Math. Z. 251, 821–826 (2005) **Mathematische Zeitschrift**

DOI: 10.1007/s00209-005-0832-7

Note on mod p Siegel modular forms II

Shoyu Nagaoka

Department of Mathematics, Kinki University, Higashi-Osaha, 577-8502, Osaka, Japan

Received: 17 May 2004; in final form: 10 March 2005 /
Published online: 21 July 2005 –

Dedicated to Professor Walter L. Baily, Jr.

Abstract. The structure of the ring of mod p Siegel modular forms of degree two is determined in the cases where the prime p is 2 or 3.

1. Introduction

The theory of mod p modular forms was classically developed by Swinnerton-Dyer [5] and Serre [4] and was applied to several fields in the theory of modular forms. The structure theorem in the elliptic modular case was obatined by Swinnerton-Dyer [5]. In a previous paper the author attempted to generalize this theory to the Siegel modular case [3]. The attempt was successful in the case of degree two and $p \geq 5$. The current paper completes the generalization for the degree two case. That is to say, the structure of the ring of mod p Siegel modular forms of degree two is determined in the remaining cases where p is 2 or 3.

2. Mod p Siegel modular forms of degree two

Let $\mathbb{H}_2$ denote the Siegel upper-half space of degree two and Z a point in $\mathbb{H}_2$; then $\Gamma_2 := Sp_4(\mathbb{Z})$ acts discontinously on $\mathbb{H}_2$. We shall denote by $M(\Gamma_2)$ the corresponding ring of modular forms. If F is an element of $M(\Gamma_2)$, then $F(Z)$ can be expressed as a Fourier series of the form:

$$F(Z) = \sum_{0 \leq T \in \Lambda_2} a_F(T) \exp\left[2\pi\sqrt{-1}\operatorname{tr}(TZ)\right],$$

where

$$\Lambda_2 = \{T = (t_{ij}) \in Sym_2(\mathbb{Q}) \mid t_{11}, t_{22} \in \mathbb{Z}\,, 2t_{12} \in \mathbb{Z}\}.$$

Taking $q_{ij} := \exp(2\pi\sqrt{-1}z_{ij})$ with $Z = (z_{ij}) \in \mathbb{H}_2$, we can write

$$q^T := \exp[2\pi\sqrt{-1}\mathrm{tr}(TZ)] = q_{12}^{2t_{12}} q_1^{t_1} q_2^{t_2},$$

where $q_i = q_{ii}$ and $t_i = t_{ii}$ $(i = 1, 2)$. Using this notation, we get the generalized q-expansion:

$$F = \sum_{0 \le T \in \Lambda_2} a_F(T) q^T = \sum_{t_1, t_2 \ge 0} \left(\sum a_F(T) q_{12}^{2t_{12}} \right) q_1^{t_1} q_2^{t_2} \in \mathbb{C}[q_{12}^{-1}, q_{12}][\![q_1, q_2]\!].$$

For any subring R of $\mathbb{C}$, we shall denote by $M_k(\Gamma_2)_R$ the R-module consisting of those F in $M_k(\Gamma_2)$ (the weight k homogeneous part of $M(\Gamma_2)$) for which $a_F(T)$ is in R for every $T \in \Lambda_2$. We denote by $M(\Gamma_2)_R$ the sum of $M_k(\Gamma_2)_R$ for $k = 0, 1, 2, \ldots$ in $M(\Gamma_2)$; then $M(\Gamma_2)_R$ forms a graded ring over R.

Let $\mathbb{Z}_{(p)}$ denote the local ring at p, namely, the ring of p-integral rational numbers. As stated above, any element F in $M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ may be regarded as an element of $\mathbb{Z}_{(p)}[q_{12}^{-1}, q_{12}][\![q_1, q_2]\!]$. We define a subset of $\mathbb{F}_p[q_{12}^{-1}, q_{12}][\![q_1, q_2]\!]$ by

$$\widetilde{M}_k(\Gamma_2)_p := \left\{ \widetilde{F} = \sum \widetilde{a_F(T)} q^T \in \mathbb{F}_p[q_{12}^{-1}, q_{12}][\![q_1, q_2]\!] \mid F \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}} \right\}$$

