

CONGRUENCES OF ANKENY-ARTIN-CHOWLA TYPE FOR PURE QUARTIC AND SECTIC FIELDS

MASATO KAMEI

§ 0. Introduction

Ankeny, Artin and Chowla [1] showed that there are congruences between class numbers of real quadratic fields and generalized Bernoulli numbers. Recently, Ito [3] has extended their results to the case of pure cubic fields using generalized Hurwitz numbers of Lichtenbaum [4]. In his paper, he suggested that similar results would be obtained for pure quartic and septic fields. In this paper, we carry out this by following his idea. To give a congruence in an exact form, we need an idea due to Matthews [5]. As the argument in the septic case is quite parallel to that in the quartic case, we shall discuss the former case briefly in the last two sections.

We will explain our result in the quartic case more exactly. Let $K = \mathbf{Q}(\sqrt{-1})$, $L = \mathbf{Q}(\sqrt[4]{m})$, and $F = \mathbf{Q}(\sqrt{m})$, where m is a positive integer prime to 6. For an arbitrary algebraic number field T , we denote its class number, ring of integers, group of units, regulator by h_T , \mathcal{O}_T , E_T , R_T respectively. Let η_1 be an element of E_L for which $\text{Ker}[N_{L/F}: E_L \rightarrow E_F] = \langle \pm 1, \eta_1 \rangle$ holds. We may assume $\eta_1 > 1$, by replacing η_1 by $-\eta_1$ or $\pm 1/\eta_1$ if necessary. Let $\eta_2 = \eta_1^2$ or η_1 according as $|E: \langle \pm 1, \varepsilon_0, \eta_1 \rangle| = 1$ or 2. Here ε_0 is the fundamental unit of F . Write η_2 as $\eta_2 = s + t\sqrt[4]{m} + u\sqrt{m} + v\sqrt[4]{m}^3$ with rational numbers s, t, u and v . Let $M = L \cdot K$ and ρ the character of $\text{Gal}(M/K)$ of order 4 defined by the quartic residue symbol $\left(\frac{m}{\cdot}\right)_4$. We denote the conductor of ρ by (f) . Take a prime number π in K which is prime to 2 and divides m exactly once, and let $k_0 = (q-1)/4$, where $q = N\pi = N_{K/\mathbf{Q}}\pi$. We may assume $\pi \equiv 1 \pmod{(1+i)^5}$, by replacing π by $-\pi$ or $\pm i\pi$ if necessary. We decompose ρ into a product of characters ρ_1, ρ_2 so that the conductor of ρ_1 is (π) , and that of ρ_2 is (f/π) . Let

Received August 23, 1986.

$G_{k_0, \rho_2}, G_{3k_0, \rho_2^{-1}}$ be the generalized Hurwitz numbers defined in Lichtenbaum [4]. In these notations, we can state our results as

THEOREM 1. *Let \mathfrak{Q}' be a prime of $\bar{\mathbf{Q}}$ lying above (π) . Then one has;*

- i) $(h_L/h_F)st \equiv G_{k_0, \rho_2}/\xi \pmod{\mathfrak{Q}'}$,
- ii) $(h_L/h_F)(3su - tu) \equiv G_{3k_0, \rho_2^{-1}}/\xi^3 \pmod{\mathfrak{Q}'}$.

Here ξ is a quartic root of $-m/\pi$.

In the above theorem, there is left the ambiguity in the determination of ξ , which arises from the gap between the local theory and the global theory (cf. Remark 3). Generally, it seems difficult to determine ξ explicitly. However, when m is a rational prime which remains prime in K , we can determine it in Section 2 studying values of the Weierstrass \mathcal{P} -function. We shall give this result as Theorem 10. A few numerical examples will be given.

§ 1. The quartic case

We use the notations introduced in Section 0. In this section, we shall prove Theorem 1. Since the proof proceeds in the same way as in Ito [3], sometimes the details will be omitted. Usually we follow the notations in Ito [3].

Decompose m as $m = ab^2c^3$, where a, b, c are square-free integers and prime to each other. Then the conductor (f) of ρ is given as follows:

$$f = \begin{cases} abc & \text{if } m \equiv 1 \pmod{8}, \\ 2abc & \text{if } m \equiv 5 \pmod{8}, \\ 4abc & \text{if } m \equiv 3, 7 \pmod{8}. \end{cases}$$

Let χ be the character of $\text{Gal}(L/F)$ of order 2. Then we have

$$L(s, \rho, M/K) = L(s, \chi, L/F)$$

and consequently

$$(1.1) \quad L'(0, \rho, M/K) = L'(0, \chi, L/F).$$

A direct computation shows

$$L'(0, \chi, L/F) = (h_L/h_F) \log \eta_2.$$

On the other hand, $L'(0, \rho, M/K)$ can be expressed by elliptic units in the following way.

For a non zero integer α of K , let K_α be the maximal ray class field modulo α of K , and $\text{Cl}(\alpha)$ the ray class group of K modulo α . For $C \in \text{Cl}(f)$, let $\phi_f(C)$ denote the Ramachandra invariant (cf. Ramachandra [6]). For $\alpha \in \mathfrak{O}_K$, let C_α be the class of (α) in $\text{Cl}(f)$. We choose $\gamma \in \mathfrak{O}_K$ which satisfies $\rho(C_\gamma) = -1$. Then we have

$$\begin{aligned}
 L'(0, \rho, M/K) &= \frac{1}{6f} \log |N_{K_f/M} \phi_f(C_\gamma) / \phi_f(C_1)| \\
 (1.2) \qquad &= \frac{1}{12f} \log \left\{ \prod_{C \in \text{Cl}(f)} \phi_f(C)^{-\left(\rho(C) + \rho^3(C)\right)} \right\}.
 \end{aligned}$$

