LMS J. Comput. Math. 17 (Special issue A) (2014) 295–302 © 2014 Authors
doi:10.1112/S146115701400014X

Class number calculation using Siegel functions

T. Fukuda and K. Komatsu

Abstract

We propose a fast method of calculating the p-part of the class numbers in certain non-cyclotomic $\mathbb{Z}_p$-extensions of an imaginary quadratic field using elliptic units constructed by Siegel functions. We carried out practical calculations for $p = 3$ and determined λ-invariants of such $\mathbb{Z}_3$-extensions which were not known in our previous paper.

1. *Introduction*

Let K be an imaginary quadratic field and p an odd prime number which splits into two distinct primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ in K. We denote by $K'_n = K(\mathfrak{p}^{n+1})$ the ray class field of K modulo $\mathfrak{p}^{n+1}$ and $K'_\infty = \bigcup_{n=0}^{\infty} K'_n$. Then there exists a unique $\mathbb{Z}_p$-extension K_∞ of K in K'_∞. We denote by K_n the nth layer of K_∞ over K.

In a previous paper [3] we studied the Iwasawa invariant $\lambda(K_\infty/K)$ for $p = 3$, while $\mu(K_\infty/K)$ is known to be zero by [4, 7]. Our investigation was based on the calculation in K_2. We were not able to handle K_n $(n \geqslant 3)$ for lack of a fine algorithm. In the present paper we develop a new algorithm based on the structure of the group of elliptic units and calculate the 3-part of the class number $h(K_n)$ of K_n $(1 \leqslant n \leqslant 5)$. We are now able to consider $\lambda(K_\infty/K)$ by observing directly the growth of the 3-part of $h(K_n)$.

We illustrate, for an odd prime number p, how to calculate the p-part of $h(K_n)$. As usual, for a Galois extension L/F of algebraic number fields, we denote by $G(L/F)$ the Galois group of L over F and by $N_{L/F}$ the norm mapping of L over F. We begin by explaining how to construct K_n explicitly. We assume that K is different from both $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. As in [3], we are interested in K_∞/K in which $\mathfrak{p}$ is totally ramified. Therefore $\widetilde{K} \cap K_\infty = K$, where $\widetilde{K}$ means the Hilbert class field of K. Let a_1, a_2 be rational numbers and τ a complex number with positive imaginary part. Then the Siegel function is defined to be

$$g(a_1, a_2)(\tau) = -q_\tau^{(1/2)(a_1^2 - a_1 + 1/6)} e^{2\pi i a_2(a_1 - 1)/2}(1 - q_z) \prod_{n=1}^{\infty} (1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1}),$$

where $q_\tau = e^{2\pi i \tau}$, $q_z = e^{2\pi i z}$, $z = a_1\tau + a_2$ and $i = \sqrt{-1}$. Then $g(a_1, a_2)(\tau)$ is a modular function of some level and K_n is generated by special values of $g(a_1, a_2)$. We refer [5, Chapter 2] for the various properties of the Siegel function.

Let ω_1 and ω_2 be elements of K with imaginary part $\mathrm{Im}(\omega_1/\omega_2) > 0$ such that $\mathfrak{p}^{n+1} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Since $(p) = \mathfrak{p}\mathfrak{p}'$, there exist integers $r, s \in \mathbb{Z}$ with

$$\frac{r}{p^{n+1}}\omega_1 + \frac{s}{p^{n+1}}\omega_2 = 1.$$

Then $g(r/p^{n+1}, s/p^{n+1})(\omega_1/\omega_2)^{12p^{n+1}}$ is in K'_n by [5, p. 234, Theorem 1.1]. We put

$$f(\tau) = \left(g\left(\frac{r}{p^{n+1}}, \frac{s}{p^{n+1}}\right)(\tau) \Big/ g\left(\frac{r(1+p)}{p^{n+1}}, \frac{s(1+p)}{p^{n+1}}\right)(\tau) \right)^4.$$

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11R29, 11R23 (primary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

We know that $f(\tau)$ is independent of r, s by [**5**, p. 33, Proposition 1.3]. Then there exists a unique $3p^{n+1}$th root of unity ζ such that $f(\omega_1/\omega_2)\zeta \in K'_n$ by [**3**, p. 472]. We put

$$\eta_n = N_{K'_n/K_n}\left(f\left(\frac{\omega_1}{\omega_2}\right)\zeta\right).$$