where $\widetilde{F} = \sum \widetilde{a_F(T)} q^T$ means the Fourier coefficientwise reduction mod p of $F \in M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$. Let $\widetilde{M}(\Gamma_2)_p$ denote the subring of $\mathbb{F}_p[q_{12}^{-1}, q_{12}][\![q_1, q_2]\!]$ generated by $\widetilde{M}_k(\Gamma_2)_p$ for $k = 0, 1, 2, \ldots$. We call $\widetilde{M}(\Gamma_2)_p$ *the ring of mod p Siegel modular forms of degree* 2. Let $\widetilde{M}^{(e)}(\Gamma_2)_p$, the *even* part of $\widetilde{M}(\Gamma_2)_p$, denote the subring generated by $\widetilde{M}_k(\Gamma_2)_p$ for $k = 0, 2, 4, \ldots$.

3. Structure of $\widetilde{M}(\Gamma_2)_p$ for $p \ge 5$

In [2] Igusa gives a minimal set of generators of $M(\Gamma_2)_{\mathbb{Z}}$ consisting of fifteen modular forms:

$$X_k (k = 4, 6, 10, 12, 16, 18, 24, 28, 30, 35, 36, 40, 42, 48),\ Y_{12},$$

where the subscript denotes the weight (for the precise definition, see [2], pp. 152-153). Each generator can be expressed as a polynomial in "theta constants" $\theta_{\mathfrak{m}}$([2], p. 155).

Example 1.

$$X_4 = 2^{-2} \cdot \sum_{\mathfrak{m}:\text{even}} \theta_{\mathfrak{m}}^8$$
$$= 1 + (240q_1 + 240q_2) + 2160q_1^2 + (240q_{12}^{-2} + 13440q_{12}^{-1} + 30240 + 13440q_{12} + 240q_{12}^2)q_1q_2 + 2160q_2^2 + \cdots .$$
$$X_6 = 2^{-2} \cdot \sum_{\substack{(\mathfrak{m}_1,\mathfrak{m}_2,\mathfrak{m}_3)\\ \text{syzygous triple}}} \left(\pm\theta_{\mathfrak{m}_1}^4\theta_{\mathfrak{m}_2}^4\theta_{\mathfrak{m}_3}^4\right)$$
$$= 1 - (504q_1 + 504q_2) - 16632q_1^2 + (-504q_{12}^{-2} + 44352q_{12}^{-1} + 166320 + 44352q_{12} - 504q_{12}^2)q_1q_2 - 16632q_2^2 + \cdots .$$
$$X_{10} = 2^{-12} \cdot \prod_{\mathfrak{m}:\text{even}} \theta_{\mathfrak{m}}^2 = (q_{12}^{-1} - 2 + q_{12})q_1q_{12} + \cdots .$$
$$X_{12} = 2^{-15} \cdot \sum_{(\mathfrak{m}_1,\mathfrak{m}_2,\dots,\mathfrak{m}_6)} \left(\theta_{\mathfrak{m}_1}\theta_{\mathfrak{m}_2}\cdots\theta_{\mathfrak{m}_6}\right)^4 = (q_{12}^{-1} + 10 + q_{12})q_1q_2 + \cdots ,$$

where the summation is extended over the set of fifteen complements of syzygous quadruples.

In [3] the author determined the structure of $\widetilde{M}^{(e)}(\Gamma_2)_p$ for $p \geq 5$. The main point is to show the existence of a modular form $F_{p-1}^{(2)} \in M_{p-1}(\Gamma_2)_{\mathbb{Z}_{(p)}}$ satisfying

$$F_{p-1}^{(2)} \equiv 1 \mod p$$

(cf. [3], Theorem A). In [3], the structure of the full ring $\widetilde{M}(\Gamma_2)_p$ ($p \geq 5$) was not mentioned. Considering odd weight forms, we can easily get the structure theorem. Igusa constructed the modular form X_{35} of weight 35 with integral Fourier coefficients ([2], Lemma 6). This is one of Igusa's 15 generators of $M(\Gamma_2)_{\mathbb{Z}}$ and any odd weight form F in $M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ is divisible by X_{35}, namely, $F = X_{35}F'$ with $F' \in M_{k-35}(\Gamma_2)_{\mathbb{Z}_{(p)}}$. Moreover the square X_{35}^2 has the following polynomial expression in $X_4,\ X_6,\ X_{10}$, and X_{12}:

