31. Congruences between Siegel Modular Forms of Degree Two. II

By Nobushige KUROKAWA

Department of Mathematics, Tokyo Institute of Technology

(Communicated by Kunihiko Kodaira, M. J. A., Feb. 12, 1981)

Introduction. We supplement the previous note [6] by describing liftings of congruences. In particular, the congruences in Theorems 2 and 3 of [6] are considered to be congruences lifted from degree 1 to degree 2. The author would like to thank Prof. H. Maass for communicating that Prof. D. Zagier ([16]) proved completely the Conjectures 1 and 2 of [5] by using recent results of Prof. W. Kohnen after Maass [10] [11] [12] and Andrianov [2] (cf. § 1 below).

§ 1. Liftings. We denote by $M_k(\Gamma_n)$ (resp. $S_k(\Gamma_n)$) the vector space over the complex number field C consisting of all Siegel modular (resp. cusp) forms of degree n and weight k for integers $n \ge 0$ and $k \ge 0$. The space of Eisenstein series is denoted by $E_k(\Gamma_n)$ which is the orthogonal complement of $S_k(\Gamma_n)$ in $M_k(\Gamma_n)$ with respect to the Petersson inner product. We say that a modular form f in $M_k(\Gamma_n)$ is eigen if f is a non-zero eigenfunction of all Hecke operators on $M_k(\Gamma_n)$. Let f be an eigen modular form in $M_k(\Gamma_n)$ for n=1, 2. We define the (standard) Hecke polynomial at a prime p by $H_p(T, f) = 1 - \lambda(p, f)T$ $+p^{k-1}T^2$ if n=1, and $H_n(T, f)=1-\lambda(p, f)T+(\lambda(p)^2-\lambda(p^2)-p^{2k-4})T^2$ $-p^{2k-3}\lambda(p)T^3+p^{4k-6}T^4$ if n=2, where T is an indeterminate and $\lambda(m, f)$ is the eigenvalue of the Hecke operator T(m) for $f: T(m) f = \lambda(m, f) f$. We define the (standard) *L*-function by $L(s, f) = \prod_{p} H_{p}(p^{-s}, f)^{-1}$ where p runs over all prime numbers. We denote by Q(f) the field generated by $\{\lambda(m, f) | m \ge 1\}$ over the rational number field Q, and we put Z(f) $= Q(f) \cap \overline{Z}$, where Z is the rational integer ring, and \overline{Z} is the ring of all algebraic integers in C. Then Q(f) is a totally real finite extension of Q, and Z(f) is the integer ring of Q(f). See [7] which contains the case of general degree.

We consider the following two liftings from degree 1 to degree 2 for each even integer $k \ge 4$.

- (A) The first lifting is the C-linear injection $[\]:M_k(\Gamma_1)\to M_k(\Gamma_2)$ defined in [8] (cf. [6] [9]), which is given by the (generalized) Eisenstein series. For each eigen modular form f in $M_k(\Gamma_1)$ we have that: [f] is an eigen modular form satisfying $H_p(T,[f])=H_p(T,f)H_p(p^{k-2}T,f)$ for all p and L(s,[f])=L(s,f)L(s-k+2,f).
 - (B) The second lifting is the C-linear injection σ_k : $M_{2k-2}(\Gamma_1)$

 $\rightarrow M_k(\Gamma_2)$ constructed by Maass [10] [11] [12], Andrianov [2] and Zagier [16], which was conjectured in [5]. For each eigen modular form f in $M_{2k-2}(\Gamma_1)$ we have that: $\sigma_k(f)$ is an eigen modular form satisfying $H_p(T,\sigma_k(f))=(1-p^{k-2}T)(1-p^{k-1}T)H_p(T,f)$ for all p and $L(s,\sigma_k(f))=\zeta(s-k+2)\zeta(s-k+1)L(s,f)$. Here we define $\sigma_k(E_{2k-2})=\varphi_k$ for the Eisenstein series; see [5, 2.2(5)].