Let Γ be the Galois group $G(K_\infty/K)$ and γ is topological generator of Γ. We put

$$\mathcal{E}_n = \langle \eta_n, \eta_n^{\gamma}, \ldots, \eta_n^{\gamma^{p^n-2}} \rangle.$$

Let E_n be the unit group of K_n. Then it is well known that the group index $(E_n : \mathcal{E}_n)$ is finite [**5**, p. 323, Theorem 4.1]. We note that $\eta_n, \eta_n^{\gamma}, \ldots, \eta_n^{\gamma^{p^n-2}}$ form a free basis of $\mathcal{E}_n$. Let E'_n be the subgroup of E_n such that $E'_n/\mathcal{E}_n$ is the p-Sylow subgroup of $E_n/\mathcal{E}_n$. Let p^{e_n} be the exact power of p dividing the class number $h(K_n)$ of K_n. Then we have

$$p^{e_n} = p^{e_0}(E'_n : \mathcal{E}_n) \tag{1.1}$$

by [**5**, p. 323, Theorem 4.1]. Our main purpose of this paper is to prove the following theorem.

THEOREM 1.1. *Let the notation and assumptions be as above. If* $e_n - e_{n-1} = 1$ *for some integer* $n \geqslant 1$*, then we have* $e_{n+1} - e_n \leqslant 1$*.*

Owing to [**2**, Theorem 1], we may convert Theorem 1.1 into the following version.

COROLLARY 1.2. *If* $e_n - e_{n-1} \leqslant 1$ *for some integer* $n \geqslant 1$*, then we have* $e_m - e_{m-1} \leqslant 1$ *for all integers* $m \geqslant n$*.*

As an application of Corollary 1.2, we show an efficient algorithm for calculating e_n in the case $e_1 - e_0 = 1$ in § 3.

2. *Proof of theorem*

Preparatory to proving Theorem 1.1, we summarize as lemmas properties of E_n, E'_n and $\mathcal{E}_n$ which were defined in the previous section.

LEMMA 2.1. *We have* $\mathcal{E}_n \cap E_{n-1} = \mathcal{E}_{n-1}$ *for* $n \geqslant 1$*.*

Proof. We write $s = p^{n-1} - 1$ and $r = p^n - p^{n-1} - 1$. Put

$$\eta = \eta_n^{x_0 + x_1\gamma + \ldots + x_{p^n-2}\gamma^{p^n-2}}$$

with rational integers x_i. We assume $\eta \in E_{n-1}$. Then $\eta^{\gamma^{p^{n-1}}} = \eta$, which implies

$$\eta^{\gamma^{p^{n-1}}} = \eta_n^{\sum_{i=0}^{p^n-2}(x_i - x_r)\gamma^{i+p^{n-1}}} = \eta$$

by $N_{K_n/K}(\eta_n) = 1$. Hence we have

$$\begin{aligned} x_i - x_r &= x_{i+p^{n-1}} \quad (0 \leqslant i \leqslant r-1),\\ x_i - x_r &= x_{i+p^{n-1}-p^n} \quad (r+1 \leqslant i \leqslant p^n - 2),\\ -x_r &= x_{p^{n-1}-1}, \end{aligned}$$

which means $x_0 - px_r = x_0$. This shows $x_r = 0$ and $x_{p^{n-1}-1} = 0$. It is known that $N_{K_n/K_{n-1}}(\eta_n) = \eta_{n-1}$ by [**5**, Theorem 1.3, p. 237]. Hence, noting the uniqueness of ζ, we have

$$\eta = N_{K_n/K_{n-1}}(\eta_n^{x_0 + x_1\gamma + \ldots + x_{s-1}\gamma^{s-1}}) = \eta_{n-1}^{x_0 + x_1\gamma + \ldots + x_{s-1}\gamma^{s-1}}. \qquad \square$$

LEMMA 2.2. *We have* $p^{e_n - e_{n-1}} = (E'_n : \mathcal{E}_n E'_{n-1})$ *for* $n \geqslant 1$.

