H. Ito
Nagoya Math. J.
Vol. 96 (1984), 95-112

CONGRUENCE RELATIONS OF ANKENY-ARTIN-CHOWLA TYPE FOR PURE CUBIC FIELDS

HIROSHI ITO

§ 1. Introduction

Ankeny, Artin and Chowla [1] proved a congruence relation among the class number, the fundamental unit of real quadratic fields, and the Bernoulli numbers. Our aim of this paper is to prove similar congruence relations for pure cubic fields. For this purpose, we use the Hurwitz numbers associated with the elliptic curve defined by $y^2 = 4x^3 - 1$ instead of the Bernoulli numbers (§ 3). As a corollary to the main theorem (§ 5), we have the following:

For a prime number p congruent to -1 modulo 9, let h and $t + u\sqrt[3]{p} + v\sqrt[3]{p}^2 > 1$ be the class number and the fundamental unit of the pure cubic field $\boldsymbol{Q}(\sqrt[3]{p})$ respectively, where t, u and v are rational numbers. Then we have:

$$2uh \equiv G_{(p^2-1)/3} \bmod p\,,$$
$$2(2v - u^2)h \equiv G_{2(p^2-1)/3} \bmod p\,.$$

Here G_k $(k \geqq 2)$ are rational numbers defined by the power series expansion of the Weierstrass p-function satisfying $p'(z)^2 = 4p(z)^3 - 1$:

$$p(z) = \frac{1}{z^2} + \sum_{k=2}^{\infty}(k-1)G_k z^{k-2}\,.$$

Let $m > 0$ be a cube-free rational integer which has a prime divisor $p \neq 2$, 3, and $\mathfrak{p}$ a prime ideal of $K = \boldsymbol{Q}(\sqrt{-3})$ over p. In this paper, we shall prove similar congruence relations modulo $\mathfrak{p}$ for the pure cubic field $\boldsymbol{Q}(\sqrt[3]{m})$. For this purpose, we first translate, in Section 2, the analytic class number formula into the form

$$(\text{the fundamental unit})^h = (\text{the elliptic unit})\,,$$

Received October 7, 1983.

and then, following the idea of Robert [11], we take Kummer's logarithmic derivatives of both sides. In the final section, we shall give some discussion concerning the p-adic L-functions of Lichtenbaum [6].

Throughout, we denote by $\bar{\boldsymbol{Q}}$ the algebraic closure of the rational number field $\boldsymbol{Q}$, $\boldsymbol{C}$ the complex number field, and $\boldsymbol{C}_p$ the completion of the algebraic closure of the p-adic number field $\boldsymbol{Q}_p$. We fix an embedding i_∞ of $\bar{\boldsymbol{Q}}$ into $\boldsymbol{C}$ and an embedding i_p of $\bar{\boldsymbol{Q}}$ into $\boldsymbol{C}_p$ such that $i_p(\mathfrak{p})$ is contained in the valuation ideal of $\boldsymbol{C}_p$. Via these embeddings, the algebraic numbers in $\boldsymbol{C}$ will be identified with the algebraic numbers in $\boldsymbol{C}_p$. Denote by h and $\varepsilon > 1$ the class number and the fundamental unit of the pure cubic field $\boldsymbol{Q}(\delta)$ respectively. Here δ is the real cube root of m.

§ 2. The analytic class number formula

In this section, we translate the analytic class number formula for $\boldsymbol{Q}(\delta)$ into the form which is suitable for the later applications ((2), (7)). Until the end of Section 3, the discussion will take place inside $\boldsymbol{C}$. Put $H = K(\delta)$ and denote by $\mathcal{O}_K$ the ring of integers of K. Note that m is uniquely expressed as $m = ab^2$, where a and b are positive integers which are square-free and prime to each other. Then the conductor of the abelian extension H/K is given by the ideal $(f) = f\mathcal{O}_K$. Here f is the rational integer defined as follows (cf. Hasse [4] and LeVeque [5]):

$$f = \begin{cases} ab & \text{if } a^2 \equiv b^2 \bmod 9\,, \\ 3ab & \text{otherwise}\,. \end{cases} \tag{1}$$

The ray class group $\mathrm{Cl}(f)$ of K modulo (f) is naturally isomorphic to $(\mathcal{O}_K/f\mathcal{O}_K)^\times/\bar{\mu}$, where $\bar{\mu}$ is the image of the group μ of units of K in $(\mathcal{O}_K/f\mathcal{O}_K)^\times$. By the assumption on m, f has a prime divisor $p \neq 2, 3$, so that $\bar{\mu}$ has order 6. If $\alpha \in \mathcal{O}_K$ is prime to f, we denote by C_α the element of $\mathrm{Cl}(f)$ represented by (α).

Denote by $(\alpha/\beta)_3$ the cubic residue symbol in K and put $\chi = (m/\cdot)_3$. Then the map $C_\alpha \mapsto \chi(\alpha)$ is well-defined and gives a character of $\mathrm{Cl}(f)$ corresponding to H/K. We denote this character also by χ. For the Dedekind zeta function $\zeta_{\boldsymbol{Q}(\delta)}(s)$ of $\boldsymbol{Q}(\delta)$, we see

$$\zeta_{\boldsymbol{Q}(\delta)}(s) = \zeta(s) L_K(s, \chi)$$

from Meyer [8]. It follows from the analytic class number formula that

$$h \log \varepsilon = L'_K(0, \varepsilon)\,.$$

Let H_f be the ray class field of K modulo (f). Take and fix $\gamma \in \mathcal{O}_K$ such that $(\gamma, 6f) = 1$ and $\chi(\gamma) \neq 1$. If we use the ray class invariant $\varphi_f(C)$ modulo (f) defined in Section 2 of Robert [10], we see

$$L'_K(0, \chi) = -\frac{1}{12f} \sum_{C \in \mathrm{Cl}(f)} \chi(C) \log|\varphi_f(C)|^2$$
$$= \frac{1}{12f} \log|N_{H_f/H}(\varphi_f(C_\gamma)/\varphi_f(C_1))|^2 .$$

Hence we obtain

$$(2) \qquad \varepsilon^{12fh} = |N_{H_f/H}(\varphi_f(C_\gamma)/\varphi_f(C_1))|^2 .$$

Since $\overline{N_{H_f/H}(\varphi_f(C_\gamma))} = N_{H_f/H}(\varphi_f(C_\gamma^{-1}))$, we also have

$$(3) \qquad \varepsilon^{12fh} = \prod_{C \in \mathrm{Cl}(f)} \varphi_f(C)^{-(\chi(C)+\chi(C)^{-1})} .$$

Now we consider the f-th root (> 0) of the right hand side of (2). Our technique here is borrowed from [10]. Let $p(z)$ be the Weierstrass p-function which satisfies

$$p'(z)^2 = 4p(z)^3 - 1 .$$

Denote by L the period lattice of $p(z)$. We may write $L = \mathcal{O}_K \Omega$ with Ω real and positive. For $\alpha \in \mathcal{O}_K$, denote by α' the conjugate of α and put $N\alpha = \alpha\alpha'$. Let $\sigma(z)$ be the Weierstrass σ-function of L, and put

$$\theta(z) = \Delta(L)\sigma^{12}(z) ,$$
$$\phi(z; \alpha) = \theta(\alpha z)/\theta(z)^{N\alpha} \quad (\alpha \in \mathcal{O}_K) .$$

Here $\Delta(L)$ is the discriminant of L which is equal to -27. It should be remarked that $\phi(z; \alpha)$ is an elliptic function with respect to L. More precisely, we have

$$(4) \qquad \phi(z; \alpha) = \alpha^{12}\Delta(L)^{1-N\alpha} \prod_{\substack{\alpha\beta=0 \\ \beta\neq 0}} (p(z) - p(\beta))^6 ,$$

where the product is taken over the non-zero α-division points β of C/L (Corollary 2.6 of [6]).

