MATHEMATICS OF COMPUTATION
Volume 72, Number 242, Pages 969–973
S 0025-5718(02)01430-8
Article electronically published on March 22, 2002

A COMPUTATION OF MINIMAL POLYNOMIALS OF SPECIAL VALUES OF SIEGEL MODULAR FUNCTIONS

TSUYOSHI ITOH

Abstract. Recently, Fukuda and Komatsu constructed units of a certain abelian extension of $\mathbb{Q}(\exp(2\pi\sqrt{-1}/5))$ using special values of Siegel modular functions. In this paper, we determine the minimal polynomials of these units.

1. Introduction

We put $\zeta_n = \exp(2\pi\sqrt{-1}/n)$ for a positive integer n, and $k = \mathbb{Q}(\zeta_5)$.

We explain about Siegel modular forms. Let $\mathfrak{H}_2$ be the set of all complex symmetric matrices of degree 2 with positive definite imaginary parts. For $u \in \mathbb{C}^2, z \in \mathfrak{H}_2$ and $r, s \in \mathbb{R}^2$ we define the theta series by

$$\Theta(u, z; r, s) = \sum_{x \in \mathbb{Z}^2} e(\frac{1}{2}{}^t(x+r)z(x+r) + {}^t(x+r)(u+s)),$$

where $e(\xi)$ denotes $\exp(2\pi\sqrt{-1}\xi)$.

Moreover we consider the following function on $\mathfrak{H}_2$:

$$\Phi(z; r, s; r', s') = \frac{2\Theta(0, z; r, s)}{\Theta(0, z; r', s')}.$$

Let

$$Sp(2, \mathbb{Z}) = \{\alpha \in GL_4(\mathbb{Z}) | {}^t\alpha J \alpha = J\}$$

be the symplectic group of degree 2 and put $\Gamma_N = \{\alpha \in Sp(2, \mathbb{Z}) | \alpha \equiv I_4 \pmod N\}$ for a positive integer N, where I_n is the unit matrix of degree n and

$$J = \begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix}.$$

For any element $\alpha = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ of $Sp(2, \mathbb{Z})$ we define an action of α on $z \in \mathfrak{H}_2$ by $\alpha(z) = (Az+B)\cdot(Cz+D)^{-1}$ as usual. If N is a positive integer and $r, s, r', s' \in \frac{1}{N}\mathbb{Z}^2$, we know that $\Phi(z; r, s; r', s')$ is a Siegel modular function with respect to Γ_{2N^2} ([S], Prop. 1.7).

Let σ be the element of the Galois group $\mathrm{Gal}(k/\mathbb{Q})$ defined by $\zeta_5^\sigma = \zeta_5^2$. We let O_k be the ring of integers in k and put $L = \{\left(\begin{smallmatrix} \xi \\ \xi^\sigma \end{smallmatrix}\right) | \xi \in O_k\}$. We define a Riemann form E on $\mathbb{C}^2/L$ for $u_i, v_i \in \mathbb{C}$ as follows:

$$E\left(\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}\right) = \rho(u_1\bar{v_1} - \bar{u_1}v_1) + \rho^\sigma(u_2\bar{v_2} - \bar{u_2}v_2),$$

Received by the editor March 15, 2000 and, in revised form, April 10, 2001.
2000 *Mathematics Subject Classification.* Primary 11G15, 11R27, 11Y40.

where $\rho = (\zeta_5 - \zeta_5^4)/5$. Moreover, for

$$\omega_1 = \begin{pmatrix} -\zeta_5 \\ -\zeta_5^2 \end{pmatrix}, \quad \omega_2 = \begin{pmatrix} \zeta_5^4 \\ \zeta_5^3 \end{pmatrix}, \quad \omega_3 = \begin{pmatrix} \zeta_5^2 + \zeta_5^4 \\ \zeta_5^4 + \zeta_5^3 \end{pmatrix}, \quad \omega_4 = \begin{pmatrix} \zeta_5^3 \\ \zeta_5 \end{pmatrix},$$