Proof. Since $\mathcal{E}_n \cap E'_{n-1} = \mathcal{E}_{n-1}$ by Lemma 2.1, we have $(\mathcal{E}_n E'_{n-1} : \mathcal{E}_n) = (E'_{n-1} : \mathcal{E}_{n-1})$. Hence we have

$$\begin{aligned} p^{e_n} = (E'_n : \mathcal{E}_n) &= (E'_n : \mathcal{E}_n E'_{n-1})(\mathcal{E}_n E'_{n-1} : \mathcal{E}_n) \\ &= (E'_n : \mathcal{E}_n E'_{n-1})(E'_{n-1} : \mathcal{E}_{n-1}) \\ &= p^{e_{n-1}}(E'_n : \mathcal{E}_n E'_{n-1}). \end{aligned}$$

□

LEMMA 2.3. *If* $E'_n/\mathcal{E}_n$ *is non-trivial, then there exists an element* η *in* $\mathcal{E}_n$ *with* $\eta \notin \mathcal{E}_n^p$ *and* $\eta^{\gamma-1} \in \mathcal{E}_n^p$, *where* $\mathcal{E}_n^p = \{\varepsilon^p \mid \varepsilon \in \mathcal{E}_n\}$.

Proof. Since $E'_n/\mathcal{E}_n$ is a non-trivial p-group, there exists an element u in E'_n such that $u \notin \mathcal{E}_n$, $u^{\gamma-1} \in \mathcal{E}_n$ and $u^p \in \mathcal{E}_n$. We put $\eta = u^p$. Then $\eta \notin \mathcal{E}_n^p$ and $\eta^{\gamma-1} = (u^{\gamma-1})^p \in \mathcal{E}_n^p$ because E_n does not contain a non-trivial pth root of unity. □

Let H be a subgroup of E_n and u, v elements of E_n. From now on, we write $u \equiv v \pmod{H}$ if $uv^{-1} \in H$. We put $T = \gamma - 1$ as usual.

LEMMA 2.4. *There exists an element* $f_n(T)$ *in* $\mathbb{Z}[T]$ *which satisfies*

$$\eta_n^{T^{p^n - p^{n-1}}} = \eta_{n-1}\eta_n^{-p(1+Tf_n(T))}.$$

Proof. Since $\sum_{i=0}^{p-1}(T+1)^{ip^{n-1}} \equiv \sum_{i=0}^{n-1}(T^{p^{n-1}}+1)^i \equiv T^{p^n - p^{n-1}} \pmod{p}$, we see that $\sum_{i=0}^{n-1}(T+1)^{ip^{n-1}} - T^{p^n-p^{n-1}} \in p\mathbb{Z}[T]$. Hence

$$f_n(T) = \frac{\sum_{i=0}^{p-1}(T+1)^{ip^{n-1}} - T^{p^n-p^{n-1}} - p}{pT}$$

is contained in $\mathbb{Z}[T]$ and

$$\eta_{n-1} = N_{K_n/K_{n-1}}(\eta_n) = \eta_n^{\sum_{i=0}^{p-1}(T+1)^{ip^{n-1}}} = \eta_n^{T^{p^n-p^{n-1}}+p+pTf_n(T)},$$

from which we derive the desired equality. □

Proof of Theorem 1. We assume $e_n - e_{n-1} = 1$ and $e_{n+1} - e_n \geqslant 2$ and derive a contradiction. We write $r = p^n - p^{n-1} - 1$. Let $\{\xi_1, \xi_2, \ldots, \xi_{p^{n-1}-1}\}$ be a free basis of E'_{n-1} and put

$$V_n = \langle \xi_1, \xi_2, \ldots, \xi_{p^{n-1}-1}, \eta_n, \eta_n^{\gamma}, \ldots, \eta_n^{\gamma^r} \rangle.$$

Since $\{\eta_n, \eta_n^{\gamma}, \ldots, \eta_n^{\gamma^{p^n-2}}\}$ is a free basis of $\mathcal{E}_n$ and since $N_{K_n/K_{n-1}}(\eta_n) = \eta_{n-1}$, we have $V_n = E'_{n-1}\mathcal{E}_n$. We note

$$V_n = \langle \xi_1, \xi_2, \ldots, \xi_{p^{n-1}-1}, \eta_n, \eta_n^{T}, \ldots, \eta_n^{T^r} \rangle.$$

Since $e_n - e_{n-1} = 1$, there exist $v_n \in V_n$, $\varepsilon \in E'_n - V_n$ and $x_i, y_i \in \{0, 1, \ldots, p-1\}$ such that

$$\varepsilon^p = v_n = \xi_1^{x_1}\xi_2^{x_2}\ldots\xi_{p^{n-1}-1}^{x_{p^{n-1}-1}}\eta_n^{y_0+y_1T+\ldots+y_rT^r}$$

and $v_n^T \equiv 1 \pmod{V_n^p}$ by Lemma 2.3. Since $\eta_n^{T^r} \equiv \eta_{n-1} \pmod{V_n^p}$ by Lemma 2.4,

https://doi.org/10.1112/S146115701400014X Published online by Cambridge University Press