Now we take the f -th power root of $L'(0, \rho, M/K)$ by Robert's unit (cf. Robert [7]). Let E be the elliptic curve given by $y^2 = 4x^3 - 4x$ and let \mathcal{L} be the period lattice associated with the differential form dx/y on E . Then $\mathcal{L} = \mathfrak{O}_K \Omega$ with some $\Omega \in \mathbf{R}_+$ ($\mathbf{R}_+ = \{a \in \mathbf{R} \mid a > 0\}$). For $\alpha \in \mathfrak{O}_K$, we introduce the elliptic function for \mathcal{L} defined by

$$\phi(z, \alpha) = \alpha^{12} \Delta(\mathcal{L})^{1-N\alpha} \prod'_{\beta \in \alpha^{-1}\mathcal{L}/\mathcal{L}} (\mathcal{P}(z) - \mathcal{P}(\beta))^6$$

where $\mathcal{P}(z)$ is the Weierstrass \mathcal{P} -function for \mathcal{L} , $\Delta(A)$ is the delta-function for the lattice A in \mathbf{C} , $N\alpha = N_{K/Q}\alpha$, and the product \prod' is extended to all over $\alpha^{-1}\mathcal{L}/\mathcal{L}$ except the class of \mathcal{L} . Choose a finite index set J and $\beta_j \in \mathfrak{O}_K$, $m_j \in \mathbf{Z}$ ($j \in J$) which satisfy the following conditions:

$$\begin{aligned}
 N\gamma - 1 + \sum_{j \in J} m(N\beta_j - 1) &= 0, \\
 \rho(C_{\beta_j}) = 1, \quad \text{and} \quad (\beta_j, 6f) &= 1.
 \end{aligned}$$

We can take such set and numbers (cf. Robert [7]). For $\tau = \Omega/f$, define η by the equation

$$\eta = \phi(\tau, \gamma) \prod_{j \in J} \phi(\tau, \beta_j)^{m_j}.$$

It is known that η is a unit in K_f and satisfies

$$N_{K_f/M} \eta^f = N_{K_f/M} \phi_f(C_\gamma) / \phi_f(C_1).$$

Hence we have

$$L'(0, \rho, M/K) = \frac{1}{12} \log \eta \bar{\eta}.$$

So we get the next relation as an exponential form of (1.1):

$$(1.3) \qquad \eta_2^{12h_{\mathcal{L}/h_F}} = N_{K_f/M} \eta \bar{\eta}.$$

Here, $\bar{\eta}$ is the complex conjugate of η , which satisfies

$$\bar{\eta} = \phi(\tau, \bar{\tau}) \prod_{j \in \mathcal{J}} \phi(\tau, \bar{\beta}_j)^{m_j}.$$

Let us recall the definition of generalized Hurwitz numbers. Decompose τ in such a way as $\tau \equiv \tau_1 + \tau_2 \pmod{\mathcal{L}}$, where τ_1 is a π -division point of \mathcal{L} and τ_2 is a f/π -division point of \mathcal{L} . For an integer k and a character $\chi = \rho_2$ or ρ_2^{-1} , let G_{k,χ,τ_2} be the generalized Hurwitz number as in Lichtenbaum [4]. We denote it by $G_{k,\chi}$, and the conductor of $\chi (= f/\pi)$ by f_2 . Then we can prove the next assertions.

PROPOSITION 2. i) $G_{k,\rho_2}, G_{k,\rho_2^{-1}} \in K_{f_2}$.

ii) $G_{k,\rho_2}/\sqrt[4]{m_2}, G_{k,\rho_2^{-1}}/\sqrt[4]{m_2^3} \in K(\sqrt{2})$, where $m_2 = m/\pi$.

iii) If m is a rational prime p such that $p \equiv 3 \pmod{4}$, then $G_{k,\rho_2}/\sqrt{2}, G_{k,\rho_2^{-1}}/\sqrt{2} \in \mathbb{Q}$.

Proof. Only iii) is the essentially new situation compared with Ito [3]. In this case, we have $f = 4p, \pi = -p$ (Recall that $\pi \equiv 1 \pmod{(1+i)^3}$), $f_2 = -4, \tau_2 \equiv -(1/4)\Omega \pmod{\mathcal{L}}$, and $\rho_2 = \rho_2^{-1}$. As ρ_2 is a non trivial even character, we know

$$\frac{1}{2} \sum_{\substack{\alpha \pmod{f_2} \\ (\alpha, f_2) = 1}} \rho_2(\alpha)^{-1} \frac{\mathcal{P}'(z)}{\mathcal{P}(z) - \mathcal{P}(\alpha\tau_2)} = -\sum_{k=1}^{\infty} G_{k,\rho_2} z^{k-1}$$

(cf. Lichtenbaum [4]). Calculation of the values of $\rho_2(\tau), \mathcal{P}(\alpha\tau_2)$ (x -coordinate of a 4-division point of $y^2 = 4x^3 - 4x$) gives the next formula:

$$-\sum_{k=1}^{\infty} G_{k,\rho_2} z^{k-1} = 2\sqrt{2} \mathcal{P}'(z) \frac{1}{(\mathcal{P}(z) - 1)^2 - 2} + \frac{1}{(\mathcal{P}(z) + 1)^2 - 2}$$

$$\left(\text{resp. } 2\sqrt{2} \mathcal{P}'(z) \frac{1}{(\mathcal{P}(z) - 1)^2 - 2} - \frac{1}{(\mathcal{P}(z) + 1)^2 - 2} \right)$$

if $p \equiv 3 \pmod{8}$ (resp. $p \equiv 7 \pmod{8}$). Thus iii) holds.