$$\begin{aligned}
X_{35}^2 &= B(X_4, X_6, X_{10}, X_{12}),\\
B(x_1, x_2, x_3, x_4) &= 2^4 \cdot 3x_3x_4^5 + 2^{10} \cdot 5^5x_3^7 + 2^3 \cdot 3^{-2} \cdot 5^3x_2x_3^4x_4^2\\
&\quad -2^{-5} \cdot 3^{-4}x_2^2x_3x_4^4 - 2^{-7} \cdot 3^{-5} \cdot 5^2x_2^3x_3^4x_4\\
&\quad +2^{-16} \cdot 3^{-9}x_2^4x_3x_4^3 + 2^{-15} \cdot 3^{-9}x_2^5x_3^4\\
&\quad -2^3 \cdot 5^2x_1x_3^3x_4^3 - 2 \cdot 3^{-2} \cdot 5^4x_1x_2x_3^6\\
&\quad +2^{-7} \cdot 3^{-5} \cdot 5 \cdot 7x_1x_2^2x_3^3x_4^2 - 2^{-16} \cdot 3^{-8}x_1x_2^4x_3^3x_4\\
&\quad +3^{-2} \cdot 5^3 \cdot 11x_1^2x_3^5x_4 + 2^{-4} \cdot 3^{-4}x_1^2x_2x_3^2x_4^3\\
&\quad +2^{-6} \cdot 3^{-5} \cdot 5^2x_1^2x_2^2x_3^5 - 2^{-5} \cdot 3^{-4}x_1^3x_3x_4^4\\
&\quad -2^{-7} \cdot 3^{-5} \cdot 5 \cdot 19x_1^3x_2x_3^4x_4 - 2^{-15} \cdot 3^{-9}x_1^3x_2^2x_3x_4^3
\end{aligned}$$

$$
\begin{aligned}
&-2^{-14}\cdot 3^{-9}x_1^3x_2^3x_3^4+2^{-7}\cdot 3^{-5}\cdot 37x_1^4x_3^3x_4^2\\
&+2^{-15}\cdot 3^{-8}x_1^4x_2^2x_3^3x_4-2^{-6}\cdot 3^{-5}x_1^5x_3^5\\
&+2^{-16}\cdot 3^{-9}x_1^6x_3x_4^3+2^{-15}\cdot 3^{-9}x_1^6x_2x_3^4\\
&-2^{-16}\cdot 3^{-8}x_1^7x_3^3x_4.
\end{aligned}
$$

It should be noted that for $p \geq 5$, all the coefficients of B are p-integral. The structure theorem can be stated as follows:

Theorem 1. *For $p \geq 5$, we have*

$$\widetilde{M}(\Gamma_2)_p \cong \mathbb{F}_p\big[\widetilde{X}_4, \widetilde{X}_6, \widetilde{X}_{10}, \widetilde{X}_{12}, \widetilde{X}_{35}\big]/(\widetilde{A}-1, \widetilde{X}_{35}^2-\widetilde{B}),$$

where $\widetilde{A}(x_1, x_2, x_3, x_4) \in \mathbb{F}_p\,[x_1, x_2, x_3, x_4]$ is the reduction modulo p of $A(x_1, x_2, x_3, x_4) \in \mathbb{Z}_{(p)}\,[x_1, x_2, x_3, x_4]$ which is determined by the relation $F^{(2)}_{p-1} = A(X_4, X_6, X_{10}, X_{12})$. (It should be noted that $\widetilde{A} \in \mathbb{F}_p\,[x_1, x_2, x_3, x_4]$ is uniquely determined and is independent of the choice of $F^{(2)}_{p-1}$.)