we have

$$\begin{aligned} v_n^T &\equiv \xi_1^{x_1 T} \dots \xi_{p^{n-1}-1}^{x_{p^{n-1}-1}T} \eta_{n-1}^{y_r} \eta_n^{-y_r p(1+Tf_n(T))} \eta_n^{y_0 T + y_1 T^2 + \dots + y_{r-1}T^r} \\ &\equiv \xi_1^{x_1 T} \dots \xi_{p^{n-1}-1}^{x_{p^{n-1}-1}T} \eta_{n-1}^{y_r} \eta_n^{y_0 T + y_1 T^2 + \dots + y_{r-1}T^r} \pmod{V_n^p}. \end{aligned}$$

Hence we have $y_0 = y_1 = \dots = y_{r-1} = 0$ and $y_r \neq 0$ by $e_n - e_{n-1} = 1$. We may assume $y_r = 1$. Hence there exists an element $\xi \in E'_{n-1}$ with

$$v_n = \xi \eta_n^{(\gamma-1)^r}$$

such that $v_n^{1/p} \in E'_n$. This means $E'_n = \langle V_n \cup \{v_n^{1/p}\} \rangle$ by $e_n - e_{n-1} = 1$. Since $(v_n^{1/p})^T = (\xi^T \eta_{n-1} \eta_n^{-p(1+Tf_n(T))})^{1/p}$, there exists an element $\xi' \in E'_{n-1}$ with

$$(v_n^{1/p})^T = \xi' \eta_n^{-(1+Tf_n(T))}. \tag{2.1}$$

We put

$$V_{n+1} = \langle E'_n \cup \{\eta_{n+1}, \eta_{n+1}^T, \dots, \eta_{n+1}^{T^{r'}}\} \rangle,$$

where $r' = p^{n+1} - p^n - 1$. Then there exist $v_{n+1} \in V_{n+1}$, $\xi^* \in E'_{n-1}$, $a_i, b_i \in \{0, 1, \dots, p-1\}$ and $\varepsilon^* \in E'_{n+1} - V_{n+1}$ such that

$$\varepsilon^{*p} = v_{n+1} = \xi^* \eta_n^{a_0 + a_1 T + \dots + a_{r-1}T^{r-1}} (v_n^{1/p})^{a_r} \eta_{n+1}^{b_0 + b_1 T + \dots + b_{r'} T^{r'}}$$

and $v_{n+1}^T \equiv 1 \pmod{V_{n+1}^p}$ by Lemma 2.3 and the assumption $e_{n+1} - e_n \geqslant 2$. Since $\eta_{n+1}^{T^{r'+1}} \equiv \eta_n \pmod{V_{n+1}^p}$ by Lemma 2.4, we have

$$\begin{aligned} v_{n+1}^T &\equiv (\xi^*)^T \eta_n^{a_o T + \dots + a_{r-2}T^{r-2}} (v_n \xi^{-1})^{a_{r-1}} \\ &\quad \cdot (\xi^* \eta_n^{-(1+Tf_n(T))})^{a_r} \eta_{n+1}^{b_0 T + \dots + b_{r'-1}T^{r'-1}} \eta_n^{b_{r'}} \\ &\equiv 1 \pmod{V_{n+1}^p}. \end{aligned}$$

This shows $b_0 = b_1 = \dots = b_{r-1} = 0$ and $a_r = b_{r'} \neq 0$. Since $b_{r'}$ is prime to p, we may assume $a_r = 1$. Hence there exists an element $\xi'' \in V_n$ with

$$v_{n+1} = \xi'' v_n^{1/p} \eta_{n+1}^{T^{r'}}. \tag{2.2}$$

Moreover, we have $(v_{n+1}^{1/p})^T = \xi''' \eta_{n+1}^{-(1+Tf_{n+1}(T))}$ for some $\xi''' \in E'_n$ by $\eta_{n+1}^{T^{r'+1}} = \eta_n \eta_{n+1}^{-p(1+Tf_{n+1}(T))}$. We put $V'_{n+1} = \langle V_{n+1} \cup \{v_{n+1}^{1/p}\} \rangle$. Then there exist $\varepsilon' \in E'_{n+1}$, $v'_{n+1} \in V_{n+1}$, $\eta^* \in V_n$ and $y, z_0, \dots, z_{r'} \in \{0, 1, \dots, p-1\}$ with