we can see that $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ is a free basis of L over $\mathbb{Z}$ and $(E(\omega_i, \omega_j))_{i,j=\{1,2,3,4\}} = J$. Hence we see that

$$z_0 = \begin{pmatrix} \zeta_5^2 + \zeta_5^4 & \zeta_5^3 \\ \zeta_5^4 + \zeta_5^3 & \zeta_5 \end{pmatrix}^{-1} \begin{pmatrix} -\zeta_5 & \zeta_5^4 \\ -\zeta_5^2 & \zeta_5^3 \end{pmatrix}$$

is a CM-point of $\mathfrak{H}_2$ corresponding to the polarized abelian variety $(\mathbb{C}^2/L, E)$. By [S], Prop. 2.2, if N is a positive integer and $r, s, r', s' \in \frac{1}{N}\mathbb{Z}^2$, $\Phi(z_0; r, s; r', s')$ is contained in some abelian extension k' of k.

Let ω be an integer of k which is prime to N. We denote by $R(\omega) \in M_4(\mathbb{Z})$ the regular representation of ω with respect to an O_k-basis $\{-\zeta_5, \zeta_5^4, \zeta_5^2 + \zeta_5^3, \zeta_5^3\}$. We put $v = N_{k/\mathbb{Q}}\omega$. Then there exists a matrix β in $Sp(2, \mathbb{Z})$ satisfying

$$R(\varphi(\omega)) \equiv \begin{pmatrix} I_2 & 0 \\ 0 & vI_2 \end{pmatrix} \beta \pmod{2N^2},$$

where φ is an endomorphism of $k^\times$ defined by $\varphi(a) = a^{1+\sigma^3}$. If r, s are in $\frac{1}{N}\mathbb{Z}^2$, we define

$$\Phi^{R(\varphi(\omega))}(z; r, s; r', s') = \Phi(\beta(z); r, vs; r', vs').$$

Then by Shimura's reciprocity law ([S]), we have

$$\Phi(z_0; r, s; r', s')^{\left(\frac{k'/k}{(\omega)}\right)} = \Phi^{R(\varphi(\omega))}(z_0; r, s; r', s').$$

We put $\zeta = \zeta_5$. Fukuda and Komatsu showed the following theorem.

Theorem ([FK])**.** *We put*

$$\varepsilon_1 = \frac{\Phi\left(z_0; \binom{\frac{1}{3}}{0}, \binom{0}{0}; \binom{0}{0}, \binom{0}{0}\right)}{\Phi^{R(\varphi(2+\zeta)^2)}\left(z_0; \binom{\frac{1}{3}}{0}, \binom{0}{0}; \binom{0}{0}, \binom{0}{0}\right)}$$

and

$$\varepsilon_2 = \frac{\Phi\left(z_0; \binom{\frac{1}{3}}{\frac{2}{3}}, \binom{\frac{1}{3}}{0}; \binom{0}{0}, \binom{0}{0}\right)}{\Phi^{R(\varphi(2+\zeta)^2)}\left(z_0; \binom{\frac{1}{3}}{\frac{2}{3}}, \binom{\frac{1}{3}}{0}; \binom{0}{0}, \binom{0}{0}\right)}.$$

Then ε_1 and ε_2 are units in k_6.

We will construct the minimal polynomials of ε_1 and ε_2 by numerically computing the conjugates of ε_i over $\mathbb{Q}$ with high precision.

These polynomials allow us to compute the approximate values of these units with arbitarily high precision. Our method will be useful to compute the rank of the unit group generated by special values of Siegel modular functions, and so on.

2. Computation of conjugates

For a positive integer N, k_N denotes the maximal ray class field of k modulo (N). We consider the structure of the Galois group $\mathrm{Gal}(k_6/k)$. Let M be the subgroup of $k^\times$ generated by integers of k which are prime to 6. We also let $\tilde{M}$ be the set of all principal ideals of k which have a generator in M. Similarly, we put $S_6 = \{a \in k^\times | a \equiv 1 \pmod{6}\}$ and $\tilde{S}_6 = \{(a) | a \in S_6\}$. Then by class field theory

$$\mathrm{Gal}(k_6/k) \cong \tilde{M}/\tilde{S}_6 \cong (M/U_k)/(S_6U_k/U_k) \cong M/S_6U_k \cong \mathbb{Z}/10\mathbb{Z},$$

where U_k is the full unit group of k. So by [FK], we know that

$$\tau = \left(\frac{k_6/k}{(\zeta_5+2)}\right)$$

generates the Galois group of k_6 over k. We extend σ to k_6.