These liftings give the following decompositions of $M_k(\Gamma_2)$: $M_k(\Gamma_2)$ = $E_k(\Gamma_2) \oplus S_k(\Gamma_2) = M_k^{\mathrm{I}}(\Gamma_2) \oplus M_k^{\mathrm{II}}(\Gamma_2) = E_k^{\mathrm{I}}(\Gamma_2) \oplus E_k^{\mathrm{II}}(\Gamma_2) \oplus S_k^{\mathrm{II}}(\Gamma_2) \oplus S_k^{\mathrm{II}}(\Gamma_2)$. The notation is as follows. We put $E_k^{\mathrm{I}}(\Gamma_2) = [E_k(\Gamma_1)] = C \cdot \varphi_k$ and $E_k^{\mathrm{II}}(\Gamma_2) = [S_k(\Gamma_1)]$, then we have $E_k(\Gamma_2) = [M_k(\Gamma_1)] = E_k^{\mathrm{I}}(\Gamma_2) \oplus E_k^{\mathrm{II}}(\Gamma_2)$. We put

$$M_k^{\mathrm{I}}(\Gamma_2) = \left\{ f \in M_k(\Gamma_2) | a(T, f) = \sum_{d \mid e(T)} d^{k-1} a\left(\left\langle \frac{1}{d}T\right\rangle, f\right) \text{ for all } T \geq 0, T \neq 0 \right\}$$

and $S_k^{\mathrm{I}}(\Gamma_2) = M_k^{\mathrm{I}}(\Gamma_2) \cap S_k(\Gamma_2)$ with the notation of [5, § 4]. Then we have $M_k^{\mathrm{I}}(\Gamma_2) = \sigma_k(M_{2k-2}(\Gamma_1)) = E_k^{\mathrm{I}}(\Gamma_2) \oplus S_k^{\mathrm{I}}(\Gamma_2)$. Here it holds that $E_k^{\mathrm{I}}(\Gamma_2) = M_k^{\mathrm{I}}(\Gamma_2) \cap E_k(\Gamma_2) = C \cdot \varphi_k$. We denote by $S_k^{\mathrm{II}}(\Gamma_2)$ the orthogonal complement of $S_k^{\mathrm{I}}(\Gamma_2)$ in $S_k(\Gamma_2)$ with respect to the Petersson inner product ([6, Remark 3]), and we put $M_k^{\mathrm{II}}(\Gamma_2) = E_k^{\mathrm{II}}(\Gamma_2) \oplus S_k^{\mathrm{II}}(\Gamma_2)$.

We note on ℓ -adic representations. We fix a prime number ℓ . Let f be an eigen modular form in $M_k(\Gamma_1)$ for even $k \ge 4$. Let \mathfrak{l} be a prime ideal of Q(f) dividing ℓ . We denote by Q(f) the ℓ -adic completion of Q(f) and by $Z(f)_i$ the integer ring of $Q(f)_i$. Then, Deligne ([3] and [4, Th. 6.1]) constructed a continuous ℓ -adic representation $\rho_{\ell}(f)$: $\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \operatorname{GL}(2, \mathbf{Z}(f)_1)$ ($\bar{\mathbf{Q}}$ being the algebraic closure of \mathbf{Q} in \mathbf{C}) attached to f such that $\rho_{\ell}(f)$ is unramified outside of ℓ and satisfies $\det(1-\rho_i(f)(\operatorname{Frob}(p))T)=H_v(T,f)$ for all prime numbers $p\neq \ell$, where Frob(p) denotes the Frobenius conjugacy class at p. We denote by $\chi_{\ell} \colon \operatorname{Gal}(\overline{Q}/Q) \to GL(1, \mathbb{Z}_{\ell})$ the cyclotomic ℓ -adic representation, where Z_{ℓ} is the ring of ℓ -adic integers. Next, let F be an eigen modular form in $M_k(\Gamma_2)$ for (even) $k \ge 4$. Let l be a prime ideal of Q(F) dividing ℓ . We denote by $Q(F)_i$ the ℓ -adic completion of Q(F) and by $Z(F)_i$ the integer ring of $Q(F)_i$. Then, it is conjectured that there exists a continuous ℓ -adic representation $\rho_{\ell}(F)$: Gal $(\bar{Q}/Q) \rightarrow GL(4, Z(F)_{\ell})$ such that $\rho_{l}(F)$ is unramified outside of ℓ and satisfies $\det(1-\rho_{l}(F)(\operatorname{Frob}(p))T)$ $=H_n(T,F)$ for all prime numbers $p\neq \ell$. For liftings (A)(B) such an \mathcal{L} -adic representation is defined as follows. (A) If F = [f] with an eigen $f \in M_k(\Gamma_1)$, then we put $\rho_1(F) = \rho_1(f) \oplus \chi_\ell^{k-2} \otimes \rho_1(f)$. (B) If $F = \sigma_k(f)$ with an eigen $f \in M_{2k-2}(\Gamma_1)$, then we put $\rho_i(F) = \chi_{\ell}^{k-2} \oplus \chi_{\ell}^{k-1} \oplus \rho_i(f)$. Note that Z(F) = Z(f) in both cases. It might be natural to consider as $\rho_1(F)$: $Gal(\overline{Q}/Q) \rightarrow CSp(4, Z(F)_1)$ by a slight modification.