Because the number of roots of unity in H is equal to that of K, by Lemma 6 of [10], we can take $\beta_j \in \mathcal{O}_K$ and $m_j \in Z$ ($j \in J$) such that

$$(5) \qquad \begin{cases} N\gamma - 1 + \sum_{j \in J} m_j(N\beta_j - 1) = 0 , \\ \chi(C_{\beta_j}) = 1, \quad (\beta_j, 6f) = 1 \quad (j \in J) . \end{cases}$$

Here J is a finite index set. We fix $\{\beta_j\}_{j\in J}$ and $\{m_j\}_{j\in J}$ which satisfy (5) throughout this paper. Set $\tau = f^{-1}\Omega$, and put

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

LEMMA 1. (i) $\eta \in H_f$.

(ii) $N_{H_f/H}(\eta)^f = N_{H_f/H}(\varphi_f(C_\gamma)/\varphi_f(C_1))$.

Proof. It is seen from (4) that $\phi(z;\alpha)$ is a polynomial of $p(z)$ with coefficients in K and $\phi(\zeta z;\alpha) = \phi(z;\alpha)$ for all $\zeta \in \mu$. Therefore $\phi(\tau;\alpha)\in H_f$ for any $\alpha \in \mathcal{O}_K$, from which follows (i). To prove (ii), we note that

$$\phi(\tau;\alpha)^f = \varphi_f(C_\alpha)/\varphi_f(C_1)^{N\alpha} \tag{6}$$

if $(\alpha, f) = 1$, and that

$$N_{H_f/H}(\varphi_f(C_{\beta_j})) = N_{H_f/H}(\varphi_f(C_1))$$

for all $j\in J$ (cf. § 2 and § 10 of [6]). Then, from (5), we see

$$\begin{aligned} N_{H_f/H}(\eta)^f &= N_{H_f/H}[\varphi_f(C_\gamma)\varphi_f(C_1)^{-N\gamma+\sum_{j\in J} m_j(1-N\beta_j)}] \\ &= N_{H_f/H}(\varphi_f(C_\gamma)/\varphi_f(C_1)), \end{aligned}$$

which completes the proof.

Since $\varepsilon > 0$ and $N_{H_f/H}(\eta\bar{\eta}) = |N_{H_f/H}(\eta)|^2 > 0$, we obtain

$$\varepsilon^{12h} = N_{H_f/H}(\eta\bar{\eta}) \tag{7}$$

from (2). Note that

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

§ 3. The generalized Hurwitz numbers

We first summarize some notation and facts concerning the elliptic curve E defined by the equation

$$y^2 = 4x^3 - 1. \tag{8}$$

The map $z \mapsto \xi(z) = (p(z), p'(z))$ gives an isomorphism from $\mathbf{C}/L$ onto the complex points of E. As usual, we identify $\mathcal{O}_K$ with the endomorphism ring of E in such a way that the endomorphism corresponding to $\alpha\in\mathcal{O}_K$ is given by $\xi(z)\mapsto\xi(\alpha z)$. For $\alpha\in\mathcal{O}_K$, we denote by F_α the field obtained by adjoining to K the coordinates of α-division points of E. It is known that F_α/K is abelian and every prime ideal of K which ramifies in F_α is a divisor of 6α. For $\alpha \in \mathcal{O}_K$, $(\alpha, 6) = 1$, denote by α^* the generator of the ideal (α) such that

$$\alpha^* \equiv \left(\frac{-1}{\alpha}\right)_2 \bmod 3\,, \tag{9}$$

where $(-1/\alpha)_2$ is the quadratic residue symbol in K. Then the next lemma follows from the results of Davenport and Hasse [3].

LEMMA 2. *Let $\nu, \mu \in \mathcal{O}_K$, $(\nu, 6\mu) = 1$, and let Q_μ be a μ-division point of E. Then*

$$Q_\mu^{\sigma_\nu} = \nu^* Q_\mu\,,$$

where σ_ν is the Artin automorphism of the ideal (ν) with respect to F_μ/K.

Let π be the generator of $\mathfrak{p}$ such that $\pi^* = \pi$ and set $q = N\pi$. Define f_0, $m_0 \in \mathcal{O}_K$ by $f = \pi f_0$, $m = \pi m_0$. It is seen from (1) that $(\pi, f_0) = 1$. Hence there exist $\tau_1, \tau_2 \in C$, which are uniquely determined modulo L, such that

$$\tau \equiv \tau_1 + \tau_2, \quad \pi\tau_1 \equiv f_0\tau_2 \equiv 0 \mod L\,.$$

Here $\tau = f^{-1}\Omega$ as in Section 2. Define the points P, P_1, P_2 of E by

$$P = \xi(\tau), \quad P_i = \xi(\tau_i) \quad (i = 1, 2)\,.$$

Let $\mathfrak{n}$ be an integral ideal of K. We call a function $\lambda : \mathcal{O}_K \to \bar{\boldsymbol{Q}}$ a Dirichlet character defined modulo $\mathfrak{n}$ if there exists a character $\tilde{\lambda}$ of $(\mathcal{O}_K/\mathfrak{n})^\times$ such that $\lambda(\alpha) = \tilde{\lambda}(\alpha \bmod \mathfrak{n})$ for $(\alpha, \mathfrak{n}) = 1$, and $\lambda(\alpha) = 0$ otherwise. We can define the conductor of λ by the usual way. A Dirichlet character is called primitive if it is defined modulo its conductor. In the following, all Dirichlet characters we consider will be primitive. Write $m = ab^2$ as explained in Section 2. We can assume $p|a$ without loss of generality by replacing m by m^2/b^3 if necessary. Then a Dirichlet character χ_2 modulo (f_0) is defined by

$$\chi(\alpha) = \chi_1(\alpha)\chi_2(\alpha), \qquad \chi_1(\alpha) = \left(\frac{\alpha}{\pi}\right)_3 \tag{10}$$

for $\alpha \in \mathcal{O}_K$, $(\alpha, f) = 1$. We also view χ and χ_1 as Dirichlet characters defined modulo (f) and (π) respectively.