By Shimura's theory, we know that $\Phi(z_0; r, s; r', s')$ is contained in k_{18} if $r, s, r', s' \in \frac{1}{3}\mathbb{Z}^2$ ([S], see also [K]). Since we will treat the case $r, s, r', s' \in \frac{1}{6}\mathbb{Z}^2$ later, we choose $\beta \in Sp(2, \mathbb{Z})$ which satisfies

$$R(\varphi(\omega)) \equiv \begin{pmatrix} I_2 & 0 \\ 0 & vI_2 \end{pmatrix} \beta \pmod{72}.$$

In the case $\omega = \zeta_5 + 2$, we choose

$$\beta = \begin{pmatrix} 3 & 0 & -1 & 1 \\ 2 & 2 & 0 & -1 \\ -111 & 26 & 46 & -59 \\ 26 & -13 & -13 & 20 \end{pmatrix} \in Sp(2, \mathbb{Z}).$$

Then we can compute $\Phi(z_0; r, s; 0, 0)^{\tau^n}$ by using β. But the theta series $\Theta(0, \beta^n(z_0); r, s)$ converges slowly if n is large, because the imaginary part of $\beta^n(z_0)$ tends to 0 quickly. So we determine $\Phi(z_0; r, s; 0, 0)^{\tau^n}$ using the fact that $\zeta_{360}^{\tau} = \zeta_{360}^{11}$ and the following lemma recursively.

Lemma (cf. [S], Prop. 1.3)**.** *If r, s are in $\frac{1}{6}\mathbb{Z}^2$ and $r', s' \in \frac{1}{2}\mathbb{Z}^2$, then there exist $r_1, s_1 \in \frac{1}{6}\mathbb{Z}^2$, $r_2, s_2 \in \frac{1}{2}\mathbb{Z}^2$ and an integer t such that*

$$\Phi(\beta(z_0); r, s; r', s') = \zeta_{360}^t \Phi(z_0; r_1, s_1; r_2, s_2)$$

Next, we shall determine $\Phi(z_0; r, s; 0, 0)^\sigma$. We know that $\Phi(z_0; r, s; 0, 0)^3$ is an algebraic integer in k_6 (cf. [FK]), and hence

$$N_{k_6/\mathbb{Q}(\sqrt{5})}\Phi(z_0; r, s; 0, 0)^3 = \prod_{n=0}^{9} |\Phi^{R(\varphi(2+\zeta)^n)}(z_0; r, s; 0, 0)^3|^2.$$

Furthermore we know that $(\Phi(z_0; r, s; 0, 0)^3)^\sigma$ is given by $\xi\Phi(z_0; r_1, s_1; r_2, s_2)^3$ for some $r_1, s_1 \in \frac{1}{6}\mathbb{Z}$, $r_2, s_2 \in \frac{1}{2}\mathbb{Z}$ and some 6-th root of unity ξ. So we computed

$$N_{k_6/\mathbb{Q}(\sqrt{5})}\Phi(z_0; r, s; 0, 0)^3 \times N_{k_6/\mathbb{Q}(\sqrt{5})}\Phi(z_0; r_1, s_1; r_2, s_2)^3 \tag{1}$$

for all r_1, s_1, r_2, s_2. Fortunately there is only one integral value for (1). Hence we can determine $\Phi(z_0; r, s; 0, 0)^\sigma$ up to conjugation by τ^n and multiplication by an 18-th root of unity.

