varphi : \quad \varphi(\bar{P}(X_1, X_2, X_3)) := \bar{P}(\bar{H}_2, \bar{H}_4, \bar{H}_6).$$

$$\varphi' : \quad \varphi'(\bar{Q}(Y_1, Y_2)) := \bar{Q}(\bar{E}_4, \bar{E}_6).$$

$$\mathbb{D}' : \quad \mathbb{D}'(P(X_1, X_2, X_3)) := P(Y_1, 0, 2^{-6} \cdot 3^{-3}(Y_1^3 - Y_2^2)).$$

$$\mathbb{D}' : \quad \mathbb{D}'(\bar{P}(X_1, X_2, X_3)) := \bar{P}(Y_1, 0, \bar{a}(Y_1^3 - Y_2^2)), \quad \bar{a} = 2^{-6} \cdot 3^{-3} \text{ mod } p.$$

By Proposition 2.1,(2), the map $\varphi$ is surjective. For the Hilbert modular form $f_{p-1}$, we represent it as a polynomial in $H_2, H_4,$ and $H_6$

$$f_{p-1} = A_p(H_2, H_4, H_6), A_p(X_1, X_2, X_3) \in \mathbb{Z}(p)[X_1, X_2, X_3].$$

The congruence $f_{p-1} \equiv 1 \pmod{p}$ implies $\bar{A}_p - 1 \in \text{Ker} \varphi$. Therefore it suffices to show that

$$\text{Ker} \varphi = (\bar{A}_p - 1) \quad \text{(principal ideal)}.$$
To prove this, we first note that
\[ \text{Im} \tilde{\mathcal{D}} = A^{(4)}_{F_p}(SL(2, \mathbb{Z})) \subset A^{(2)}_{F_p}(SL(2, \mathbb{Z})) \]
and
\[ \text{Krull dim} A^{(4)}_{F_p}(SL(2, \mathbb{Z})) = \text{Krull dim} A^{(2)}_{F_p}(SL(2, \mathbb{Z})) = 1. \]
The first identity in the second formula comes from the fact that \( \tilde{E}_6 \) is integral over \( A^{(4)}_{F_p}(SL(2, \mathbb{Z})) \). Since \( \text{Ker} \tilde{D} \neq 0 \) (for example, \( 0 \neq \tilde{H}_4 \in \text{Ker} \tilde{D} \)), we have
\[ \text{Krull dim} A^{(2)}_{F_p}(\Gamma_K) = 2. \]
Hence, the irreducibility of \( \tilde{A}_p - 1 \) implies our statement:
\[ A^{(2)}_{F_p}(\Gamma_K) \cong F_p[\tilde{H}_2, \tilde{H}_4, \tilde{H}_6] / (\tilde{A}_p(\tilde{H}_2, \tilde{H}_4, \tilde{H}_6) - 1) \]
We shall show the irreducibility under the condition \( p \equiv 3 \pmod{4} \). For this purpose, we recall the corresponding fact in the elliptic modular case. The normalized Eisenstein series \( E_{p-1} \) satisfies \( E_{p-1} \equiv 1 \pmod{p} \). Moreover, if we represent \( E_{p-1} \) as
\[ E_{p-1} = B_p(E_4, E_6) \quad \text{with} \quad B_p(Y_1, Y_2) \in \mathbb{Z}_p[Y_1, Y_2], \]
then \( B_p(Y_1, Y_2) - 1 \) is irreducible in \( F_p[Y_1, Y_2] \) (cf. \( [9] \)). From this fact, we get the decomposition
\[ (4.1) \quad \tilde{\mathcal{D}}'(\tilde{A}_p(X_1, X_2, X_3) - 1) = (\tilde{B}_p(Y_1, Y_2) + 1)(\tilde{B}_p(Y_1, Y_2) - 1). \]
Here, we note that both factors \( \tilde{B}_p + 1 \) and \( \tilde{B}_p - 1 \) are irreducible. Now we assume that \( \tilde{A}_p - 1 \) is reducible. Then, the shape of the decomposition must be
\[ (4.2) \quad \tilde{A}_p - 1 = (\tilde{G}^{(a)} + \tilde{G}^{(a-1)} + \ldots + \tilde{G}^{(0)})(\tilde{H}^{(a)} + \tilde{H}^{(a-1)} + \ldots + \tilde{H}^{(0)}), \]
where \( G^{(j)} \) (also \( H^{(j)} \)) is a polynomial consisting of terms such as
\[ a_{\alpha \beta \gamma} X_1^\alpha X_2^\beta X_3^\gamma \]
with \( 2\alpha + 4\beta + 6\gamma = j \), namely, terms of isobaric degree \( j \). Combining (4.1) and (4.2), we have \( 2a = p - 1 \). Since \( a \) is even, the prime \( p \) must be congruent to one modulo 4. This contradicts our assumption. (2) If \( p = 2 \) or \( 3 \), then \( \tilde{H}_2 = 1 \). Moreover, \( \tilde{H}_4 \) and \( \tilde{H}_6 \) are algebraically independent because the Fourier expansion of \( H_4 \) (resp. \( H_6 \)) starts at the term \( (x^{-1} - 2 + x)q \) (resp. \( q \)).
From the above result and Proposition 2.2, we can easily determine the structure of the whole ring $A_{F_3} (\Gamma_\mathbb{K}) = A_{F_2} (\Gamma_\mathbb{K})$.