Denote by $\zeta(z)$ the Weierstrass ζ-function of L, i.e., $\zeta(z) = (d/dz)\log \sigma(z)$. For any $\ell \in L$ there is a constant $\kappa(\ell)$ such that

$$\zeta(z + \ell) = \zeta(z) + \kappa(\ell)\,.$$

The function $\ell \mapsto \kappa(\ell)$ is clearly linear in ℓ, and we extend it by $\boldsymbol{R}$-linearity to a function on $\boldsymbol{C}$. Let $w \in \boldsymbol{C}/L$ and take a representative $r_w \in \boldsymbol{C}$ of w. Then $\zeta(z+r_w)-\kappa(r_w)$ does not depend on the choice of r_w. We put $\zeta^*(z; w)=\zeta(z+r_w)-\kappa(r_w)$ (cf. Lemma 3.1 of [6]). For $\lambda=\chi_2$ or χ_2^{-1}, we define the generalized Hurwitz numbers $G_{k,\lambda}$ ($k \geqq 0$), following [6], by

$$\sum_{\alpha \in (\mathcal{O}_K/f_0\mathcal{O}_K)^\times} \lambda(\alpha)^{-1}\zeta^*(z; \alpha\tau_2) = -\sum_{k=0}^{\infty} G_{k,\lambda} z^{k-1}. \tag{11}$$

It is easily seen that

$$G_{0,\lambda} = \begin{cases} -1 & \text{if } (f_0)=(1), \\ 0 & \text{otherwise}. \end{cases}$$

As is shown in Section 7 of [6], $G_{k,\lambda}$ ($k \geqq 1$) are numbers related to Hecke L-functions associated with K. Because $-(d/dz)\zeta(z)=\wp(z)$, we have $G_{k,\lambda}=G_k$ ($k \geqq 2$) if $(f_0)=(1)$, where G_k are the numbers defined in the introduction.

LEMMA 3. (i) *G_{k,χ_2}, $G_{k,\chi_2^{-1}} \in F_{f_0}$ ($k \geqq 0$).*
(ii) *$G_{k,\chi_2}/\sqrt[3]{m_0}$, $G_{k,\chi_2^{-1}}/\sqrt[3]{m_0}^2 \in K$ ($k \geqq 0$).*
(iii) *When $q=p^2$, we have*

$$G_{k,\chi_2}/\sqrt[3]{m_0}, \qquad G_{k,\chi_2^{-1}}/\sqrt[3]{m_0}^2 \in \boldsymbol{Q} \quad (k \geqq 0)$$

if $\sqrt[3]{m_0}$ is real.

Proof. We only consider the assertions concerning to the numbers G_{k,χ_2}, because those concerning to $G_{k,\chi_2^{-1}}$ can be proved similarly. If $(f_0)=(1)$, them $m_0=-1$, $G_{0,\chi_2}=-1$, $G_{1,\chi_2}=0$, and $G_{k,\chi_2}=G_k$ ($k \geqq 2$), from which all the assertions follow. Assume $(f_0) \neq (1)$. Because $\chi_2(-1)=1$, we have

$$\frac{1}{2}\sum_{\substack{\alpha \bmod f_0 \\ (\alpha, f_0)=1}} \chi_2(\alpha)^{-1} \frac{\wp'(z)}{\wp(z)-\wp(\alpha\tau_2)} = -\sum_{k=1}^{\infty} G_{k,\chi_2} z^{k-1} \tag{12}$$

by Lemma 3.3 of [6]. Then the assertion (i) is clear from the definition of F_{f_0}.

To prove (ii), let (ν) be an integral ideal of K prime to $6f$, and σ_ν the Artin automorphism of (ν) with respect to $F_{f_0}(\sqrt[3]{m_0})/K$. By Lemma 2,

$$-\sum_{k=1}^{\infty} G_{k,\chi_2}^{\sigma_\nu} z^{k-1} = \frac{1}{2}\sum_{\alpha} \chi_2(\alpha)^{-1} \frac{\wp'(z)}{\wp(z)-\wp(\alpha\tau_2)^{\sigma_\nu}}$$

$$= \frac{1}{2} \sum_{\alpha} \chi_2(\alpha)^{-1} \frac{p'(z)}{p(z) - p(\nu^* \alpha \tau_2)}$$

$$= \frac{1}{2} \chi_2(\nu^*) \sum_{\alpha} \chi_2(\alpha)^{-1} \frac{p'(z)}{p(z) - p(\alpha \tau_2)}$$

$$= - \chi_2(\nu^*) \sum_{k=1}^{\infty} G_{k,\chi_2} z^{k-1} .$$

Hence

$$G_{k,\chi_2}^{\sigma_\nu - 1} = \chi_2(\nu^*) = \left(\frac{m}{\nu}\right)_3 \left(\frac{\nu^*}{\pi}\right)_3^{-1} = \left(\frac{m}{\nu}\right)_3 \left(\frac{\pi}{\nu}\right)_3^{-1} = \left(\frac{m_0}{\nu}\right)_3 .$$

On the other hand,

$$\sqrt[3]{m_0}^{\sigma_\nu - 1} = \left(\frac{m_0}{\nu}\right)_3 .$$

Thus (ii) is proved.

Finally assume $q = p^2$. Then it is easily seen that G_{k,χ_2} are real. This proves (iii).

§ 4. Kummer's logarithmic derivatives

In this section, we introduce certain group homomorphisms ψ_k $(1 \leqq k \leqq q - 1)$ which are used in [11] and were referred to as Kummer's logarithmic derivatives in the introduction (See also § 3 and § 4 of Coates and Wiles [2].). Let M_0 be a finite abelian extension of K such that the prime ideal $\mathfrak{p}$ does not ramify at M_0/K, and put $M = M_0 L$, where $L = F_\pi$. Then, since L/K is an abelian extension of degree $q - 1$ where $\mathfrak{p}$ ramifies completely, the prime ideal $\mathfrak{q}$ of M_0 corresponding to the fixed embedding $i_p : \bar{\boldsymbol{Q}} \hookrightarrow \boldsymbol{C}_p$ ramifies completely at M/M_0 and $[M : M_0] = q - 1$. Denote by $\mathfrak{Q}$ the prime ideal of M above $\mathfrak{q}$. Let $M_{\mathfrak{Q}}$ and $M_{0,\mathfrak{q}}$ be the completions of M and M_0 at $\mathfrak{Q}$ and $\mathfrak{q}$ respectively. For any subfield N of $\boldsymbol{C}_p$, denote by $\mathcal{O}(N)$ the ring of integers of N, $\mathfrak{m}(N)$ the maximal ideal of $\mathcal{O}(N)$. Put $\mathcal{O}_{\mathfrak{Q}} = \mathcal{O}(M_{\mathfrak{Q}})$, $\mathfrak{m}_{\mathfrak{Q}} = \mathfrak{m}(M_{\mathfrak{Q}})$, $\mathcal{O}_{\mathfrak{q}} = \mathcal{O}(M_{0,\mathfrak{q}})$, and $\mathfrak{m}_{\mathfrak{q}} = \mathfrak{m}(M_{0,\mathfrak{q}})$. We remark here that, in the later sections, we shall apply the argument of this section to $M_0 = F_{f_0}$.