$$\varepsilon'^p = v'_{n+1} = \eta^* (v_n^{1/p})^y \eta_{n+1}^{z_0 + z_1 T + \dots + z_{r'-1}T^{r'-1}} (v_{n+1}^{1/p})^{z_{r'}}$$

and $(v'_{n+1})^T \equiv 1 \pmod{V'^p_{n+1}}$ by the assumption $e_{n+1} - e_n \geqslant 2$. Since

$$\begin{aligned} (v'_{n+1})^T &\equiv (\eta^*)^T (\xi' \eta_n^{-(1+Tf_n(T))})^y \eta_{n+1}^{z_0 T + \dots + z_{r'-1}T^{r'-1}} \\ &\quad \cdot (\xi''^{-1} v_n^{-1/p})^{z_{r'-1}} (\xi''' \eta_{n+1}^{-(1+f_{n+1}(T))})^{z_{r'}} \\ &\equiv 1 \pmod{V'^p_{n+1}}, \end{aligned}$$

we have $z_0 = z_1 = \dots = z_{r'} = 0$. This contradicts the assumptions.

https://doi.org/10.1112/S146115701400014X Published online by Cambridge University Press

3. *Algorithm for constructing* E'_n

As we explain in the later section, we often meet the situation $e_1 - e_0 = 1$. In this case, we are able to develop an efficient algorithm for constructing E'_n. By Corollary 1.2 and (2.2), $E'_n/\mathcal{E}_n$ is a cyclic group with order $|E'_n/\mathcal{E}_n| \leqslant p^n$. We assume $|E'_n/\mathcal{E}_n| = p^n$ and construct E'_n as follows.

Based on the cyclicity of $E'_n/\mathcal{E}_n$, there exist unique subgroups $V_{n,k}$ $(0 \leqslant k \leqslant n)$ which satisfy

$$\mathcal{E}_n = V_{n,0} \subset V_{n,1} \subset V_{n,2} \subset \ldots \subset V_{n,n} = E'_n,$$
$$(V_{n,k+1} : V_{n,k}) = p.$$

We write V_k for $V_{n,k}$.

Let $r = p^n - 2$ and $\varepsilon_i = \eta_n^{\gamma^i}$ $(0 \leqslant i \leqslant r)$. Then V_k has the form

$$V_k = \langle \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{r-1}, v_k \rangle$$

with $v_k \in E'_n$. Note that $v_0 = \varepsilon_r$. We explain how to construct v_{k+1} from v_k. By an argument similar to the proof of Lemma 2.3, we may assume $v_{k+1}^p \in V_k$ and $v_{k+1}^{p(1-\gamma)} \in V_k^p$. Namely, we search for integers x_{ik}, y_{ik} and $v_{k+1} \in E'_n$ satisfying

$$v_{k+1}^p = \left(\prod_{i=0}^{r-1} \varepsilon_i^{x_{ik}}\right) v_k, \tag{3.1}$$

$$v_{k+1}^{p(1-\gamma)} = \left(\left(\prod_{i=0}^{r-1} \varepsilon_i^{y_{ik}}\right) v_k^{y_{rk}}\right)^p. \tag{3.2}$$

If v_{k+1} exists, then the following relations hold:

$$v_k^{-p^k} = \left(\prod_{i=0}^{r-1} \varepsilon_i^{p^k x_{ik}}\right) v_{k+1}^{-p^{k+1}}, \tag{3.3}$$

$$v_{k+1}^{1-\gamma} = \left(\prod_{i=0}^{r-1} \varepsilon_i^{y_{ik} - y_{rk} x_{ik}}\right) v_{k+1}^{p y_{rk}}. \tag{3.4}$$

The first step is to find $a_{ij} \in \mathbb{Z}$ which satisfy

$$\varepsilon_j^{1-\gamma} = \prod_{i=0}^{r} \varepsilon_i^{a_{ij}} \quad (0 \leqslant j \leqslant r).$$

This is straightforward because

$$\varepsilon_j^{1-\gamma} = \varepsilon_j \varepsilon_{j+1}^{-1} \quad (0 \leqslant j \leqslant r-1),$$
$$\varepsilon_r^{1-\gamma} = \varepsilon_0 \varepsilon_1 \ldots \varepsilon_{r-1} \varepsilon_r^2.$$