Set

$$C(X_1, X_2, X_3, X_4) := X_1^3X_3^2 + 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^5 \cdot X_1X_2X_3^2 - 2^{10}X_3^2X_3 - 2^6 \cdot 3^3X_3^3 - X_3^4 \in \mathbb{Z}[X_1, X_2, X_3, X_4]$$

It should be noted that the polynomial is chosen as

$$C(H_2, H_4, H_6, H_9) = 0, \quad \text{(cf. (2.3))}.$$ 

Let $\tilde{C}_p(X_1, X_2, X_3, X_4) \in F_p [X_1, X_2, X_3, X_4]$ be the reduction modulo $p$. Combining this and Theorem 4.2, we obtain the following:

**Theorem 4.3** Assume that $\mathbb{K} = \mathbb{Q}(\sqrt{2})$.

1. If $p \geq 5$ and $p \equiv 3 \pmod{4}$, then
   $$A_{F_3} (\Gamma_\mathbb{K}) \cong \mathbb{F}_p [\tilde{H}_2, \tilde{H}_4, \tilde{H}_6, \tilde{H}_9] / (\tilde{A}_p (\tilde{H}_2, \tilde{H}_4, \tilde{H}_6) - 1, \tilde{C}_p (\tilde{H}_2, \tilde{H}_4, \tilde{H}_6, \tilde{H}_9)).$$

2. If $p = 2$ or $3$,
   $$A_{F_2} (\Gamma_\mathbb{K}) \cong \mathbb{F}_p [\tilde{H}_4, \tilde{H}_6, \tilde{H}_9] / (\tilde{C}_p),$$
   that is
   $$A_{F_3} (\Gamma_\mathbb{K}) \cong \mathbb{F}_2 [\tilde{H}_4, \tilde{H}_6] / (\tilde{H}_6^2 + \tilde{H}_6^2 \tilde{H}_6 + 2\tilde{H}_6 + 2\tilde{H}_6^2),$$
   $$A_{F_2} (\Gamma_\mathbb{K}) = \mathbb{F}_2 [\tilde{H}_4, \tilde{H}_6].$$

5. **Remark**

1. Case $p \equiv 1 \pmod{4}$:
   In the above discussion, the result was restricted to the case $p \equiv 3 \pmod{4}$. What about the case $p \equiv 1 \pmod{4}$? In this case also, the irreducibility of $\tilde{A}_p - 1$ produces similar results. The first few examples show the irreducibility.