For any prime element Λ of $M_{\mathfrak{Q}}$ we can define group homomorphisms

$$\psi_k : M_{\mathfrak{Q}}^\times \longrightarrow \mathcal{O}_{\mathfrak{q}}/\mathfrak{m}_{\mathfrak{q}} \quad (1 \leqq k \leqq q - 1)$$

as follows. First, suppose u is a unit of $M_{\mathfrak{Q}}$ congruent to 1 modulo $\mathfrak{m}_{\mathfrak{Q}}$. Choose a power series $f(T) = 1 + \sum_{k=1}^{\infty} a_k T^k$, with coefficients in $\mathcal{O}_{\mathfrak{q}}$, such that $u = f(\Lambda)$. For $1 \leqq k \leqq q-1$, we define $\psi_k(u)$ to be the residue class in $\mathcal{O}_q/\mathfrak{m}_q$ of the coefficient of T^k in $T(d/dT)\log f(T)$. Since $M_\mathfrak{Q}/M_{0,q}$ is completely ramified, $\psi_k(u)$ is independent of the choice of $f(T)$. Because any element α of $M_\mathfrak{Q}$ is written uniquely in the form $\Lambda^n \zeta u$ ($n \in Z$, $\zeta^{N\mathfrak{Q}-1} = 1$, $u \equiv 1 \bmod \mathfrak{m}_\mathfrak{Q}$), we can extend ψ_k on $M_\mathfrak{Q}$ by defining

$$\psi_k(\Lambda) = \psi_k(\zeta) = 0 .$$

The homomorphisms ψ_k depend on the choice of the prime element Λ. We shall now make a particular choice of Λ. Let $\mathfrak{P}$ be the prime ideal of L over $\mathfrak{p}$, and let $L_\mathfrak{P}$ denote the completion of L at $\mathfrak{P}$ and $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$. Set $\mathcal{O}_\mathfrak{p} = \mathcal{O}(K_\mathfrak{p})$ and $\mathfrak{m}_\mathfrak{p} = \mathfrak{m}(K_\mathfrak{p})$. Let E be the elliptic curve defined by (8), and let $\hat{E}$ denote the formal group over $\mathcal{O}_\mathfrak{p}$ of the kernel of reduction modulo $\mathfrak{m}_\mathfrak{p}$ on E, with parameter $t = -2x/y$ (Tate [12]). By the definition of π, the endomorphism π on E reduces to the Frobenius endomorphism of E modulo $\mathfrak{p}$. Therefore $\hat{E}$ is a Lubin-Tate formal group for the uniformizing parameter π of $K_\mathfrak{p}$ (Lubin and Tate [7]), and is isomorphic over $\mathcal{O}_\mathfrak{p}$ to the formal group $\mathcal{E}$ defined by the endomorphism

$$[\pi]_\mathcal{E}(T) = \pi T + T^q . \tag{13}$$

Denote by w the isomorphism from $\hat{E}$ to $\mathcal{E}$ over $\mathcal{O}_\mathfrak{p}$, and put $\Lambda = w(t(P_1))$. Then $t(P_1)$ and Λ are prime elements of $L_\mathfrak{p}$. Since $M_\mathfrak{Q}/L_\mathfrak{P}$ is unramified, they are also prime elements of $M_\mathfrak{Q}$. In the following, we consider the homomorphisms ψ_k $(1 \leqq k \leqq q-1)$ with respect to this Λ. It is seen from $[\pi]_\mathcal{E}(\Lambda) = 0$ that

$$\Lambda^{q-1} = -\pi . \tag{14}$$

Although Λ depends on the choice of the embedding i_p, $\Lambda^{(q-1)/3}$ gives a cube root of $-\pi$ which is independent of i_p.[1] In fact, $\Lambda^{(q-1)/3}$ is contained in L and is determined by

$$\Lambda^{(q-1)/3} \equiv t(P_1)^{(q-1)/3} \bmod \mathfrak{P}^{(q-1)/3+1} .$$

From this congruence, it is also seen that $\Lambda^{(q-1)/3}$ is the real cube root of $-\pi = p$ in case $q = p^2$.

The homomorphisms ψ_k have the following property which will be

1) Concerning this point, the author is indebted to Masato Kamei for pointing out an error in the original manuscript.

used later. If we identify $\mathrm{Gal}(M_{\mathfrak{Q}}/M_{0,\mathfrak{q}})$ with $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, and with $\mathrm{Gal}(L/K)$ naturally, we obtain the isomorphism

$$(15) \qquad (\mathcal{O}_K/\mathfrak{p})^{\times} \longrightarrow \mathrm{Gal}(M_{\mathfrak{Q}}/M_{0,\mathfrak{q}})$$

by considering the actions of both groups on the group of $\mathfrak{p}$-division points of E. Denote by g_ν the element of $\mathrm{Gal}(M_{\mathfrak{Q}}/M_{0,\mathfrak{q}})$ corresponding to ν modulo $\mathfrak{p} \in (\mathcal{O}_K/\mathfrak{p})^{\times}$. The following lemma is proved by the same way as in Proposition 45 of [11].

LEMMA 4. *Let k be an integer such that $1 \leqq k \leqq q-1$. For any $\alpha \in M_{\mathfrak{Q}}$ and $\nu \in \mathcal{O}_K$, $(\nu, \pi) = 1$, we have*

$$\psi_k(\alpha^{g_\nu}) = \nu^k \psi_k(\alpha)\,.$$

§ 5. Main theorem

We define $\sqrt[3]{\pi}$ and $\sqrt[3]{m_0}$ by

$$\sqrt[3]{\pi} = -\Lambda^{(q-1)/3}, \qquad \delta = \sqrt[3]{\pi}\sqrt[3]{m_0}\,.$$

The generalized Hurwitz numbers G_{k,χ_2}, $G_{k,\chi_2^{-1}}$ and the cube root $\sqrt[3]{m_0}$ of m_0 defined above are elements of F_{f_0}. Although these numbers depend on the choice of the embedding $i_\infty : \bar{\boldsymbol{Q}} \hookrightarrow \boldsymbol{C}$, the numbers $G_{k,\chi_2}/\sqrt[3]{m_0}$ and $G_{k,\chi_2^{-1}}/\sqrt[3]{m_0^2}$ $(k \geqq 0)$ are elements of K which are independent of i_∞ and i_p. Moreover they are rational numbers in case $q = p^2$ (cf. Lemma 3).

We are now ready to state the main theorem of this paper.