Next, we shall determine $\Phi(z_0; r, s; 0, 0)^{\sigma^2}$. We know that σ^2 acts as complex conjugation on k. So we computed

$$Tr_{k_6/k}\Phi(z_0; r, s; 0, 0)^3 + Tr_{k_6/k}\xi\Phi(z_0; r_1, s_1; r_2, s_2)^3$$

for all r_1, s_1, r_2, s_2 and a 6-th root of unity ξ, and we found only one value which is in $\mathbb{R}$. We can determine $\Phi(z_0; r, s; 0, 0)^{\sigma^3}$ in a similar way. We note that $\Phi(z_0; r, s; 0, 0)^{\sigma^2}$ and $\Phi(z_0; r, s; 0, 0)^{\sigma^3}$ are also determined up to conjugation by τ^n and multiplication by an 18-th root of unity.

By the above argument, we can determine all $\Phi(z_0; r, s; 0, 0)^{\sigma^i\tau^j}$ and hence $\varepsilon_1^{\sigma^i\tau^j}$ $(0 \le i \le 3, 0 \le j \le 9)$ up to multiplication by an 18-th root of unity. We note that $\varepsilon_1 \in k_6$, and $\mathrm{Gal}(k_6/\mathbb{Q}) = \{\sigma^i\tau^j | 0 \le i \le 3, 0 \le j \le 9\}$ as a set. We were able to determine the 18-th root of unity $\xi^{(i)}$ for each σ^i so that the all fundamental symmetric forms of $\{(\xi^{(i)}\varepsilon_1^{\sigma^i})^{\tau^j}\}$ are close to rational integers. Consequently the set $\{\varepsilon_1^{\rho} | \rho \in \mathrm{Gal}(k_6/\mathbb{Q})\}$ was determined. The same method is applicable to ε_2.

3. Minimal polynomials

Now it is easy to compute the minimal polynomials of ε_i using approximate values of the conjugates of ε_i. We know that the coefficients of these polynomials are in $\mathbb{Z}$. So we computed these fundamental symmetric forms with a precision of 300 digits by using TC on Sparc Station 5. These values are close to integers, which is enough to recognize the coefficients of minimal polynomials.

(1) The case of $\varepsilon_1 = \frac{\Phi(z_0; \binom{1/3}{0}, \binom{0}{0}; \binom{0}{0}, \binom{0}{0})}{\Phi^{R(\varphi(\zeta+2)^2)}(z_0; \binom{1/3}{0}, \binom{0}{0}; \binom{0}{0}, \binom{0}{0})}$.

ε^{σ} up to conjugation by τ^i	$\zeta_3^2 \frac{\Phi(z_0; \binom{1/6}{1/6}, \binom{0}{0}; \binom{1/2}{1/2}, \binom{1/2}{1/2})}{\Phi^{R(\varphi(\zeta+2)^4)}(z_0; \binom{1/6}{1/6}, \binom{0}{0}; \binom{1/2}{1/2}, \binom{1/2}{1/2})}$
ε^{σ^2} up to conjugation by τ^i	$\frac{\Phi^{R(\varphi(\zeta+2)^9)}(z_0; \binom{1/3}{0}, \binom{0}{0}; \binom{0}{0}, \binom{0}{0})}{\Phi^{R(\varphi(\zeta+2)^7)}(z_0; \binom{1/3}{0}, \binom{0}{0}; \binom{0}{0}, \binom{0}{0})}$
ε^{σ^3} up to conjugation by τ^i	$\zeta_3^2 \frac{\Phi^{R(\varphi(\zeta+2)^5)}(z_0; \binom{1/6}{1/6}, \binom{0}{0}; \binom{1/2}{1/2}, \binom{1/2}{1/2})}{\Phi^{R(\varphi(\zeta+2))}(z_0; \binom{1/6}{1/6}, \binom{0}{0}; \binom{1/2}{1/2}, \binom{1/2}{1/2})}$

minimal polynomial
$1 - 13x + 66x^2 + 173x^3 + 748x^4 + 1914x^5 + 7122x^6 + 14100x^7$
$+35202x^8 + 71843x^9 + 144694x^{10} + 258459x^{11} + 452770x^{12}$
$+727529x^{13} + 1110726x^{14} + 1578249x^{15} + 2120130x^{16}$
$+2655756x^{17} + 3143526x^{18} + 3468090x^{19} + 3594591x^{20}$
$+3468090x^{21} + 3143526x^{22} + 2655756x^{23} + 2120130x^{24}$
$+1578249x^{25} + 1110726x^{26} + 727529x^{27} + 452770x^{28}$
$+258459x^{29} + 144694x^{30} + 71843x^{31} + 35202x^{32} + 14100x^{33}$
$+7122x^{34} + 1914x^{35} + 748x^{36} + 173x^{37} + 66x^{38} - 13x^{39} + x^{40}$