Let us recall the definition of Kummer’s logarithmic derivatives. Let S/R be a totally ramified extension of p -adic fields. Choose a prime element λ of S . Let $\mathcal{O}_S, \mathcal{O}_R$ be the ring of p -adic integers and $\mathfrak{m}_S, \mathfrak{m}_R$ the valuation ideals respectively. For $u \in 1 + \mathfrak{m}_S$, we can take $f_u(T) \in \mathcal{O}_R[[T]]$ which satisfies $f_u(\lambda) = u$. Then for $k, 1 \leq k \leq \#(\mathcal{O}_R/\mathfrak{m}_R) - 1$, the k -th Kummer’s logarithmic derivative $\phi_k = \phi_{k,\lambda}: 1 + \mathfrak{m}_S \rightarrow \mathcal{O}_R/\mathfrak{m}_R$ is defined as

$$\phi_k(u) = \left(\text{the coefficient of } T^k \text{ in } T \frac{d}{dT} \log f_u(T) \pmod{m_\pi} \right).$$

We extend this to S^\times in the usual way.

Now we will calculate $\phi_k(\eta)$. To carry out this, we embed $\bar{\mathbf{Q}}$ into C_p , the completion of the algebraic closure of \mathbf{Q}_p . For $\alpha \in \mathfrak{O}_K$, let $K(E_\alpha)$ be the field generated by the coordinates of α -division points of E over K . We know that $K(E_\pi)$ is a cyclic extension of degree $q - 1$ ($q = N\pi$) with the conductor $(\pi(1 + i)^3)$. Note that (π) totally ramifies in $K(E_{f_2})$, and is unramified in $K(E_{f_2})$.

Choose a prime ideal \mathfrak{Q} of $K(E_f)$ over (π) and embed $K(E_f)$ into C_p , so that \mathfrak{Q} is contained in the valuation ideal of C_p . Put $\mathfrak{q} = \mathfrak{Q} \cap K(E_\pi)$, $\mathfrak{P} = \mathfrak{Q} \cap K(E_\pi)$, $\mathfrak{p} = \mathfrak{Q} \cap K = (\pi)$, and denote the completions of $K, K(E_\pi), K(E_{f_2}), K(E_f)$ in C_p through this embedding by $K_p, K_{\mathfrak{P}}, K_{\mathfrak{q}}, K_{\mathfrak{Q}}$, and let $\mathfrak{O}_p, \mathfrak{O}_{\mathfrak{P}}, \mathfrak{O}_{\mathfrak{q}}, \mathfrak{O}_{\mathfrak{Q}}$ be the rings of p -adic integers, $\mathfrak{m}_p, \mathfrak{m}_{\mathfrak{P}}, \mathfrak{m}_{\mathfrak{q}}, \mathfrak{m}_{\mathfrak{Q}}$ the valuation idelas of those fields respectively.

Now consider the following three formal groups over \mathfrak{O}_p : G_a , the formal additive group, \hat{E} the formal group of kernel of reduction mod p , \mathcal{E} the basic Lubin-Tate group. These three formal groups are isomorphic over K_p to each other. We denote these isomorphisms by

$$\begin{aligned} s: G_a &\rightarrow \hat{E} & s(z) &= -2\mathcal{P}(z)/\mathcal{P}'(z) = z + (\text{higher terms}), \\ w: \hat{E} &\rightarrow \mathcal{E} & w(t) &= t + (\text{higher terms}). \end{aligned}$$

Especially, w is an isomorphism over \mathfrak{O}_p . Put $\lambda = -2\mathcal{P}(\tau_1)/\mathcal{P}'(\tau_1)$ and $A = w(\lambda)$. Then they satisfy the equations $[\pi]_{\hat{E}}(\lambda) = 0$ and $[\pi]_{\mathcal{E}}(A) = 0$. So λ and A are prime elements of $K_{\mathfrak{P}}$, and satisfy the equation $\lambda \equiv A \pmod{\mathfrak{m}_{\mathfrak{P}}^2}$. From now on, using this A and taking $K_{\mathfrak{Q}}/K_{\mathfrak{q}}$ or $K_{\mathfrak{P}}/K_{\mathfrak{p}}$ as S/R , we define Kummer's logarithmic derivatives ϕ_k as $\phi_{k,A}: K_{\mathfrak{Q}}^\times \rightarrow \mathfrak{O}_{\mathfrak{q}}/\mathfrak{m}_{\mathfrak{q}}$, or its restriction $\phi_{k,A}: K_{\mathfrak{P}}^\times \rightarrow \mathfrak{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$. (Note that A is also a prime element of $K_{\mathfrak{Q}}$.)

Remark 3. Once we fix the embedding $K(E_f) \rightarrow C_p$, λ can be seen as an element of C_p , and so the corresponding A can be determined uniquely as an element of C_p . But if we think A merely as an element of $\bar{\mathbf{Q}}$ which satisfies $A^{q-1} + \pi = 0$, we can not determine which root we have to take. In fact, determining the root is equivalent to choosing the prime ideal of $K(E_f, \mu_{q-1}, \sqrt[q-1]{-\pi})$ lying above \mathfrak{Q} . This is the reason why the ambiguity of theorem 1 appears. We shall consider this problem for a special case in the next section.

Take $u \in 1 + \mathfrak{m}_{\mathfrak{a}}$ and choose $f_u(T) \in \mathfrak{D}_q[[T]]$ which satisfies $f_u(A) = u$. Let $g_u(z) = f_u(w \circ s(z)) \in K_q[[z]]$ be the pull back of $f_u(T)$ by the isomorphisms s, w . Then we have

PROPOSITION 4 (Coates-Wiles [2]).

$$\phi_k(u) = \text{the coefficient of } z^k \text{ in } z \frac{d}{dz} \log g_u(z) \pmod{\mathfrak{m}_q}$$

for $1 \leq k \leq q - 2$.

The Kummer’s logarithmic derivatives $\phi_{k,A}$ are easier to calculate than $\phi_{k,\lambda}$, but elliptic units are “expressed” by λ . This proposition fills this gap.