THEOREM. *Let $m > 0$ be a cube-free rational integer which is divisible by a prime number $p \neq 2$, 3 and not divisible by p^2. Let $\mathfrak{p}$ be a prime ideal of $\boldsymbol{Q}(\sqrt{-3})$ over p and π its generator such that $\pi \equiv (-1/\mathfrak{p})_2 \bmod 3$. Define the Dirichlet character χ_2 of $\boldsymbol{Q}(\sqrt{-3})$ by $(m/\cdot)_3 = (\cdot/\mathfrak{p})_3\chi_2$ and let $G_{k,\lambda}$ $(\lambda = \chi_2, \chi_2^{-1})$ be the Hurwitz numbers defined in* Section 3. *Further let $\sqrt[3]{m_0}$ be the cube root of $m_0 = m/\pi$ defined as above. Then, if we denote by h and $\varepsilon = t + u\sqrt[3]{m} + v\sqrt[3]{m^2} > 1$ $(t, u, v \in \boldsymbol{Q})$ the class number and the fundamental unit of the pure cubic field $\boldsymbol{Q}(\sqrt[3]{m})$ respectively, we have:*

$$(16) \qquad \begin{aligned} -2\frac{u}{t}h &\equiv G_{(N\mathfrak{p}-1)/3,\chi_2}/\sqrt[3]{m_0} \bmod \mathfrak{p}\,, \\ 2\left(2\frac{v}{t} - \left(\frac{u}{t}\right)^2\right)h &\equiv G_{2(N\mathfrak{p}-1)/3,\chi_2^{-1}}/\sqrt[3]{m_0}^2 \bmod \mathfrak{p}\,. \end{aligned}$$

Moreover, in case p is congruent to -1 modulo 3, both sides of the above *congruences are rational numbers, and* 'mod $\mathfrak{p}$' *can be replaced by* 'mod p'. *In this case, we also have* $t \equiv 1 \bmod p$.

Remark. Suppose $m = p \equiv -1 \bmod 9$. Then we have $\pi = -p$, $m_0 = -1$, and $\sqrt[3]{m_0} = -1$. We also have $(f_0) = (1)$, hence $G_{k,\chi_2} = G_{k,\chi_2^{-1}} = G_k$ $(k \geqq 2)$. Therefore the statement in the introduction follows from the above theorem.

To prove the theorem we prepare a proposition. In the following, we set $M_0 = F_{f_0}$ and use the notation of the previous section. In particular $M = F_f$. As is noted in the proof of Lemma 1, $\phi(z; \alpha)$ $(\alpha \in \mathcal{O}_K)$ is a polynomial of $p(z)$ with coefficients in K and $\phi(\zeta z; \alpha) = \phi(z; \alpha)$ for all $\zeta \in \mu$. It follows that $\phi(\tau_1 + \mu\tau_2; \alpha) \in M$ for any α, $\mu \in \mathcal{O}_K$.

PROPOSITION. *Let* $\alpha \in \mathcal{O}_K$, $(\alpha, f) = 1$, *and let* k *be an integer such that* $1 \leqq k < q - 1$. *If* λ *coinsides with* χ_2 *or* χ_2^{-1}, *we have*

$$\sum_{\substack{\mu \bmod f_0 \\ (\mu, f_0)=1}} \lambda(\mu)^{-1}\psi_k(\phi(\tau_1 + \mu\tau_2; \alpha)) = 12(N\alpha - \alpha^k\lambda(\alpha))G_{k,\lambda} \bmod \mathfrak{m}_q .$$

Proof. Our proof is almost the same as that of Coates and Wiles [2] or Robert [11]. For simplicity, we assume $(f_0) \neq (1)$. The case $(f_0) = (1)$ is treated in [11], Proposition 46. Put $\phi(z) = \phi(z; \alpha)$. We first note that

$$\frac{d}{dz}\log \theta(z) = 12\zeta(z) .$$

For $\mu \in \mathcal{O}_K$, $(\mu, f_0) = 1$, we define the complex numbers $d_k(\mu)$ $(k \geqq 0)$ by

$$\zeta^*(z; \mu\tau_2) = \sum_{k=0}^{\infty} d_k(\mu) z^{k-1} .$$

Then, from the definition of $G_{k,\lambda}$, it is seen that

$$G_{k,\lambda} = -\sum_{\substack{\mu \bmod f_0 \\ (\mu, f_0)=1}} \lambda(\mu)^{-1} d_k(\mu) .$$

Hence

$$\sum_{\mu} \lambda(\mu)^{-1}[\alpha^k d_k(\alpha\mu) - (N\alpha) d_k(\mu)] = (N\alpha - \alpha^k\lambda(\alpha))G_{k,\lambda} . \tag{17}$$

On the other hand, since $\phi(z) = \theta(\alpha z)/\theta(z)^{N\alpha}$, we have

$$\begin{aligned} z\frac{d}{dz}\log \phi(z + \mu\tau_2) &= 12\alpha z\zeta(\alpha z + \alpha\mu\tau_2) - 12(N\alpha) z\zeta(z + \mu\tau_2) \\ &= 12\sum_{k=0}^{\infty} [\alpha^k d_k(\alpha\mu) - (N\alpha) d_k(\mu)] z^k . \end{aligned}$$

It follows from the above remark on the function $\phi(z)$ that $\alpha^k d_k(\alpha\mu) - (N\alpha)d_k(\mu)$ $(k \geqq 0)$ are elements of M_0. We shall prove that these numbers are contained in $\mathcal{O}_q$ and

$$\psi_k(\phi(\tau_1 + \mu\tau_2)) = 12[\alpha^k d_k(\alpha\mu) - (N\alpha)d_k(\mu)] \bmod \mathfrak{m}_q$$

if $1 \leqq k < q-1$. Then the proof will be completed by (17).

Fix an integer $\mu \in \mathcal{O}_K$ such that $(\mu, f_0) = 1$. The formula (4) and the addition theorem for $p(z)$ give

$$\begin{aligned} \phi(z + \mu\tau_2) &= \alpha^{12}\Delta(L)^{1-N\alpha} \prod_{\substack{\alpha\beta=0 \\ \beta\neq 0}} (p(z+\mu\tau_2) - p(\beta))^6 \\ &= \alpha^{12}\Delta(L)^{1-N\alpha} \prod_{\beta} \left[-p(z) - p(\mu\tau_2) + \frac{1}{4}\left(\frac{p'(z) - p'(\mu\tau_2)}{p(z) - p(\mu\tau_2)}\right)^2 - p(\beta)\right]^6 . \end{aligned} \tag{18}$$

Let ℓ be the isomorphism over $K_{\mathfrak{p}}$ from $\hat{E}$ to the formal additive group G_a ($G_a(X, Y) = X + Y$), and $p(\ell(T))$ and $p'(\ell(T))$ the formal power series obtained by substituting $z = \ell(T)$ in the Laurent expansions at the origin of $p(z)$ and $p'(z)$ respectively. Then there exists a power series $a(T) \in \boldsymbol{Z}[[T]]$ such that $a(T) \equiv 1$ mod degree 1 and

$$p(\ell(T)) = T^{-2}a(T), \qquad p'(\ell(T)) = -2T^{-3}a(T).$$

Moreover $x(P_1) = t(P_1)^{-2}a(t(P_1))$ and $y(P_1) = -2t(P_1)^{-3}a(t(P_1))$ in $L_{\mathfrak{P}}$ (cf. [12]). Here $x(P_1)$ and $y(P_1)$ are the x-coordinate and the y-coordinate of P_1 respectively. Let $g(T)$ be the formal power series obtained from (18) by substituting $z = \ell(T)$, i.e.,

$$\begin{aligned} g(T) = \alpha^{12}\Delta(L)^{1-N\alpha} \prod_{\beta} \Big[&- T^{-2}a(T) - p(\mu\tau_2) \\ &+ \frac{1}{4}\left(\frac{-2T^{-3}a(T) - p'(\mu\tau_2)}{T^{-2}a(T) - p(\mu\tau_2)}\right)^2 - p(\beta)\Big]^6 . \end{aligned}$$