Then $A_0 = (a_{ij})$ is the representation matrix of $1 - \gamma : V_0 \longrightarrow V_0$ with respect to the basis $\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{r-1}, v_0\}$. It is easy to see that the rank of A_0 modulo p is r and $\dim \operatorname{Ker}(A_0 : \mathbb{F}_p^{r+1} \ni x \mapsto A_0 x \in \mathbb{F}_p^{r+1}) = 1$. Let $x_{i0} \equiv r - i + 1 \pmod{p}$ $(0 \leqslant i \leqslant r)$ with $0 \leqslant x_{i0} \leqslant p - 1$ and put ${}^t x_0 = (x_{00}, x_{10}, \ldots, x_{r0}) \in \mathbb{Z}^{r+1}$. Then there exists ${}^t y_0 = (y_{00}, y_{10}, \ldots, y_{r0}) \in \mathbb{Z}^{r+1}$ satisfying $A_0 x_0 = p y_0$. By the assumption $e_1 - e_0 = 1$, we see that $|E'_n/\mathcal{E}_n| \geqslant p$ and there exists $v_1 \in E'_n$ which satisfies (3.1) and (3.2) for $k = 0$. It is straightforward to see that

$$\varepsilon_{r-1}^{1-\gamma} = \left(\prod_{i=0}^{r-1} \varepsilon_i^{x_{i0}}\right) \varepsilon_{r-1} v_1^{-p}. \tag{3.5}$$

From (3.5) and (3.4), we immediately construct the representation matrix A_1 of $1-\gamma : V_1 \longrightarrow V_1$ with respect to the basis $\{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{r-1}, v_1\}$. The first $r-1$ columns of A_0 and A_1 coincide. The last two columns vary.

When we construct v_{k+1} from v_k for $k \geqslant 1$, we need some trials. We note the following property of the representation matrix A_k of $1-\gamma : V_k \longrightarrow V_k$ with respect to the basis $\{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{r-1}, v_k\}$.

Lemma 3.1. *For any $k \geqslant 1$, the rank of A_k modulo p is greater than $r-2$.*

Proof. The determinant of the $(r-1)\times(r-1)$ matrix obtained from the first $r-1$ rows and $r-1$ columns of A_k is 1. □

Namely, $\dim \operatorname{Ker}(A_k{:}\mathbb{F}_p^{r+1} \ni x \mapsto A_k x \in \mathbb{F}_p^{r+1}) \leqslant 2$ and we easily find ${}^t x_k = (x_{0k}, x_{1k}, \dots, x_{rk}) \in \mathbb{Z}^{r+1}$ with $0 \leqslant x_{ik} \leqslant p-1$ $(0 \leqslant i \leqslant r)$, $x_{rk} = 1$ and ${}^t y_k = (y_{0k}, y_{1k}, \dots, y_{rk}) \in \mathbb{Z}^{r+1}$ which satisfy $A_k x_k = p y_k$. Starting with v_1, we try to find $v_2, v_3, \dots, v_n$. If $v_1, \dots, v_k$ exist and v_{k+1} does not exist, then we have $(E_n' : \mathcal{E}_n) = p^k$. Note that A_{k+1} is constructed using the relations (3.3)–(3.5).

A naive method constructing V_{k+1} from V_k needs p^r trials. A sophisticated idea of Zassenhaus in [**6**, p. 66] reduces it to pr trials but usually requires an integral basis of K_n. Our method does not need an integral basis and finds v_{k+1} within p trials.

4. *Examples*

We carry out practical calculations when $p = 3$ and try to apply our technique to determinethe Iwasawa λ-invariant $\lambda(K_\infty/K)$. In the preceding paper [**3**], we studied $\lambda(K_\infty/K)$ for several imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-m})$. We showed $\lambda(K_\infty/K) = 0$ for most of these K. Values of m for which we were not able to assert $\lambda(K_\infty/K) = 0$ are $-2183, -4637, -6761, -7907$ and $-17\,786$. For these m, we calculate the 3-part 3^{e_n} of the ideal class number $h(K_n)$ of K_n.

The first step is the calculation of e_1. This is easily done because the rank of $\mathcal{E}_1$ is 2, and E_1' is constructed straightforwardly. We verified $e_1 - e_0 = 1$ for all above m. So we are able to calculate e_n according to the technique in the previous section. We show the results in the following table, from which we see $\lambda(K_\infty/K) = 0$ for all those K using Theorem 1 in [**2**].

m	e_0	e_1	e_2	e_3	e_4	e_5
−2183	1	2	3	4	4	4
−4637	1	2	3	4	4	4
−6761	1	2	3	4	5	5
−7907	1	2	3	4	4	4
−17 786	2	3	4	5	6	6

5. *Miscellaneous techniques in calculations*

We explain how we calculate special values of Siegel functions quickly and how we construct the cube root of an integer of K_n. First we consider the expression of an integer of K_n.