We will calculate $\phi_k(\eta)$ by considering η as an element of $K_{\mathfrak{a}}$. What we have to do is to choose $f_{\eta}(T) \in \mathfrak{D}_q[[T]]$ which satisfies $f_{\eta}(A) = \eta$, and to take logarithmic derivatives of $g_{\eta}(z) = f_{\eta}(w \circ s(z))$. As $\eta = \phi(\tau, \gamma) \prod \phi(\tau, \beta_j)^{m_j}$, it is sufficient to calculate $\phi_k(\phi(\tau, \delta))$ for each $\delta \in \{\gamma\} \cup \{\beta_j \mid j \in J\}$. Now $\phi(z, \delta) = \delta^{12} \Delta(\mathcal{L})^{1-N\delta} \prod'_{\beta \in \delta^{-1}\mathcal{L}/\mathcal{L}} (\mathcal{P}(z) - \mathcal{P}(\beta))^{\delta}$, so we might expect that $\phi(z + \tau_2, \alpha)$ is a formal power series which is a pull back by s of some $f_{\phi(\tau,\alpha)}(t)$, a power series expanding $\phi(\tau, \alpha)$ by λ . The next proposition shows that this is actually true if $f_2 \neq 1$.

PROPOSITION 5. Assume $f_2 \neq 1$. Let $\delta \in \{\gamma\} \cup \{\beta_j\}$, $\mu \in (\mathfrak{D}_K/f_2\mathfrak{D}_K)^{\times}$. Then the following assertions hold.

- i) $\phi(\tau_1 + \mu\tau_2, \delta) \in \mathfrak{D}_{\mathfrak{a}}^{\times}$.
- ii) $\phi(z + \mu\tau_2, \delta) \in K_q[[z]]$.
- iii) Define $h(t) \in K_q[[t]]$ by $h(s(z)) = \phi(z + \mu\tau_2, \delta)$, then $h(t) \in \mathfrak{D}_q[[t]]$.
- iv) $h(\lambda) = \phi(\tau_1 + \mu\tau_2, \delta)$.

Proof. We prove iii) and iv). For the proof of i) and ii), see Ito [3]. Put

$$F(x, y) = \delta^{12} \Delta(\mathcal{L})^{1-N\delta} \prod'_{\beta} \left(-x - \mathcal{P}(\mu\tau_2) + \frac{1}{4} \left(\frac{y - \mathcal{P}'(\mu\tau_2)}{x - \mathcal{P}(\mu\tau_2)} \right)^2 - \mathcal{P}(\beta) \right)^{\delta}$$

$\in K_q(x, y)$.

We get $\phi(\tau_1 + \mu\tau_2, \delta) = F(\mathcal{P}(\tau_1), \mathcal{P}'(\tau_2))$ as an element of $K_{\mathfrak{a}}$. Now $\lambda = -2\mathcal{P}(\tau_1)/\mathcal{P}'(\tau_1)$ is a prime element of $K_{\mathfrak{p}}$, and it is easily shown that $\mathcal{P}(\tau_1) = \mathcal{P}(s^{-1}(t))|_{t=\lambda}$, $\mathcal{P}'(\tau_1) = \mathcal{P}'(s^{-1}(t))|_{t=\lambda}$ are elements of $K_{\mathfrak{p}}$. Here $\mathcal{P}(s^{-1}(t)) = a(t)/t^2$, $\mathcal{P}'(s^{-1}(t)) = -2a(t)/t^3$ for some $a(t) \in 1 + tZ[[t]]$. So, considering $h(t) = F(\mathcal{P}(s^{-1}(t)), \mathcal{P}'(s^{-1}(t)))$ as a power series of t , we get

$$h(s(z)) = \phi(z + \mu\pi_2, \delta),$$

$$h(\lambda) = \phi(\tau_1 + \mu\tau_2, \delta).$$

This is iv).

Next we want to show iii). As $(\delta, \pi) = (f_2, \pi) = 1$, $\delta, \mathcal{P}(\mu\tau_2), \mathcal{P}'(\mu\tau_2), \mathcal{P}(\beta)$ are units of K_q . Thus we see $F(\mathcal{P}(s^{-1}(t)), \mathcal{P}'(s^{-1}(t))) \in t^{-2}\mathcal{O}_q[[t]]$. On the other hand, we have $\phi(z + \mu\tau_2, \delta) \in K_q[[z]]$, so $h(t)$ has no terms of negative power of t . This is iii).

Remark 6. In the above arguments, we regard $\phi(z + \mu\pi_2, \delta)$ as an element of $K_q[[z]]$, which need not converge in C .

Due to Proposition 5, we obtain the next proposition.

PROPOSITION 7. *Let $\lambda = \rho_2$ or ρ_2^{-1} . Then*

$$\prod_{\mu \in (\mathcal{O}_K/f_2)^\times} \lambda(\mu^{-1})\phi_k(\phi(\tau_1 + \mu\tau_2, \delta)) = 12(N\delta - \delta^k\lambda(\delta))G_{k,\lambda} \pmod{\mathcal{O}}.$$

With these data, we can take Kummer’s logarithmic derivatives of $N_{K_f/M}\eta\bar{\eta}$ following the manner of Ito [3]. The result in this case is as follows.

THEOREM 8. *The following assertions hold.*

- i) $\phi_{k_0}(N_{K_f/M}\eta\bar{\eta}) = -3G_{k_0,\rho_2} \pmod{\mathcal{O}}$.
- ii) $\phi_{3k_0}(N_{K_f/M}\eta\bar{\eta}) = -3G_{3k_0,\rho_2^{-1}} \pmod{\mathcal{O}}$.
- iii) $\phi_k(N_{K_f/M}\eta\bar{\eta}) = 0 \pmod{\mathcal{O}}$, for $k \neq k_0, 3k_0, 1 \leq k \leq q - 2$.