§ 2. Congruences. We recall the definition of Hecke operators following Andrianov [1, § 1.3] (cf. [7]). For integers $n \ge 1$ and $m \ge 1$ we put $S^{(n)} = \{M \in M(2n, \mathbb{Z}) | {}^tMJ_nM = \nu(M)J_n \text{ with an integer } \nu(M) \ge 1\}$

and $S_m^{(n)} = \{M \in S^{(n)} | \nu(M) = m\}$, where tM denotes the transposed matrix of M and $J_n = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}$ with the identity matrix E_n of size n. For each subring R of C we denote by $L_R^{(n)}$ (resp. $L_{R,m}^{(n)}$) the R-module generated by the double cosets $\Gamma_n M \Gamma_n$ for all $M \in S^{(n)}$ (resp. $S_m^{(n)}$). Under the usual multiplication, $L_R^{(n)}$ is an R-algebra (the abstract Hecke algebra of degree n over R). We put $H_R^{(n)} = \bigcup_{m \geq 1} L_{R,m}^{(n)}$ (the set of "homogeneous" elements of $L_R^{(n)}$), and we define a map $\nu: H_R^{(n)} \to Z$ by $\nu(X) = m$ if $X \in L_{R,m}^{(n)}, X \neq 0$, and $\nu(0) = 0$. Then ν is a homomorphism between (multiplicative) semi-groups. We denote by $\tau = \tau_k^{(n)}: L_C^{(n)} \to \operatorname{End}_C(M_k(\Gamma_n))$ the representation of the Hecke algebra $L_C^{(n)}$ on $M_k(\Gamma_n)$ defined in Andrianov [1, (1.3.3)].

Let $f \in M_k(\Gamma_n)$ and $g \in M_{k-r}(\Gamma_n)$ be eigen modular forms for an integer $n \ge 1$ and even integers $k \ge r \ge 0$. In [6], we defined the eigencharacter $\lambda(f)$ (resp. $\lambda(g)$) and a totally real finite number field Q(f) (resp. Q(g)) attached to f (resp. g). We denote by Q(f,g) = Q(f)Q(g) the composite field and by Z(f,g) the integer ring of Q(f,g). For an ideal c of Z(f,g) we write $\lambda(f) \equiv \nu^{nr/2} \lambda(g) \mod c$ if $\lambda(f)(\tau_k^{(n)}(X)) - \nu(X)^{nr/2} \cdot \lambda(g)(\tau_{k-r}^{(n)}(X))$ belongs to \bar{c} for all $X \in H_Z^{(n)}$, where $\bar{c} = \{\alpha/\beta | \alpha \in c, \beta \in Z(f,g), ((\beta),c) = Z(f,g)\}$. (The case r=0 coincides with the definition in [7, § 4].) For n=1 and 2, this condition is equivalent to the following: $\lambda(m,f) \equiv m^{nr/2} \lambda(m,g) \mod c$ for all integers $m \ge 1$. Moreover we can restrict to m=p (resp. m=p, p^2) for n=1 (resp. n=2) where p runs over all prime numbers, and this is equivalent to the following congruence between Hecke polynomials: $H_p(T,f) \equiv H_p(p^{nr/2}T,g) \mod c$ for all prime numbers p. In fact, $\sum_{\delta \ge 0} (\lambda(p^\delta,f) - p^{nr\delta/2}\lambda(p^\delta,g))T^\delta = (H_p(T,f)^{-1} - H_p(p^{nr/2}T,g)^{-1}) \times \begin{cases} 1 & \text{if } n=1, \\ (1-p^{2k-4}T^2) & \text{if } n=2. \end{cases}$