When $n = 1$, a well-known method due to Pohst and Zassenhaus enables us to construct an integral basis of K_n easily. When $n = 2$, we used a special techniques to construct an integral basis of K_n in [**3**]. It seems very hard to get an integral basis when $n \geqslant 3$. So we adopt another method. Let α be an integer of K_n not contained in K_{n-1}. Then

$$f_{n,\alpha}(X) = \prod_{\sigma \in \mathrm{Emb}(K_n, \mathbb{C})} (X - \alpha^\sigma)$$

https://doi.org/10.1112/S146115701400014X Published online by Cambridge University Press

is an irreducible polynomial in $\mathbb{Z}[X]$, where $\mathrm{Emb}(K_n, \mathbb{C})$ means the set of all embeddings of K_n into $\mathbb{C}$. Then $f_{n,\alpha}(X)$ is considered to express $2 \cdot 3^n$ conjugates of α. We can specify α rigorously by using $f_{n,\alpha}(X)$ and an approximate value of α with an appropriate precision. Namely, we use a correspondence

$$\alpha \longleftrightarrow \begin{cases} \text{approximate values of } \alpha^\sigma, & \sigma \in \mathrm{Emb}(K_n, \mathbb{C}), \\ f_{n,\alpha}(X). \end{cases}$$

Next we discuss how to get a cube root of α for an integer α in K_n. If one of the cube roots of α is contained in K_n, then only one of them, which we write $\sqrt[3]{\alpha}$, is contained in K_n because ζ_3 is not contained in K_n. We note the following fact.

LEMMA 5.1. *Let α be an integer of K_n. If $f_{n,\alpha}(X) = g(X)^{3^e}$ with an irreducible monic polynomial $g(X) \in \mathbb{Z}[X]$ and a non-negative integer e, then $\alpha \in K_{n-e}$. More precisely, we have $K_{n-e} = \mathbb{Q}(\alpha)$ and $g(X) = f_{n-e,\alpha}(X)$.*

Proof. If $e = 0$, then the assertion is trivial. So we assume $1 \leqslant e \leqslant n$. Let $G(K_n/K) = \langle \gamma \rangle$. Then,

$$\mathrm{Emb}(K_n, \mathbb{C}) = \{\gamma^i \mid 0 \leqslant i \leqslant 3^n - 1\} \cup \{\gamma^i J \mid 0 \leqslant i \leqslant 3^n - 1\},$$

where J is the complex conjugation. First, we claim that $\alpha = \alpha^{\gamma^i}$ for some $0 < i < 3^n$. Indeed, if $\alpha \neq \alpha^{\gamma^i}$ for any $0 < i < 3^n$, then we have

$$\alpha = \alpha^{\gamma^i J} = \alpha^{\gamma^j J}$$

for some $0 \leqslant i < j \leqslant 3^n - 1$, which yields $\alpha = \alpha^{\gamma^{j-i}}$. This is a contradiction.

Let i be the least positive integer such that $\alpha = \alpha^{\gamma^i}$ and put $i = 3^a b$ with an integer b prime to 3. Since $\gamma^{3^n} = 1$, we have

$$\alpha = \alpha^{\gamma^{3^a}},$$

which leads to $b = 1$ because of the minimality of $i = 3^a b$. Since

$$G(K_n/K_a) = \langle \gamma^{3^a} \rangle,$$

we have $\alpha \in K_a - K_{a-1}$ and

$$f_{n,\alpha}(X) = g(X)^{3^e} = h(X)^{3^{n-a}}$$

for some monic polynomial $h(X) \in \mathbb{Z}[X]$. Since $g(X)$ is irreducible, we have $e \geqslant n - a$ and

$$h(X) = g(X)^{3^{e+a-n}}.$$

If $e + a > n$, then the above argument implies $\alpha \in K_{a-1}$. This contradicts the fact that $\alpha \in K_a - K_{a-1}$. Hence we have $e + a = n$ and complete the proof. □

LEMMA 5.2. *Assume that $K_n = \mathbb{Q}(\alpha)$ with an integer α in K_n.*
(1) *If $f_{n,\alpha}(X^3)$ is irreducible over $\mathbb{Q}$, then $\sqrt[3]{\alpha} \notin K_m$ for all $m \geqslant n$.*
(2) *If $f_{n,\alpha}(X^3) = g_1(X) g_2(X)$ with an irreducible polynomial $g_1(X) \in \mathbb{Z}[X]$ of degree $2 \cdot 3^n$ and an irreducible polynomial $g_2(X) \in \mathbb{Z}[X]$ of degree $4 \cdot 3^n$, then $\sqrt[3]{\alpha} \in K_n$.*