Since $(f_0, \pi) = 1$ and $(\alpha, \pi) = 1$, we see that both $p(\mu\tau_2)$ and $p(\beta)$ are $\mathfrak{p}$-integral elements of $\bar{\boldsymbol{Q}}$. Moreover the leading degree of $g(T)$ is not negative because, by the assumption that $(f_0) \neq (1)$, $\phi(z + \mu\tau_2)$ is regular at $z = 0$. Hence $g(T) \in \mathcal{O}_q[[T]]$. Since $g(t(P_1)) = \phi(\tau_1 + \mu\tau_2)$ by (18), we have $f(\Lambda) = \phi(\tau_1 + \mu\tau_2)$ for the power series $f(T) = g(w^{-1}(T)) \in \mathcal{O}_q[[T]]$. Note that the constant term of $f(T)$ is equal to $\alpha^{12}\Delta^{1-N\alpha} \prod_{\beta} (p(\mu\tau_2) - p(\beta))^6$, which is a unit of $\mathcal{O}_q$. Then we have the expansion

$$T\frac{f'(T)}{f(T)} = \sum_{k=0}^{\infty} b_k T^k ,$$

with $b_k \in \mathcal{O}_\mathfrak{q}$. From the definition of ψ_k, it is seen that

$$\psi_k(\phi(\tau_1 + \mu\tau_2)) = b_k \bmod \mathfrak{m}_\mathfrak{q}$$

for $1 \leqq k < q - 1$. As is well-known (see, for example, Lemma 7 of [2] or Lemma 44 of [11]), we have, for the isomorphism $\ell \circ w^{-1}$ from $\mathcal{E}$ to G_a,

$$\ell \circ w^{-1}(T) \equiv T \text{ mod degree } q\,.$$

Hence

$$f(T) \equiv g(\ell^{-1}(T)) \text{ mod degree } q\,.$$

Here the right hand side is equal to the power series obtained from (18) by replacing z by T. Therefore,

$$b_k = 12[\alpha^k d_k(\alpha\mu) - (N\alpha)d_k(\mu)] \qquad \text{if } k < q\,.$$

This completes the proof.

Proof of the theorem. The congruences (16) will be obtained by applying $\psi_{(q-1)/3}$ and $\psi_{2(q-1)/3}$ to both sides of (7). We only consider the first congruence because the second one can be proved similarly. Put $k = (q-1)/3$. Let γ, $\beta_j \in \mathcal{O}_K$ and $m_j \in Z$ $(j \in J)$ be the integers fixed in Section 2. We first calculate $\psi_k(N_{H_f/H}(\phi(\tau;\gamma)))$. Set $\phi(z) = \phi(z;\gamma)$. By Lemma 2, we have

$$\phi(\tau)^{\sigma_\alpha} = \phi(\alpha^*\tau) = \phi(\alpha\tau)$$

for any $\alpha \in \mathcal{O}_K$, $(\alpha, 6f) = 1$. Here σ_a is the Artin automorphism of (α) with respect to M/K. Since $\mathrm{Cl}(f)$ is isomorphic to $(\mathcal{O}_K/f\mathcal{O}_K)^\times/\bar{\mu}$ and the number of elements of $\bar{\mu}$ is 6, we see

$$\begin{aligned} N_{H_f/H}(\phi(\tau))^{18} &= \prod_{\substack{\alpha \bmod f \\ \chi(\alpha)=1}} \phi(\alpha\tau)^3 \\ &= \prod_{\substack{\alpha \bmod f \\ (\alpha,f)=1}} \phi(\alpha\tau)^{1+\chi(\alpha)+\chi^{-1}(\alpha)} \\ &= (N_{H_f/K}(\phi(\tau)))^6 \prod_{\alpha \bmod f} \phi(\alpha\tau)^{\chi(\alpha)+\chi^{-1}(\alpha)}\,. \end{aligned}$$

Because $\psi_k(u) = 0$ for $u \in M_{0,\mathfrak{q}}$, we obtain

$$\begin{aligned} &18\psi_k(N_{H_f/H}(\phi(\tau))) \\ &\quad = \sum_{\alpha \bmod f} (\chi(\alpha) + \chi^{-1}(\alpha))\psi_k(\phi(\alpha\tau)) \\ &\quad = \sum_{\mu \bmod f_0} \sum_{\nu \bmod \pi} (\chi(\mu + \nu f_0) + \chi^{-1}(\mu + \nu f_0))\psi_k(\phi((\mu + \nu f_0)(\tau_1 + \tau_2))) \end{aligned}$$

$$= \sum_{\mu} \sum_{\nu} (\chi_1(\mu + \nu f_0)\chi_2(\mu) + \chi_1^{-1}(\mu + \nu f_0)\chi_2^{-1}(\mu))\psi_k(\phi_k((\mu + \nu f_0)\tau_1 + \mu\tau_2))$$
$$= \sum_{\mu} \sum_{\nu} (\chi_1(\nu)\chi_2(\mu) + \chi_1^{-1}(\nu)\chi_2^{-1}(\mu))\psi_k(\phi(\nu\tau_1 + \mu\tau_2)) .$$

By Lemma 4 and by the fact that $\chi_1(\nu) = (\nu/\pi)_3 \equiv \nu^k \bmod \mathfrak{p}$, we have

$$\begin{aligned}\psi_k(\phi(\nu\tau_1 + \mu\tau_2)) &= \psi_k(\phi(\tau_1 + \mu\tau_2)^{g_\nu}) \\ &= \nu^k \psi_k(\phi(\tau_1 + \mu\tau_2)) \\ &= \chi_1(\nu)\psi_k(\phi(\tau_1 + \mu\tau_2))\end{aligned}$$

if ν is prime to π. Hence, by the Proposition,

$$\begin{aligned}18\psi_k(N_{H_f/H}(\phi(\tau))) &= \sum_{\mu} \sum_{\substack{\nu \bmod \pi \\ (\nu,\pi)=1}} (\chi_1(\nu)^2\chi_2(\mu) + \chi_2^{-1}(\mu))\psi_k(\phi(\tau_1 + \mu\tau_2)) \\ &= (q-1) \sum_{\mu} \chi_2^{-1}(\mu)\psi_k(\phi(\tau_1 + \mu\tau_2)) \\ &= 12(\gamma^k\chi_2(\gamma) - N\gamma)G_{k,\chi_2} \bmod \mathfrak{m}_q \\ &= 12(\chi(\gamma) - N\gamma)G_{k,\chi_2} \bmod \mathfrak{m}_q .\end{aligned}$$