4. Structure of $\widetilde{M}(\Gamma_2)_p$ for $p = 2$ or 3

In this section we shall give the structure theorem of $\widetilde{M}(\Gamma_2)_p$ in the case where $p = 2$ or 3, which is the main purpose of this paper.
We begin with the following lemma:

Lemma 1. *Assume that $p = 2$ or 3. If we take one of Igusa's generators X_k, except for X_{35}, then there exists a polynomial $F_{k,p}$ with integral coefficients satisfying*

$$X_k \equiv F_{k,p}(X_{10}, Y_{12}, X_{16}) \mod p.$$

Proof. If we use the result in Lemma 1 of [2] and an argument in the proof of Lemma 2 of [2], we get the following congruences:

For $p = 2$,

$$
\begin{aligned}
&X_4 \equiv X_6 \equiv 1 \mod 2, \quad X_{12} \equiv X_{10} \mod 2, \quad X_{18} \equiv X_{16} \mod 2,\\
&X_{24} \equiv X_{10}X_{16} \mod 2, \quad X_{28} \equiv X_{30} \equiv X_{16}^2 \mod 2,\\
&X_{36} \equiv X_{10}X_{16}^2 \mod 2, \quad X_{40} \equiv X_{42} \equiv X_{16}^3 \mod 2,\\
&X_{48} \equiv X_{16}^4 + X_{10}X_{16}^3 + X_{10}^4Y_{12} \mod 2.
\end{aligned}
$$

For $p = 3$,

$$
\begin{aligned}
&X_4 \equiv X_6 \equiv 1 \mod 3, \quad X_{12} \equiv X_{10} \mod 3, \quad X_{18} \equiv X_{16} \mod 3,\\
&X_{24} \equiv X_{10}X_{16} \mod 3, \quad X_{28} \equiv X_{30} \equiv X_{16}^2 \mod 3,\\
&X_{36} \equiv X_{16}^3 + 2X_{10}^3Y_{12} + X_{10}X_{16}^2 \mod 3, \quad X_{40} \equiv X_{16}^3 + 2X_{10}^3Y_{12} \mod 3,\\
&X_{42} \equiv X_{10}^3Y_{12} + X_{16}^3 \mod 3, \quad X_{48} \equiv X_{10}X_{16}^3 + 2X_{10}^4Y_{12} \mod 3.
\end{aligned}
$$

The above congruences mean that every generator with even weight can be expressed as a polynomial of X_{10}, Y_{12}, and X_{16} under congruence modulo p $(p = 2$ or 3). □

From this result, we get the following theorem:

Theorem 2. *For $p = 2$ or 3,*

$$\widetilde{M}^{(e)}(\Gamma_2)_p = \mathbb{F}_p\big[\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16}\big],$$

where $\widetilde{X}_{10}$, $\widetilde{Y}_{12}$, and $\widetilde{X}_{16}$ are algebraically independent over $\mathbb{F}_p$.

Proof. We assume that $p = 2$ or 3. If we take a modular form F in $M_k(\Gamma_2)_{\mathbb{Z}_{(p)}}$ for even k, then the Fourier coefficients $a_F(T)$ have bounded denominators because F has a polynomial expression in X_4, X_6, X_{10}, and X_{12} with rational coeffcients (for general case, see [1]). Then we can take a constant $c \in \mathbb{Z}$, with $(c, p) = 1$, such that $c \cdot F \in M_k(\Gamma_2)_{\mathbb{Z}}$. Hence we can express $c \cdot F$ as a polynomial of Igusa's generators X_k $(k \neq 35)$ and Y_{12}:

$$c \cdot F = P(X_4, X_6, \cdots),$$

with $P(x_1, \cdots) \in \mathbb{Z}[x_1, \cdots]$. Taking the reduction modulo p of both sides, by Lemma 1, we have

$$\tilde{c} \cdot \widetilde{F} = \widetilde{P}(\widetilde{X}_4, \widetilde{X}_6, \cdots) = \widetilde{Q}(\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16}),$$

for some $\widetilde{Q}(x_1, x_2, x_3) \in \mathbb{F}_p\,[x_1, x_2, x_3]$. Consequently, we have

$$\widetilde{F} = \tilde{c}^{-1} \cdot \widetilde{Q}(\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16}).$$