Eigenvalues of Hecke operators in [5] suggest, for example, the following congruences: $\lambda(\chi_{20}^{(3)}) \equiv \nu^2 \lambda([\varDelta_{18}]) \mod 7^2$, $\lambda(\chi_{20}^{(3)}) \equiv \nu^4 \lambda([\varDelta_{16}]) \mod 11$, $\lambda(\chi_{20}^{(3)}) \equiv \nu^3 \lambda([\varDelta_{12}]) \mod 7 \cdot 29$. These congruences supplement the following congruence proved in Theorem 1 of [6]: $\lambda(\chi_{20}^{(3)}) \equiv \lambda([\varDelta_{20}]) \mod 71^2$ which is equivalent to $H_p(T,\chi_{20}^{(3)}) \equiv H_p(T,[\varDelta_{20}]) \mod 71^2$ for all p. They seem to suggest to use a derivation $\partial = \bigoplus_{k \geq 0} \partial_k$ of $M(\Gamma_n) = \bigoplus_{k \geq 0} M_k(\Gamma_n)$ (a graded C-algebra) such that $\partial_k(M_k(\Gamma_n)) \subset M_{k+2}(\Gamma_n)$ and $\partial(M(\Gamma_n)_Z) \subset M(\Gamma_n)_Z$ where $M(\Gamma_n)_Z$ denotes the graded Z-algebra $\bigoplus_{k \geq 0} M_k(\Gamma_n)_Z$ consisting of Siegel modular forms of degree n with Fourier coefficients in Z. See Ramanujan [13], Serre [14] and Swinnerton-Dyer [15] for the case n=1. We remark that similar congruences such as $\lambda(\chi_{10}) \equiv \nu^2 \lambda(\varphi_8)$ mod 5 are proved by reducing to the elliptic modular case; see the next section (type (B)).

§ 3. Liftings of congruences. We note three types of congruences lifted from degree 1 to degree 2.

Theorem. Let $k \ge 4$ be an even integer. Then the following hold.

- (A) Let f and g be eigen modular forms in $M_{k}(\Gamma_{1})$ satisfying $\lambda(f) \equiv \lambda(g) \mod c$ with an ideal c of Z(f, g). Then we have $\lambda([f]) \equiv \lambda([g]) \mod c$.
- (B) Let $f \in M_{2k-2}(\Gamma_1)$ and $g \in M_{2k-2r-2}(\Gamma_1)$ be eigen modular forms for an even integer r in $0 \le r \le k-4$. Assume that $\lambda(f) \equiv \nu^r \lambda(g) \mod \mathfrak{c}$ for an ideal \mathfrak{c} of Z(f,g). Then we have $\lambda(\sigma_k(f)) \equiv \nu^r \lambda(\sigma_{k-r}(g)) \mod \mathfrak{c}$.
- (C) (Mixed type) Let $f \in M_k(\Gamma_1)$ and $g \in M_{2k-2}(\Gamma_1)$ be eigen modular forms. Let r=0 or 1. Assume that $\lambda(f) \equiv \nu^r \lambda(E_{k-2r}) \mod \mathfrak{c}$ and $\lambda(g) \equiv \nu^r \lambda(E_{2k-2r-2}) \mod \mathfrak{c}$ for an ideal \mathfrak{c} of Z(f,g). Then we have $\lambda([f]) \equiv \lambda(\sigma_k(g)) \mod \mathfrak{c}$.

Proof. It is sufficient to show the congruences for Hecke polynomials. Let p be a prime number and T an indeterminate.