Now take a prime ideal \mathcal{O}' of $K' = K(E_f, \mu_{q-1}, \sqrt[q-1]{-\pi})$ lying above \mathcal{O} , and consider λ as an element of K' as we have referred in Remark 3. Let $\xi = \sqrt[q]{m}/\lambda^{k_0}$, so ξ is a quartic root of $-m_2$ and is contained in K' . Considering K' to be a subfield of K_Σ , we can take Kummer’s logarithmic derivatives of η_2 , by using the function

$$f_{\eta_2}(T) = s + t\xi T^{k_0} + u\xi^2 T^{2k_0} + v\xi^3 T^{3k_0}.$$

Taking Kummer’s logarithmic derivatives of each side of (1.3), we get the desired congruences in Theorem 1.

§ 2. Determination of $\xi \pmod{\mathcal{O}'}$ in special cases

Theorem 1 involves a quartic root and we did not determine it (or rather its value modulo \mathcal{O}') exactly. In case that m is a prime number p which is congruent to 3 modulo 4 and $\pi = -p$, we can determine it.

The method we use is to combine λ and Λ in K' through the values of \mathcal{P} -function (associated to $\Omega_{\mathfrak{D}_K}$) at division points.

By the definition, $q = p^2$. We can easily show that

$$\prod_{\alpha \in (\mathfrak{D}_K/\pi)^\times} \mathcal{P}\left(\frac{\alpha}{\pi}\Omega\right) = \pi^{-2},$$

and

$$\prod_{\alpha \in (\mathfrak{D}_K/\pi)^\times} \mathcal{P}'\left(\frac{\alpha}{\pi}\Omega\right) = (-64)^{(q-1)/4}\pi^{-3}.$$

So we get

$$\prod_{\alpha \in (\mathfrak{D}_K/\pi)^\times} \frac{-2\mathcal{P}\left(\frac{\alpha}{\pi}\Omega\right)}{\mathcal{P}'\left(\frac{\alpha}{\pi}\Omega\right)} = \frac{\pi}{(1+i)^{q-1}} = -p/16^{(q-1)/8}.$$

(Note that this is a real negative number.)

We introduce a forth-set according to Matthews [5]. A representative set of $(\mathfrak{D}_K/\pi)^\times/\mu_4$ ($\mu_4 = \{\pm 1, \pm i\}$) in $(\mathfrak{D}_K/\pi)^\times$ is called a forth-set. If S is a forth-set, $(\mathfrak{D}_K/\pi)^\times$ is decomposed into four disjoint subsets $S, -S, iS, -iS$. Define

$$G(S) = \prod_{\alpha \in S} \left\{ -2\mathcal{P}\left(\frac{\alpha}{\pi}\Omega\right) / \mathcal{P}'\left(\frac{\alpha}{\pi}\Omega\right) \right\}.$$

As $\mathcal{P}(iz) = -\mathcal{P}(z)$ and $\mathcal{P}'(iz) = i\mathcal{P}'(z)$, $G(\beta S) = \left(\frac{\beta}{\pi}\right)_4 G(S)$ for all $\beta \in (\mathfrak{D}_K/\pi)^\times$.

Therefore

$$G(S) = \sqrt[4]{-p/16^{(q-1)/8}} = \sqrt[4]{p/2^{(q-1)/8}}\zeta_8\varepsilon$$

for some $\varepsilon \in \mu_4$. Define $\alpha(S) \in (\mathfrak{D}_K/\pi)^\times$ as $\alpha(S) = \prod_{\beta \in S} \beta$. Then $G(S)$ depends only on $\alpha(S)$. In fact, if we consider $\alpha(S)$ as an element of K' through the natural map $(\mathfrak{D}_K/\pi)^\times \rightarrow \mathfrak{D}_K^\times$, then $G(S)/\alpha(S)$ is defined as an element of K' independently of S .

Now we make a special choice of S , and determine $G(S)$ and $\alpha(S)$. Let $S_1 = \{a \in N \mid 1 \leq a \leq (p-1)/2\}$, $S_2 = iS_1$, $S_+ = \{a + bi \in \mathfrak{D}_K \mid 2 \leq a \leq (p-1)/2, 0 < b < a\}$ and $S_- = \bar{S}_+$ (complex conjugate). Then $S = S_1 \cup S_2 \cup S_+ \cup S_-$ (disjoint union) is a forth-set. Put $\tau_0 = (1/p)\Omega$. We know that $\mathcal{P}(\bar{z}) = \overline{\mathcal{P}(z)}$, $\mathcal{P}'(\bar{z}) = \overline{\mathcal{P}'(z)}$, and that $-2\mathcal{P}(\alpha\tau_0)/\mathcal{P}'(\alpha\tau_0) \in \mathbf{R}_+$ if $\alpha \in S_1$, and $-2\mathcal{P}(\alpha\tau_0)/\mathcal{P}'(\alpha\tau_0) \in \zeta_8\mathbf{R}_+$ if $\alpha \in S_2$. So we get

$$G(S) = \zeta_8^{(p-1)/2} \sqrt[4]{p/2^{(q-1)/8}}.$$

Next we have to determine $\alpha(S)$. Let F_l be the finite field with l elements. The norm map $N: F_q^\times \rightarrow F_p^\times$ is a surjection, and $N^{-1}(x)$ consists of $(p + 1)$ elements for any $x \in F_p^\times$. As $N(\mu_4) = \{1\}$, the restriction of N to S is also a surjection, and each fibre of it consists of $(p + 1)/4$ elements.