Similar formulas hold for $\phi(\tau;\gamma')$, $\phi(\tau;\beta_j)$ and $\phi(\tau;\beta_j')$ $(j \in J)$, and we get

$$\psi_k(N_{H_f/H}(\eta\bar{\eta}))$$
$$= \frac{2}{3}[\chi(\gamma) + \chi(\gamma') - 2N\gamma + \sum_{j\in J} m_j(\chi(\beta_j) + \chi(\beta_j') - 2N\beta_j)]G_{k,\chi_2} \bmod \mathfrak{m}_q .$$

Note that $\chi(\alpha') = \chi^{-1}(\alpha)$ for any $\alpha \in \mathcal{O}_K$. Then it follows from (5) that the number in the square bracket is equal to

$$-1 - 2N\gamma + 2\sum_{j\in J} m_j(1 - N\beta_j) = -3 .$$

This gives

$$\psi_k(N_{H_f/H}(\eta\bar{\eta})) = -2G_{k,\chi_2} \bmod \mathfrak{m}_q .$$

On the other hand, we have, by the definition of $\sqrt[3]{m_0}$,

$$\frac{\varepsilon}{t} = 1 - \frac{u}{t}\sqrt[3]{m_0}\,\Lambda^k + \frac{v}{t}\sqrt[3]{m_0}^2\Lambda^{2k} . \tag{19}$$

Therefore,

$$\psi_k(\varepsilon) = \psi_k\left(\frac{\varepsilon}{t}\right) = \frac{u}{3t}\sqrt[3]{m_0} \bmod \mathfrak{m}_q .$$

Hence, by (7),

$$-2\frac{u}{t}h \equiv G_{k,\chi_2}/\sqrt[3]{m_0} \bmod \mathfrak{m}_q .$$

We complete the proof of the first congruence of (16) by observing that the both sides of the above congruence are contained in K.

Finally, suppose $p \equiv -1 \bmod 3$. Then $N_{Q(\delta)/Q}(\varepsilon) = 1$ gives $t^3 \equiv 1 \bmod p$, hence $t \equiv 1 \bmod p$.

EXAMPLE. Take $m = 10$, $p = 5$. Then $h = 1$, $\varepsilon = (23 + 11\sqrt[3]{10} + 5\sqrt[3]{10^2})/3$ (Wada [13]), and

$$-2uh \equiv 1, \qquad 2(2v - u^2)h \equiv 2 \quad \bmod 5 .$$

On the other hand, we see $f = 10$, $f_0 = -2$, and

$$(\mathcal{O}_K/f_0\mathcal{O}_K)^\times = \{\bar{\zeta} \mid \zeta^3 = 1\} ,$$

where the bar denotes the residue class modulo f_0. By (10),

$$\chi_2(\zeta) = \left(\frac{\zeta}{5}\right)_3^{-1} = \zeta \qquad \text{if } \zeta^3 = 1 .$$

Furthermore, the equations $4p(\tau_2)^3 - 1 = p'(\tau_2)^2 = 0$ ($\tau_2 = \Omega/2$) give

$$p(\zeta\tau_2) = \zeta p(\tau_2) = \zeta\sqrt[3]{4}^{\,-1} \qquad \text{if } \zeta^3 = 1 .$$

Hence, we see from (12)

$$\frac{1}{2}\sum_{\zeta^3=1}\zeta^{-1}\frac{p'(z)}{p(z) - \zeta\sqrt[3]{4}^{\,-1}} = -\sum_{k=1}^{\infty} G_{k,\chi_2} z^{k-1} .$$

Similar formula holds for $G_{k,\chi_2^{-1}}$. The differentiation of $p'(z)^2 = 4p(z)^3 - 1$ gives $p''(z) = 6p(z)^2$, from which follows

$$p(z) = \frac{1}{z^2} + \frac{1}{28}z^4 + \frac{1}{10192}z^{10} + \cdots .$$

Thus we obtain

$$G_{8,\chi_2} = \frac{3^2\sqrt[3]{2}}{2^3 7}, \qquad G_{16,\chi_2^{-1}} = \frac{3^2 19\sqrt[3]{2}^{\,2}}{2^6 7^2 13} .$$

Since $\sqrt[3]{m_0} = -\sqrt[3]{2}$,

$$G_{8,\chi_2}/\sqrt[3]{m_0} = -\frac{3^2}{2^3 7} \equiv 1 \qquad \bmod 5 ,$$

$$G_{16,\chi_2^{-1}}/\sqrt[3]{m_0}^2 = \frac{3^2 19}{2^6 7^2 13} \equiv 2 \quad \mod 5\,,$$

and we see the congruence (16) hold.

Remark. Let K_4 be a real pure quartic field and K_2 the quadratic subfield of K_4. Let H_+ be the group of positive relative units of K_4/K_2, and ε_0 (> 1) the generator of H_+, i.e.,

$$H_+ = \{\varepsilon \in E | \varepsilon > 0,\ N_{K_4/K_2}(\varepsilon) = 1\} = \langle \varepsilon_0 \rangle\,.$$

Here E denotes the group of all units of K_4. Then, we can formulate a class number formula such as

$$\varepsilon_0^{h_4/h_2} = (\text{the elliptic unit})\,,$$

where h_4 and h_2 denote the class number of K_4 and that of K_2 respectively (cf. Nakamula [9] and the papers quoted there). Taking Kummer's logarithmic derivatives of both sides, we will be able to obtain congruence relations similar to (16).[2] The same procedure will apply to pure sextic fields.

§ 6. *P*-adic *L*-functions

In the special case that p splits in K, we can also derive our congruence relations (16) from the discussion concerning the p-adic L-functions associated with the elliptic curve E. Throughout this section, we assume $p \equiv 1 \mod 3$. Recall that the algebraic numbers in $\boldsymbol{C}_p$ are identified with those in $\boldsymbol{C}$ via i_∞ and i_p. We shall work mainly in $\boldsymbol{C}_p$.

Let $\mathscr{T} = (E, dx/2y, r)$ be a triple consisting of our elliptic curve E, the invariant differential $dx/2y$ on E, and an isomorphism r of formal groups from the formal multiplicative group G_m (i.e., $G_m(X, Y) = X + Y + XY$) to $\hat{E}$, with coefficients in $\mathcal{O}(K_{\mathfrak{p},nr}^{\wedge})$. Here $K_{\mathfrak{p},nr}^{\wedge}$ denotes the completion of the maximal unramified extension of $K_{\mathfrak{p}}$. The existence of r follows from Lemma 2 of [7]. Further, put $\chi = (m/\cdot)_3$ and let P be the f-division point on E fixed in Section 3. With these data, Lichtenbaum [6] associated $\boldsymbol{C}_p$-valued continuous functions $L(\mathscr{T}, \chi, P)(s)$ and $L(\mathscr{T}, \chi^{-1}, P)(s)$ on $\boldsymbol{Z}_p$. Take a positive integer N such that $\chi(N) \neq 0, 1$. Then by Theorem 8.11 of [6] any by the definition of $L(\mathscr{T}, \chi, P)$, we can write

$$L(\mathscr{T}, \chi, P)(s) = h((1+p)^s - 1)/(\chi(N)\langle N\rangle^{-s+1} - 1)$$

2) These congruence relations have been obtained by Masato Kamei.

for some $h(T) \in \mathcal{O}(C_p)[[T]]$. Here, $\langle N \rangle$ is a p-adic integer determined by

$$N = \omega(N)\langle N \rangle ,$$
$$\omega(N)^{p-1} = 1, \qquad \omega(N) \equiv N \bmod p .$$

Hence, we have

$$L(\mathcal{T}, \chi, P)(m) \equiv L(\mathcal{T}, \chi, P)(n) \mod p \tag{20}$$

for any rational integers m and n.