Proof. The proof is straightforward, noting that $\zeta_3 \notin K_n$. □

According to the above lemmas, we obtain $\sqrt[3]{\alpha}$ for an integer α of K_m as follows. Factoring $f_{m,\alpha}(X)$, we find n with $0 \leqslant n \leqslant m$ and the minimal polynomial $f_{n,\alpha}(X)$ of α. If $f_{n,\alpha}(X^3)$ is irreducible, then $\sqrt[3]{\alpha} \notin K_m$. If $f_{n,\alpha}(X^3)$ has an irreducible factor $g(X)$ of degree $2 \cdot 3^n$, then

https://doi.org/10.1112/S146115701400014X Published online by Cambridge University Press

$\sqrt[3]{\alpha} \in K_m$. Let σ be an element of $\mathrm{Emb}(K_m, \mathbb{C})$. Then $\sqrt[3]{\alpha}^{\sigma}$ is one of $\rho\zeta^i$ $(i = 0, 1, 2)$, where ρ is a fixed cube root of α^σ. We specify $\rho\zeta^i$ so that $g(\rho\zeta^i) = 0$. In this manner, we get the minimal polynomial of $\sqrt[3]{\alpha}$ and all conjugates of $\sqrt[3]{\alpha}$ explicitly.

Finally, we make a remark on the calculation of Siegel functions. In [**3**], we needed approximate values of $g(a_1, a_2)(\tau)$ with the precision of several thousand digits and calculated the infinite product straightforwardly. In this paper, we calculated the 3-part of the class number of K_5 and needed approximate values with 10^5 digits. So we translated an infinite product into an infinite sum.

LEMMA 5.3. *Let q_τ and q_z be complex numbers defined in § 1. Then we have*

$$-(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}) = q_z^{1/2}\,\frac{\sum_{n=0}^{\infty}(-1)^n(q_z^{n+1/2}-q_z^{-n-1/2})q_\tau^{n(n+1)/2}}{1+\sum_{n=1}^{\infty}(-1)^n(q_\tau^{n(3n-1)/2}+q_\tau^{n(3n+1)/2})}.$$

Proof. See [**1**, Proposition 6.3.14 and Corollaries 6.3.16 and 6.3.18]. □

REMARK 1. The convergence of the left-hand side depends on q_τ^n. On the other hand, the right-hand side converges very quickly because it depends essentially on $q_\tau^{n^2}$.

REMARK 2. When $a_1 = 0$, $q_z = e^{2\pi i a_2}$ is a purely imaginary number and it happens that $q_z^{n+1/2} = q_z^{-n-1/2}$ for small n. So we have to stop summing based on the magnitude of $|q_\tau^{n(n+1)/2}|$.

REMARK 3. There is another way to use the σ-function to construct ray class fields of imaginary quadratic fields. But the σ-function needs calculations of quasi-periods which are essentially the sum of q_τ^n. Though the Siegel function is similar to the σ-function, it does not need quasi-periods and hence has an advantage of fast convergence.

References

1. H. COHEN, *Advanced topics in computational number theory*, Graduate Texts in Mathematics 193 (Springer, Berlin, 2000).

2. T. FUKUDA, 'Remarks on $\mathbb{Z}_p$-extensions of number fields', *Proc. Japan Acad. Ser. A Math. Sci.* 65 (1989) 260–262.

3. T. FUKUDA and K. KOMATSU, 'Non-cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields', *Exp. Math.* 11 (2002) 469–475.

4. R. GILLARD, 'Fonctions Lp-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes', *J. reine angew. Math.* 358 (1985) 76–91.

5. D. S. KUBERT and S. LANG, *Modular units*, Grundlehren der Mathematischen Wissenschaften 244 (Springer, 1981).

6. M. E. POHST, 'Computing invariants of algebraic number fields', *Group theory, algebra, and number theory* (ed. H. G. Zimmer; de Gruyter, 1996) 53–73.

7. L. SCHNEPS, 'On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication', *J. Number Theory* 25 (1987) 20–33.

T. Fukuda
Department of Mathematics
College of Industrial Technology
Nihon University, 2-11-1 Shin-ei
Narashino, Chiba 275-8576
Japan

fukuda.takashi@nihon-u.ac.jp

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

kkomatsu@waseda.jp