- (A) $H_p(T, [f]) \equiv H_p(T, [g]) \mod \mathfrak{c}$ follows from $H_p(T, f) \equiv H_p(T, g)$ mod \mathfrak{c} .
- (B) $H_p(T, \sigma_k(f)) \equiv H_p(p^r T, \sigma_{k-r}(g)) \mod \mathfrak{c}$ follows from $H_p(T, f) \equiv H_p(p^r T, g) \mod \mathfrak{c}$.
- (C) We have $H_p(T,f) \equiv (1-p^rT)(1-p^{k-r-1}T) \mod \mathfrak{c}$ from $\lambda(f) \equiv \nu^r \lambda(E_{k-2r}) \mod \mathfrak{c}$. Hence $H_p(T,[f]) \equiv (1-p_rT)(1-p^{k-r-1}T)(1-p^{k+r-2}T) \pmod \mathfrak{c}$. We have $H_p(T,g) \equiv (1-p^rT)(1-p^{2k-r-3}T) \mod \mathfrak{c}$ from $\lambda(g) \equiv \nu^r \lambda(E_{2k-2r-2}) \mod \mathfrak{c}$. Hence $H_p(T,\sigma_k(g)) \equiv (1-p^rT)(1-p^{k-2}T) \pmod \mathfrak{c}$. Since r=0 or 1, we have $H_p(T,[f]) \equiv H_p(T,\sigma_k(g)) \mod \mathfrak{c}$.

Alternatively we can use the equality of the following type (here we note on (B) as an example): $\sum_{\delta\geq 0} (\lambda(p^{\delta}, \sigma_{k}(f)) - p^{r\delta}\lambda(p^{\delta}, \sigma_{k-r}(g)))T^{\delta} = (1 - p^{2k-4}T^{2})(1 - p^{k-2}T)^{-1}(1 - p^{k-1}T)^{-1}\sum_{\delta\geq 0} (\lambda(p^{\delta}, f) - p^{r\delta}\lambda(p^{\delta}, g))T^{\delta}.$ Q.E.D.

Examples. From some congruences in the elliptic modular case (see Ramanujan [13], Serre [14], and Swinnerton-Dyer [15]) we have the following congruences. We use the notation of [5] for modular forms.

- (A) We note a typical example. From the Ramanujan's congruence $\lambda(\Delta_{12}) \equiv \lambda(E_{12}) \mod 691$, we have $\lambda([\Delta_{12}]) \equiv \lambda(\varphi_{12}) \mod 691$. This is proved also as in [6].
 - (B) $\lambda(\Delta_{18}) \equiv \lambda(E_{18}) \mod 43867 \Rightarrow \lambda(\chi_{10}) \equiv \lambda(\varphi_{10}) \mod 43867.$ $\lambda(\Delta_{22}) \equiv \lambda(E_{22}) \mod 131 \cdot 593 \Rightarrow \lambda(\chi_{12}) \equiv \lambda(\varphi_{12}) \mod 131 \cdot 593.$ $\lambda(\Delta_{28}) \equiv \lambda(E_{28}) \mod 657931 \Rightarrow \lambda(\chi_{14}) \equiv \lambda(\varphi_{14}) \mod 657931.$

The above three congruences coincide with Theorem 2 of [6].

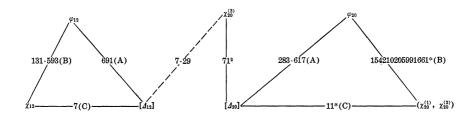
$$\lambda(\Delta_{18}) \equiv \nu^2 \lambda(E_{14}) \mod 5 \quad \Rightarrow \lambda(\chi_{10}) \equiv \nu^2 \lambda(\varphi_8) \mod 5.$$

$$\lambda(\Delta_{22}) \equiv \nu^2 \lambda(E_{18}) \mod 5 \quad \Rightarrow \lambda(\chi_{12}) \equiv \nu^2 \lambda(\varphi_{10}) \mod 5.$$

$$\lambda(\Delta_{28}) \equiv \nu^2 \lambda(E_{22}) \mod 5 \cdot 7 \Rightarrow \lambda(\chi_{14}) \equiv \nu^2 \lambda(\varphi_{12}) \mod 5 \cdot 7.$$

(C) From $\lambda(\Delta_{12}) \equiv \nu \lambda(E_{10}) \mod 7$ and $\lambda(\Delta_{22}) \equiv \nu \lambda(E_{20}) \mod 7$ we have $\lambda(\chi_{12}) \equiv \lambda([\Delta_{12}]) \mod 7$. This congruence coincides with Theorem 3 of [6]. We may consider $7 \mid L_2^*(22, \Delta_{12})$ as an interpretation for $\lambda(\Delta_{12}) \equiv \nu \lambda(E_{10}) \mod 7$.