Now, taking the p-adic logarithms of (3), we obtain

$$12fh \log_p \varepsilon = -\frac{1}{6} \sum_{\substack{\alpha \bmod f \\ (\alpha, f)=1}} (\chi(\alpha) + \chi^{-1}(\alpha)) \log_p \varphi_f(C_\alpha) . \tag{21}$$

Define a primitive p-th root of unity ζ by $\zeta - 1 = r^{-1}(t(P_1))$, and put

$$S_\chi = \tau(\chi_1, \zeta)/p, \qquad \tau(\chi_1, \zeta) = \sum_{a=1}^{p-1} \chi_1(a)\zeta^a .$$

By Corollary 4.2 of [6], we can define a unit u_0 of $K^{\wedge}_{\mathfrak{p},nr}$ by

$$\ell^{-1}(T) = r(e^{u_0 T} - 1) . \tag{22}$$

Then, if we put $k = (p-1)/3$, it follows from Corollary 9.4 of [6] (Note that the left hand side of the formula of Corollary 9.2 and the right hand side of the formula of Corollary 9.4 should be multiplied by 1/2), the formula (20), and Theorem 8.2 of [6], that

$$\begin{aligned} \frac{1}{6f} \sum_{\substack{\alpha \bmod f \\ (\alpha, f)=1}} \chi^{-1}(\alpha) \log_p \varphi_f(C_\alpha) &= 2S_\chi^{-1} u_0^{-1} L(\mathcal{T}, \chi, P)(1) \\ &\equiv 2S_\chi^{-1} u_0^{-1} L(\mathcal{T}, \chi, P)(1-k) \\ &\equiv 6k!\, S_\chi^{-1} u_0^{-k} G_{k,\chi_2} \mod p . \end{aligned}$$

LEMMA 5. (i) $S_\chi^{-1} \equiv -\pi'(k!)^{-1} u_0^{-2k} \Lambda^k \mod p$.
(ii) $u_0^{p-1} \equiv \pi' \bmod p$.

The proof will be given later. By this lemma, we get

$$\frac{1}{6f} \sum_\alpha \chi^{-1}(\alpha) \log_p \varphi_f(C_\alpha) \equiv -6G_{k,\chi_2} \Lambda^k \mod p .$$

Similar consideration gives

$$\frac{1}{6f} \sum_\alpha \chi(\alpha) \log_p \varphi_f(C_\alpha) \equiv -3G_{2k,\chi_2^{-1}} \Lambda^{2k} \mod p .$$

On the other hand, we see, from $t^3 \equiv 1 \bmod p$ and (19),

$$\log_p \varepsilon \equiv \log_p\left(\frac{\varepsilon}{t}\right) \equiv -\frac{u}{t}\sqrt[3]{m_0}\Lambda^k + \frac{1}{2}\left(2\frac{v}{t} - \left(\frac{u}{t}\right)^2\right)\sqrt[3]{m_0^2}\Lambda^{2k} \mod p .$$

Then we obtain the congruences (16) from (21).

Proof of Lemma 5. By (22),

$$r(T) \equiv u_0^{-1}T \mod \text{degree } 2 ,$$

hence

$$\zeta - 1 \equiv u_0 t(P_1) \equiv u_0 \Lambda \mod \Lambda^2 . \tag{23}$$

On the other hand, as is well-known (e.g., see Weil [14]), we have

$$\begin{aligned} &\tau(\chi_1, \zeta) \equiv k!(\zeta - 1)^{2k} \mod \Lambda^{2k+1} , \\ &\tau(\chi_1, \zeta)^3 = -(-1)^{(p-1)/2} p\pi , \\ &\left(\frac{\pi'}{\pi}\right)_3 = 1 . \end{aligned} \tag{24}$$

It follows from (14) that

$$\tau(\chi_1, \zeta)/\Lambda^{2k} \in K_{\mathfrak{p}}(\sqrt[3]{\pi'}) = K_{\mathfrak{p}} .$$

Then, by (23) and (24),

$$\tau(\chi_1, \zeta)/\Lambda^{2k} \equiv k!\, u_0^{2k} \mod p .$$

Therefore we obtain

$$S_\chi^{-1} = -\pi'\Lambda^{3k}/\tau(\chi_1. \zeta) \equiv -\pi'(k!)^{-1}u_0^{-2k}\Lambda^k \mod p .$$

To prove (ii), observe that the isomorphism r from G_m to $\hat{E}$ satisfies

$$r([p]_{G_m}(T)) = [\pi]_{\hat{E}}(r([\pi']_{G_m}(T))) .$$

Comparing the coefficients of T^p, we obtain (ii).

ACKNOWLEDGEMENT. I would like to thank Masao Koike, Hiromichi Yanai, and Hideo Yokoi for helpful suggestions on the manuscript.

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. Davenport and H. Hasse, Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen, J. reine angew. Math., **172** (1935), 151–182.

[4] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grandlage, Math. Z., **31** (1930), 565–582.
[5] W. J. LeVeque, Topics in number theory, Vol. II, Reading, Mass., 1961.
[6] S. Lichtenbaum, On p-adic L-functions associated to elliptic curves, Invent. math., **56** (1980), 19–55.
[7] J. Lubin and J. Tate, Formal complex multiplication in local fields, Ann. of Math., **8** (1965), 380–387.
[8] C. Meyer, Die Berechnung der Klassenzahl abelscher Körper uber quadratischen Zahlkörpern, Akademie-Verlag, 1957.
[9] K. Nakamula, Class number calculation and elliptic units. I, II, III, Proc. Japan Acad., **57A** (1981), 56–59, 117–120, 363–366.
[10] G. Robert, Unités elliptiques, Bull. Soc. Math. France, Mém., **36** (1973).
[11] ——, Numbre de Hurwitz et unités elliptiques, Ann. Sci. École Norm. Sup., 4ᵉ série, **11** (1978), 297–389.
[12] J. Tate, The arithmetic on elliptic curves, Invent. math., **23** (1974), 179–206.
[13] H. Wada, A table of fundamental units of pure cubic fields, Proc. Japan Acad., **46** (1970), 1135–1140.
[14] A. Weil, La cyclotomie jadis et naguère, Sém. Bourbaki, 1973/1974, Exp. no. 452, Springer Lecture Notes in Math., Vol. **431** (1975), 318–338.

Department of Mathematics
Nagoya University
Chikusa-ku, Nagoya, 464
Japan