If $p \equiv 3 \pmod 8$, $N(a + ai) = 2a^2$ is not contained in $(F_p^\times)^2$, and so $N; S_1 \cup S_2 \rightarrow F_p^\times$ is a bijection. Thus we obtain

$$\prod_{\alpha \in S} \alpha = \left(\prod_{\alpha \in S_1 \cup S_2} \alpha \right) \left(\prod_{\alpha \in S_+} N\alpha \right) = (-1)^{(p-3)/8} (1 + i)^{(p-1)/2} \pmod{\pi}.$$

If $p \equiv 7 \pmod 8$, $N(a + ai) = 2a^2$ is contained in $(F_p^\times)^2$. So if $x \in (F_p^\times)^2$, $N^{-1}(x) \cap S_+$ consists of $(p - 7)/8$ elements, and if not, $(p + 1)/8$ elements. Thus we obtain

$$\prod_{\alpha \in S} \alpha = \left(\prod_{\alpha \in S_1 \cup S_2} \alpha \right) \left(\prod_{\alpha \in S_+} N\alpha \right) = (-1)^{(p+1)/8} (1 + i)^{(p-1)/2} \pmod{\pi}.$$

Now we want to relate $A^{(q-1)/4}$ to $G(S)$ and $\alpha(S)$. We have defined $\lambda, A \in K'$ as $\lambda = -2\mathcal{P}(\tau_1) | \mathcal{P}'(\tau_1)$, A a root of $T^{q-1} + \pi = 0$ which satisfies $\lambda \equiv A \pmod{\mathfrak{Q}^2}$. Observing the action of $\text{Gal}(K'/K)$, we see

$$(2.1) \quad -2\mathcal{P}(\nu\tau_1) | \mathcal{P}'(\nu\tau_1) \equiv \zeta_\nu A \pmod{\mathfrak{Q}^2},$$

for all $\nu \in (\mathfrak{O}_K/\pi)^\times$, where $\zeta_\nu \in \mu_{q-1}$, $\zeta_\nu \equiv \nu \pmod{\mathfrak{Q}'}$. By the definition, we know that $\pi = -p$ hence $f = 4p$, $4\tau_1 \equiv \tau_0 \pmod{\mathcal{L}}$. Multiplying (2.1) for all ν in S , we obtain

$$G(-4^{-1}S) \equiv \alpha(S)A^{(q-1)/4} \pmod{\mathfrak{Q}'^{(q-1)/4+1}}.$$

As $\left(\frac{-1}{\pi}\right)_4 = \left(\frac{4}{\pi}\right)_4 = 1$, $G(-4^{-1}S) = G(S)$. After all, we get

PROPOSITION 9.

$$\begin{aligned} \xi &= \sqrt[4]{p} | A^{(q-1)/4} \equiv \sqrt[4]{p} \alpha(S) / G(S) \pmod{\mathfrak{Q}'} \\ &\equiv \begin{cases} -\sqrt{2} 2^{(p-3)/4} \pmod{\mathfrak{Q}'}, & \text{if } p \equiv 3, 7 \pmod{16}, \\ \sqrt{2} 2^{(p-3)/4} \pmod{\mathfrak{Q}'}, & \text{if } p \equiv 11, 15 \pmod{16}. \end{cases} \end{aligned}$$

By this proposition, we can rewrite Theorem 1 in this case in the following exact form.

THEOREM 10. *Let $L = \mathbf{Q}(\sqrt[4]{p})$, where p is a rational prime and $p \equiv 3 \pmod 4$. Put $k_0 = (p^2 - 1)/4$. Then*

$$i) \quad (h_L/h_F)st \equiv 2^{(p+1)/4} G_{k_0, \rho_2} / \sqrt{2} \times \varepsilon \pmod p,$$

where $\varepsilon = 1$ if $p \equiv 3, 15 \pmod{16}$, and $\varepsilon = -1$ if $p \equiv 7, 11 \pmod{16}$.

$$\text{ii) } (h_L/h_F)(3sv - tu) \equiv 2^{(p+1)/4} G_{3k_0, \rho_2} / \sqrt{2} \times \varepsilon \pmod{p},$$

where $\varepsilon = 1$ if $p \equiv 11, 15 \pmod{16}$, and $\varepsilon = -1$ if $p \equiv 3, 7 \pmod{16}$.

EXAMPLE 11. Let $p = 7$, $L = \mathbf{Q}(\sqrt[4]{7})$, $F = \mathbf{Q}(\sqrt{7})$. Then we have $\eta_1 = 13 + 8\sqrt[4]{7} + 5\sqrt{7} + 3\sqrt[4]{7^3}$, $h_2 = 43 + 26\sqrt[4]{7} + 16\sqrt{7} + 10\sqrt[4]{7^3}$, $h_K = 1$, $h_L = 2$. So in this case, $(h_L/h_F)st \equiv 3 \pmod{7}$ and $(h_L/h_F)(3sv - tu) \equiv 5 \pmod{7}$. On the other hand, we have

$$G_{12, \rho_2} = \sqrt{2} \times 11232/25 \equiv \sqrt{2} \pmod{7},$$

$$G_{36, \rho_2} = \sqrt{2} \times 1447788874210204192/127679296875 \equiv 4\sqrt{2} \pmod{7}.$$

So we see

$$2^{(7+1)/4} G_{12, \rho_2} / \sqrt{2} \times (-1) \equiv 3 \pmod{7},$$

$$2^{(7+1)/4} G_{36, \rho_2} / \sqrt{2} \times (-1) \equiv 5 \pmod{7}.$$

This gives a numerical example of Theorem 10.

§ 3. The septic case

Let a, b, c, d, e be square free integers such that $a \neq 1$ and $a, b, c, d, e, 6$ are prime to each other. Let $m = ab^2c^3d^4e^5$. For m , put $L = \mathbf{Q}(\sqrt[6]{m})$, $F = \mathbf{Q}(\sqrt[3]{m})$, $N = \mathbf{Q}(\sqrt{m})$, $K = \mathbf{Q}(\omega)$ ($\omega = e^{2\pi i/3}$), $M = K \cdot L$. Let ρ be the character of $\text{Gal}(M/K)$ corresponding to the septic residue symbol $\left(\frac{m}{\cdot}\right)_6$ through the Artin map. Then we have

$$L(s, \rho, M/K) = \zeta_L(s)\zeta_Q(s)/\zeta_N(s)\zeta_F(s)$$

and consequently we have

$$L'(0, \rho, M/K) = (h_L/h_N h_F)(R_L/R_N R_F).$$

It is easy to see that $h_L/h_N h_F$ is an integer.