To prove the algebraic independence, we note the Fourier series expansions:

$$\begin{aligned} X_{10} &= (q_{12}^{-1} - 2 + q_{12})q_1q_2 + \cdots , \\ Y_{12} &= q_1 + q_2 + \cdots , \\ X_{16} &= q_1q_2 + \cdots . \end{aligned}$$

We assume that $\widetilde{X}_{10}$, $\widetilde{Y}_{12}$, and $\widetilde{X}_{16}$ have an algebraic relation

$$\sum \gamma_{abc}\widetilde{X}_{10}^a\widetilde{Y}_{12}^b\widetilde{X}_{16}^c = \sum(\gamma_{abc}q_{12}^{-a}q_1^{a+b+c}q_2^{a+c} + \cdots) = 0$$

$(\gamma_{abc} \in \mathbb{F}_p)$. If $(a, b, c) \neq (a', b', c')$, then

$$q_{12}^{-a}q_1^{a+b+c}q_2^{a+c} \neq q_{12}^{-a'}q_1^{a'+b'+c'}q_2^{a'+c'}.$$

This implies that all γ_{abc} vanish. This completes the proof of Theorem 2. □

By Igusa's expression for X_{35}^2, we have the following lemma:

Lemma 2. *(1)*

$$X_{35}^2 \equiv X_{10}^2 Y_{12}^2 X_{16}^2 + X_{10}^6 \mod 2.$$

(2)

$$X_{35}^2 \equiv 2X_{10}X_{16}^4 + X_{10}Y_{12}^2X_{16}^3 + 2X_{10}^2X_{16}^3 + X_{10}^2Y_{12}^2X_{16}^2 + 2X_{10}^3Y_{12}X_{16}^2 \\ +2X_{10}^4Y_{12}^3 + X_{10}^4X_{16}^2 + 2X_{10}^7 \mod 3.$$

The final result is as follows:

Theorem 3. *(1) For the case $p = 2$,*

$$\widetilde{M}(\Gamma_2)_2 \cong \mathbb{F}_2\big[\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16}, \widetilde{X}_{35}\big]/(\widetilde{X}_{35}^2 - \widetilde{P}_2(\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16})),$$

where $\widetilde{P}_2(x_1, x_2, x_3) = x_1^2x_2^2x_3^2 + x_1^6 \in \mathbb{F}_2\,[x_1, x_2, x_3]$.
(2) For the case $p = 3$,

$$\widetilde{M}(\Gamma_2)_3 \cong \mathbb{F}_3\big[\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16}, \widetilde{X}_{35}\big]/(\widetilde{X}_{35}^2 - \widetilde{P}_3(\widetilde{X}_{10}, \widetilde{Y}_{12}, \widetilde{X}_{16})),$$

where

$$\widetilde{P}_3(x_1, x_2, x_3) = 2x_1x_3^4 + x_1x_2^2x_3^3 + 2x_1^2x_3^3 + x_1^2x_2^2x_3^2 + 2x_1^3x_2x_3^2 \\ +2x_1^4x_2^3 + x_1^4x_3^2 + 2x_1^7 \in \mathbb{F}_3\,[x_1, x_2, x_3]\,.$$

Acknowledgements. The main part of this work was done during my stay at the University of Chicago in the winter of 2004. I thank the University of Chicago for its hospitality. I also thank the referee for his/her suggestions and comments.

References

1. Baily, W.L. Jr.: Automorphic forms with integral Fourier coeffcients. Lecture Notes in Math. **155**, Springer, Berlin Heidelberg, 1970, pp. 1–8
2. Igusa, J.-I.: On the ring of modular forms degree two over $\mathbb{Z}$. Am. J. Math. **101**, 149–183 (1979)
3. Nagaoka, S.: Note on mod p Siegel modular forms. Math. Z. **235**, 405–420 (2000)
4. Serre, J.-P.: Formes modulaires et fonctions zêta p-adiques, Lecture Notes in Math. **350**, Modular Functions of One Variable III. Springer, Berlin Heidelberg, 1973, pp. 191–268
5. Swinnerton-Dyer, H.P.F.: On l-adic representations and congruences for coefficients of modular forms, Lecture Notes in Math. **350**, Modular Functions of One Variable III. Springer, Berlin Heidelberg, 1973, pp. 1–55