   - $p = 5$: $\tilde{A}_5 - 1 = X_1^2 + 4X_2 - 1, \quad D'(\tilde{A}_5 - 1) = Y_1^2 - 1, \quad \tilde{B}_5 - 1 = Y_1 - 1.$
   - $p = 7$: $\tilde{A}_7 - 1 = X_1^3 + 3X_1X_2 + X_3 - 1, \quad D'(\tilde{A}_7 - 1) = Y_2^2 - 1, \quad \tilde{B}_7 - 1 = Y_2 - 1.$
   - $p = 11$: $\tilde{A}_{11} - 1 = X_1^5 + 2X_1^3X_2 + 10X_1X_2^2 + X_1^2X_3 + X_2X_3 - 1, \quad D'(\tilde{A}_{11} - 1) = Y_3^2Y_2 - 1, \quad \tilde{B}_{11} - 1 = Y_1Y_2 - 1.$
   - $p = 13$: $\tilde{A}_{13} - 1 = X_1^6 + 11X_1^3X_2 + 3X_1^3X_3 + 11X_1^2X_2^2 + 2X_1X_2X_3 + 10X_3^3 + 12X_3^2 - 1, \quad D'(\tilde{A}_{13} - 1) = 10Y_1^6 + 5Y_1^3Y_2^2 + 12Y_1^3Y_2^2 - 1, \quad \tilde{B}_{13} - 1 = 6Y_1^3 + 8Y_2^2 - 1.$
(2) Case for $\mathbb{K} = \mathbb{Q}(\sqrt{5})$:

The proposed method is applicable for the case $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. In this paper, we present the statement without proof.

Let $G_k$ be the normalized Eisenstein series of weight $k$ for $\Gamma_{\mathbb{Q}(\sqrt{5})}$. We define four modular forms $J_k(k = 2, 6, 10, 12)$ as follows:

\[
J_2 := G_2 = 1 + 2^3 \cdot 3 \cdot 5 \left\{ (x^{-1} + x)q + (x^{-4} + 5x^{-2} + 6 + 5x^2 + x^4)q^2 + \cdots \right\},
\]

\[
J_6 := 2^{-5} \cdot 3^{-3} \cdot 5^{-2} \cdot 67(G_2^2 - G_6) = (x^{-1} + x)q + (x^{-4} + 20x^{-2} - 90 + 20x^2 + x^4)q^2 + \cdots,
\]

\[
J_{10} := 2^{-10} \cdot 3^{-5} \cdot 5^{-5} \cdot 7^{-1}(412751 G_{10} - 5 \cdot 67 \cdot 2293 G_2^2 G_6 + 2^2 \cdot 3 \cdot 7 \cdot 4231 G_2^2)
= (x^{-1} - x)^2 q^2 - 2(x^{-1} - x)(x^{-4} + 10x^{-2} - 10x^2 - x^4)q^3 + \cdots,
\]

\[
J_{12} := 2^{-2} (J_6^2 - J_2 J_{10}) = q^2 + (x^{-5} - 15x^{-3} - 10x^{-1} - 10x - 15x^3 + x^5)q^3 + \cdots,
\]

where $x = \exp \left[ \pi \sqrt{-1}(z_1 - z_2)/\sqrt{5} \right]$, $q = \exp \left[ \pi \sqrt{-1}(z_1 + z_2) \right]$.

**Theorem 5.1 (Existence Theorem)** Assume that $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ and $p \geq 3$. Then, there exists a Hilbert modular form $f_{p-1} \in A_{\mathbb{Z}(p)}(\Gamma_{\mathbb{K}})_{p-1}$ satisfying

\[ f_{p-1} \equiv 1 \pmod{p}. \]

**Theorem 5.2** Assume that $\mathbb{K} = \mathbb{Q}(\sqrt{5})$.

(1) If $p \geq 5$ is a prime number such that $p \equiv 3 \pmod{4}$, then

\[
A_p^{(2)}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p[\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}]/(A_p(\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}) - 1)
\]

where $J_2, J_6, J_{10}$ are generators of $A_{\mathbb{Z}(p)}^{(2)}(\Gamma_{\mathbb{K}})$ and

\[ A_p(X_1, X_2, X_3) \in \mathbb{Z}(p)[X_1, X_2, X_3] \]

is a polynomial defined by

\[ f_{p-1} = A_p(J_2, J_6, J_{10}). \]