Let $\varepsilon_N, \varepsilon_F$ be the fundamental units of N, F respectively, and η_1 a generator of $\text{Ker}[N_{L/N}: E_L \rightarrow E_N] \cap \text{Ker}[N_{L/F}: E_L \rightarrow E_F]$. We may assume $\eta_1 > 1$. Then $E_0 = \langle \pm 1, \varepsilon_N, \varepsilon_F, \eta_1 \rangle$ is of finite index in E_L and the index divides 6. A simple calculation shows

$$R_L/R_N R_F = (6/[E_L: E_0]) \log \eta_1,$$

so we have

$$(3.1) \quad L'(0, \rho, M/K) = (h_L/h_N h_F)(6/[E_L: E_0]) \log \eta_1.$$

We will express $L'(0, \rho, M/K)$ by elliptic units as in the quartic case. In this case, we use the elliptic curve $y^2 = 4x^3 - 1$, instead of $y^2 = 4x^3 - 4x$, and we use the same notations for the corresponding object. For example, E is the elliptic curve $y^2 = 4x^3 - 1$, \mathcal{L} the associated lattice, $\phi_f(C)$ the Ramachandra invariant with C a ideal class modulo (f) .

Let (f) be the conductor of ρ , and let $\gamma_{-1}, \gamma_\omega, \gamma_{-\omega}$ be elements of \mathfrak{O}_K prime to 6 which satisfy $\rho(C_{\gamma_{-1}}) = -1, \rho(C_{\gamma_\omega}) = \omega, \rho(C_{\gamma_{-\omega}}) = -\omega$. Then we have

$$(3.2) \quad L'(0, \rho, M/K) = \frac{1}{6f} \left| N_{K_f/M} \frac{\phi_f(C_{\gamma_\omega})\phi_f(C_{\gamma_{-1}})}{\phi_f(C_{\gamma_{-\omega}})\phi_f(C_1)} \right|.$$

Take a finite index set $J, \beta_j \in \mathfrak{O}_K$ and $m_j \in \mathbb{Z} (j \in J)$ which satisfy the following conditions:

$$(N\gamma_\omega - 1) + (N\gamma_{-1} - 1) - (N\gamma_{-\omega} - 1) + \sum_j m(N\beta_j - 1) = 0,$$

$$\rho(C_{\beta_j}) = 1, \quad (\beta_j, 6f) = 1.$$

Let $\tau = \Omega/f (\Omega \in \mathbb{R}_+, \Omega\mathfrak{O}_K = \mathcal{L})$ and define η by

$$\eta = \phi(\tau, \gamma_\omega)\phi(\tau, \gamma_{-1})\phi(\tau, \gamma_{-\omega})^{-1} \prod_j \phi(\tau, \beta_j)^{m_j}.$$

Then η is a unit in K_f and satisfies

$$N_{K_f/M}(\eta)^f = N_{K_f/M} \frac{\phi_f(C_{\gamma_\omega})\phi_f(C_{\gamma_{-1}})}{\phi_f(C_{\gamma_{-\omega}})\phi_f(C_1)}.$$

Combining this with (3.1) and (3.2), we obtain

$$(3.3) \quad N_{K_f/M}(\eta\tilde{\eta}) = \eta_1^{36(h_L/h_{N^h E})/([E_L:E_0])}.$$

Take a prime factor π of a in K . We assume that $\pi = \psi((\pi))$, where ψ is the grössencharacter associated to E . We consider $K(E_j), K(E_{j^2}), K(E_x), K$ to be subfields of C_p so that π is contained in the valuation ideal, and denote the completions of those fields by $K_\mathfrak{a}, K_\mathfrak{a}, K_\mathfrak{p}, K_\mathfrak{v}$ respectively. We also define $\mathfrak{O}, \mathfrak{O}_\mathfrak{a}, \mathfrak{m}_\mathfrak{a}$ and so on as in the quartic case. Take the prime element A of $K_\mathfrak{p}$ such that

$$A^{N\pi-1} = -\pi, \quad A \equiv \frac{-2\mathcal{P}(\tau_1)}{\mathcal{P}'(\tau_1)} \pmod{\mathfrak{m}_\mathfrak{p}^2},$$

and define ϕ_k as $\phi_k = \phi_{k,A}: K_\mathfrak{a}^\times \rightarrow \mathfrak{O}_\mathfrak{a}/\mathfrak{m}_\mathfrak{a}$. Here τ_1 is a π -division point of \mathcal{L} defined from τ as in Section 1. Calculating Kummer's logarithmic derivatives of each sides of (3.3), we obtain the next theorem.

THEOREM 12. *Let $k_0 = (N\pi - 1)/6$ and \mathfrak{Q}' be the prime ideal of $K' = K(E_f, \zeta_{N\pi-1}, (-\pi)^{1/(N\pi-1)})$ lying above \mathfrak{Q} . Embed K' into $K_{\mathfrak{Q}}$ so that $\mathfrak{Q}' \subset \mathfrak{m}_{\mathfrak{Q}}$, and consider λ as an element of K' . Let $\eta_1 = s + t \sqrt[3]{m} + u \sqrt[3]{m} + v \sqrt{m} + w \sqrt[3]{m^2} + x \sqrt[3]{m^5}$ with $s, t, u, v, w, x \in \mathbf{Q}$. Then we have;*

- i) $(h_L/h_N h_F)(6/[E_L : E_0])t \equiv G_{k_0, \rho_2}/\xi \pmod{\mathfrak{Q}'},$
- ii) $(h_L/h_N h_F)(6/[E_L : E_0])(5x - tw) \equiv G_{5k_0, \rho_2^{-1}}/\xi^5 \pmod{\mathfrak{Q}'},$

where ξ is the septic root of $-m/\pi$ defined by the equation $\sqrt[7]{m} = \xi A^{k_0}$, ρ_2 the f/π -part of ρ , and $G_{k, \chi} = G_{k, \chi, \tau_2}$ ($\chi = \rho_2$ or ρ_2^{-1}) the generalized Hurwitz number.