(2) The case of $\varepsilon_2 = \frac{\Phi(z_0;\binom{1/3}{2/3},\binom{1/3}{0};\binom{0}{0},\binom{0}{0})}{\Phi^{R(\varphi(\zeta+2)^2)}(z_0;\binom{1/3}{2/3},\binom{1/3}{0};\binom{0}{0},\binom{0}{0})}$**.**

ε^{σ} up to conjugation by τ^i	$\zeta_3 \frac{\Phi(z_0;\binom{5/6}{1/6},\binom{0}{0};\binom{1/2}{1/2},\binom{1/2}{1/2})}{\Phi^{R(\varphi(\zeta+2)^4)}(z_0;\binom{5/6}{1/6},\binom{0}{0};\binom{1/2}{1/2},\binom{1/2}{1/2})}$
ε^{σ^2} up to conjugation by τ^i	$\frac{\Phi^{R(\varphi(\zeta+2)^9)}(z_0;\binom{1/3}{2/3},\binom{1/3}{0};\binom{0}{0},\binom{0}{0})}{\Phi^{R(\varphi(\zeta+2)^7)}(z_0;\binom{1/3}{2/3},\binom{1/3}{0};\binom{0}{0},\binom{0}{0})}$
ε^{σ^3} up to conjugation by τ^i	$\zeta_3 \frac{\Phi^{R(\varphi(\zeta+2)^5)}(z_0;\binom{5/6}{1/6},\binom{0}{0};\binom{1/2}{1/2},\binom{1/2}{1/2})}{\Phi^{R(\varphi(\zeta+2))}(z_0;\binom{5/6}{1/6},\binom{0}{0};\binom{1/2}{1/2},\binom{1/2}{1/2})}$

minimal polynomial
$1+5x+12x^2+29x^3+130x^4+606x^5+2094x^6+5880x^7$ $+16206x^8+45569x^9+116218x^{10}+251421x^{11}+481804x^{12}$ $+915197x^{13}+1839114x^{14}+3687489x^{15}+6748272x^{16}$ $+10784772x^{17}+14938512x^{18}+18059322x^{19}+19215855x^{20}$ $+18059322x^{21}+14938512x^{22}+10784772x^{23}+6748272x^{24}$ $+3687489x^{25}+1839114x^{26}+915197x^{27}+481804x^{28}$ $+251421x^{29}+116218x^{30}+45569x^{31}+16206x^{32}+5880x^{33}$ $+2094x^{34}+606x^{35}+130x^{36}+29x^{37}+12x^{38}+5x^{39}+x^{40}$

Acknowledgments

The author would like to thank Professor K. Komatsu for giving useful advice, and Professor T. Fukuda for instruction about computational techniques for theta series.

The computations are mainly due to TC, which is an interpreter of multi-precision C language developed by T. Fukuda, which is available from
`ftp://tnt.math.metro-u.ac.jp/pub/math-packs/tc/`.

References

[FK] T. Fukuda and K. Komatsu: *On a unit group generated by special values of Siegel modular functions*, Math. Comp. 69 (2000), 1207–1212. MR **2000j:**11089

[K] K. Komatsu: *Construction of normal basis by special values of Siegel modular functions*, Proc. Amer. Math. Soc., **128** (2000), 315–323. MR **2000d:**11139

[S] G. Shimura: *Theta functions with complex multiplication*,Duke Math. J. **43** (1976), 673–696. MR **54:**12664

Department of Mathematical Sciences, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, Japan

E-mail address: `tsitoh@mn.waseda.ac.jp`