We may list some congruences according to the decomposition $M_k(\Gamma_2) = E_k^{\text{I}}(\Gamma_2) \oplus E_k^{\text{I}}(\Gamma_2) \oplus S_k^{\text{I}}(\Gamma_2) \oplus S_k^{\text{I}}(\Gamma_2)$ for weight k = 12 and 20 as follows.



We remark that $Q(\chi_{20}^{(1)}) = Q(\chi_{20}^{(2)}) = Q(\sqrt{63737521})$, and the two congruences related to $\chi_{20}^{(1)}$ for i=1 and 2 indicate that: $N(\lambda(m,\chi_{20}^{(1)}) - \lambda(m,\varphi_{20})) \equiv 0 \mod 154210205991661$ and $N(\lambda(m,\chi_{20}^{(1)}) - \lambda(m,[\mathcal{L}_{20}])) \equiv 0 \mod 11$, for all $m \geq 1$, where $N: Q(\sqrt{63737521}) \rightarrow Q$ denotes the norm map. These congruences are proved as in [6]. On the other hand, they are also reduced to the elliptic modular case by (B) with r=0 and (C) with r=1 respectively.

We note a congruence for Fourier coefficients. From [6] we see that the Fourier coefficients $7a(T, [\Delta_{12}])$ are integers for all $T \ge 0$, and some numerical values (cf. [9, Table I]) suggest that $7a(T, [\Delta_{12}]) \equiv 0 \mod 23$ for all T > 0. We remark that $\ell = 23$ is an exceptional prime for Δ_{12} of type (ii) in the sense of Serre [14] and Swinnerton-Dyer [15] and 23 = 2k - 1 with k = 12. Similar possible examples are $\ell = 31$ (resp. 47) for k = 16 (resp. 24).

References

- [1] A. N. Andrianov: Euler products corresponding to Siegel modular forms of genus 2. Russian Math. Surveys, 29, 45-116 (1974) (English translation).
- [2] —: Modular descent and the Saito-Kurokawa conjecture. Invent. Math., 53, 267-280 (1979).
- [3] P. Deligne: Formes modulaires et représentations ℓ-adiques. Séminaire Bourbaki, exp. 355 (February 1969), Lect. Notes in Math., vol. 179, Springer-Verlag, pp. 139-186 (1971).
- [4] P. Deligne and J.-P. Serre: Formes modulaires de poids 1. Ann. sci. E.N.S. 4° ser., 7, 507-530 (1974).
- [5] N. Kurokawa: Examples of eigenvalues of Hecke operators on Siegel cusp forms of degree two. Invent. Math., 49, 149-165 (1978).
- [6] —: Congruences between Siegel modular forms of degree two. Proc.

- Japan Acad., 55A, 417-422 (1979).
- [7] N. Kurokawa: On Siegel eigenforms. Proc. Japan Acad., 57A, 47-50 (1981).
- [8] —: On Eisenstein series for Siegel modular groups. Proc. Japan Acad., 57A, 51-55 (1981); II (preprint).
- [9] N. Kurokawa and S. Mizumoto: On Eisenstein series of degree two. Proc. Japan Acad., 57A, 134-139 (1981).
- [10] H. Maass: Über eine Spezialschar von Modulformen zweiten Grades. Invent. Math., 52, 95-104 (1979).
- [11] —: Über eine Spezialschar von Modulformen zweiten Grades (II). Invent. Math., 53, 249-253 (1979).
- [12] —: Über eine Spezialschar von Modulformen zweiten Grades (III). Invent. Math., 53, 255-265 (1979).
- [18] S. Ramanujan: On certain arithmetical functions. Trans. Cambridge Philos. Soc., 22, 159-184 (1916).
- [14] J.-P. Serre: Congruences et formes modulaires. Séminaire Bourbaki, exp. 416 (June 1972), Lect. Notes in Math., vol. 317, Springer-Verlag, pp. 319– 338 (1973).
- [15] H. P. F. Swinnerton-Dyer: On ℓ-adic representations and congruences for coefficients of modular forms. Lect. Notes in Math., vol. 350, Springer-Verlag, pp. 1-55 (1973).
- [16] D. Zagier: A talk at the symposium "Modular Functions of Several Variables". Oberwolfach, 1980.