§ 4. Determination of $\xi \pmod{\mathfrak{Q}'}$ in the septic case

Let $\mathcal{P}(z)$ be the Weierstrass function associated to $E: y^2 = 4x^3 - 1$. Take a rational prime number p such that $p \equiv -1 \pmod{9}$, $p \equiv 1 \pmod{4}$, and consider the case when $m = p$ and $\pi = p$. Then we have

$$\prod'_{\alpha \pmod{\pi}} \mathcal{P}((\alpha/\pi)\Omega) = \pi^{-2},$$

and

$$\prod'_{\alpha \pmod{\pi}} \mathcal{P}'((\alpha/\pi)\Omega) = -27^{(N\pi-1)/4} \pi^{-3}.$$

Let $S (\subset (\mathfrak{D}_K/\pi)^\times)$ be a sixth-set, and define $G(S), \alpha(S)$ by the following equation:

$$G(S) = \prod_{\alpha \in S} (-2\mathcal{P}((\alpha/\pi)\Omega)/\mathcal{P}'((\alpha/\pi)\Omega)),$$

$$\alpha(S) = \prod_{\alpha \in S} \alpha.$$

Then it holds $G(S)^6 = p (16/27)^{(N\pi-1)/4}$. Now consider $\alpha(S)$ to be an element of K' through the canonical map $(\mathfrak{D}_K/\pi)^\times \rightarrow K_{\mathfrak{Q}}^\times$. As elements of K' , we see the next relation between λ and $G(S)$:

$$\lambda^{(N\pi-1)/6} \equiv G(S)/\alpha(S) \pmod{\mathfrak{Q}'^{(N\pi-1)/6+1}}.$$

To determine $G(S)/\alpha(S)$, we choose the sixth-set $S = S_1 \cup S_2 \cup S_+ \cup S_-$ as follows:

- $S_1 = \{z \in \mathfrak{D}_K \cap \mathbf{R}_+ \mid 0 < |z| < \pi/2\},$
- $S_2 = \{z \in \mathfrak{D}_K \cap i\mathbf{R}_+ \mid 0 < |z| < \sqrt{3}\pi/2\},$
- $S_+ = \{z \in \mathfrak{D}_K \mid 0 < \arg z < \text{“}\pi\text{”}/6, \operatorname{Re} z < \pi/2\},$
- (Here “ π ” = $3.14 \dots$ = the usual number π . We use this number only here. π in other places mean the factor of a .)
- $S_- = \bar{S}_+ \text{ (complex conjugate).}$

Observing the argument of $\mathcal{P}(z)$, $\mathcal{P}'(z)$ for each $z \in S$, we see that $G(S)$ is a negative real number if $p \equiv 1 \pmod 8$, and is a positive real number if $p \equiv 5 \pmod 8$. Thus we have

$$G(S) = p^{1/6}(16/27)^{(N\pi-1)/24} \times \varepsilon,$$

where $\varepsilon = -1$ if $p \equiv 1 \pmod 8$, and $\varepsilon = 1$ if $p \equiv 5 \pmod 8$. On the other hand, counting the number of elements of each fibre of the norm map $N: S_+ \rightarrow F_p^\times$, we see $\alpha(S) \equiv 3^{(p-1)/4} \pmod \pi$. After all we see that $\xi \equiv 1 \pmod \mathfrak{Q}'$ in this case, and the theorem can be refined into the following exact form.

THEOREM 13. *Let $L = \mathfrak{Q}(\sqrt[3]{p})$, where $p \equiv -1 \pmod 9$ and $p \equiv 1 \pmod 4$. Then we have;*

- i) $(h_L/h_N h_F)(6/[E_L : E_0])t \equiv G_{(p^2-1)/6} \pmod p,$
- ii) $(h_L/h_N h_F)(6/[E_L : E_0])(5x - tw) \equiv G_{5(p^2-1)/6} \pmod p.$

EXAMPLE 14. Let $L = \mathfrak{Q}(\sqrt[3]{17})$. In this case we have;

$$\begin{aligned} \varepsilon_N &= 4 + \sqrt{17}, \\ \varepsilon_F &= 324 + 126 \sqrt[3]{17} + 49 \sqrt[3]{17^2}, \\ \eta_1 &= 71/3 + 14 \sqrt[3]{17} + (22/3) \sqrt[3]{17} + 4\sqrt{17} + (8/3) \sqrt[3]{17^2} + 2 \sqrt[3]{17^5}, \\ h_L &= h_N = h_F = 1, \quad [E_L : E_0] = 6. \end{aligned}$$

So the left hand side of Theorem 13, i) is 14. On the other hand,

$$G_{48} = 939/10469809348083296575 \times 47 \equiv 14 \pmod{17}.$$

This gives a numerical example of Theorem 13, i).

REFERENCES

- [1] N. Ankeny, E. Artin and S. Chowla, The class number of real quadratic fields, *Ann. of Math.*, (2), **56** (1952), 479-493.
- [2] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. math.*, **39** (1977), 223-251.
- [3] H. Ito, Congruence relations of Ankeny-Artin-Chowla type for pure cubic fields, *Nagoya Math. J.*, **96** (1984), 95-112.
- [4] S. Lichtenbaum, On p -adic L -functions associated to elliptic curves, *Invent. math.*, **56** (1980), 19-55.
- [5] C. R. Matthews, Gauss sums and elliptic functions, (I) *Invent. math.*, **52** (1979), 163-185. (II) *Invent. math.*, **54** (1979), 23-52.
- [6] K. Ramachandra, Some applications of Kronecker's limit formulas, *Ann. of Math.*,

80 (1964), 104–148.

[7] G. Robert, Unités elliptiques, Bull. Soc. Math. France, Mémoire **36** (1974).

*Department of Mathematics
Faculty of Science
Kyoto University
Sakyō-ku, Kyoto 606
Japan*