(2)

\[
A_p^{(2)}(\Gamma_{\mathbb{K}}) = \mathbb{F}_3[\tilde{J}_6, \tilde{J}_{10}],
\]

\[
A_p^{(2)}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_2[\tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{12}]/(\tilde{J}_6^2 + \tilde{J}_{10}^2). \]
Proposition 5.1 ([6, Theorem 3.1 and Proposition 3.3])

(1) There exists an odd weight form $J_{15}$ with integral Fourier coefficients:

$$J_{15} = q^2 - (x^{-5} + 275x^{-1} + 275x + x^5)q^3 + \cdots \in A_2(\Gamma_0)_{15} \subset A_2(p)(\Gamma_0)_{15}.$$ 

(2) If $k$ is odd, then $A_{Z(p)}(\Gamma_0)_k = J_{15} \cdot A_{Z(p)}(\Gamma_0)_{k-15}.$

(3) $J^2_{15}$ has the following polynomial expressions:

$$J^2_{15} = 5^3 J^3_{10} - 2 \cdot 3^3 J^5_6 + 2 \cdot 5^2 J^6_2 J^3_{10} + 2 \cdot 5^3 J^3_2 J^5_6 J^3_{10} + 2 \cdot 5 J^3_2 J^5_6 J^3_{10} + J^3_2 J^5_{12}$$

$$= 5^3 J^3_{10} - 2 \cdot 3^3 J^5_6 + 2^{-1} \cdot 3^2 \cdot 5^2 J^6_2 J^3_{10} - 2^{-1} \cdot 5^3 J^3_2 J^5_6 J^3_{10}$$

$$+ 2^{-4} J^3_2 J^5_6 - 2^{-3} J^4 J^2_2 J^3_{10} + 2^{-4} J^3_2 J^2_{10}.$$

Set

$$C(X_1, X_2, X_3, X_4) := X^4_1 - 5^3 X^3_3 + 2 \cdot 3^3 X^5_2 - 2^{-1} \cdot 3^2 \cdot 5^2 X_1 X^2_2 X^3_3$$

$$+ 2^{-1} \cdot 5^3 X^2_1 X^2_2 X^2 - 2^{-4} X^3_1 X^2_1 + 2^{-3} X^4_1 X^2_2 X^3_3$$

$$- 2^{-4} X^5_1 X^3_3 \in \mathbb{Q}[X_1, X_2, X_3, X_4].$$

If $p \neq 2$, then $C(X_1, X_2, X_3, X_4) \in \mathbb{Z}(p)[X_1, X_2, X_3, X_4]$. Denote by $\tilde{C}_p(X_1, X_2, X_3, X_4) \in \mathbb{F}[X_1, X_2, X_3, X_4]$ the reduction modulo $p$ ($p \neq 2$).

Theorem 5.3 Assume that $\mathbb{K} = \mathbb{Q}(\sqrt{5})$.

(1) If $p \geq 5$ is a prime number such that $p \equiv 3 \pmod{4}$, then

$$A_{F_0}(\Gamma_0) \cong \mathbb{F}_p[\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{15}]/(\tilde{A}_p(\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{15}) - 1, \tilde{C}_p(\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{15}))$$

(2) $$A_{F_2}(\Gamma_0) \cong \mathbb{F}_2[\tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{12}, \tilde{J}_{15}]/(\tilde{J}^2_6 + \tilde{J}^2_{10}, \tilde{J}^3_6, \tilde{J}^2_{12})$$

References


*Recibido*: 19 de septiembre de 2003

Shoyu Nagaoka
Department of Mathematics
Kinki University
Higashi-Osaka
Osaka 577-8502, Japan
nagaoka@math.kindai.ac.jp