J. Math. Soc. Japan
Vol. 27, No. 1, 1975

On a class number relation of imaginary abelian fields

By Aichi KUDO

(Received March 5, 1974)

§ 1. Introduction.

Let k_0 be the cyclotomic field $Q(\zeta_p)$ generated by a primitive p-th root of unity ζ_p over the rationals Q, where p is a prime number >3. Let k_0^+ be the maximal real subfield of k_0. Recently, Metsänkylä [7], [8] gave a relation between the class number h_0^+ of k_0^+ and the relative class number h_0^- of k_0/k_0^+ in the form

$$h_0^- \equiv G h_0^+ \pmod{p}, \tag{1}$$

where G is an explicitly given integer.

In this paper we shall generalize this relation (1) to the class number factors h_K^- and h_K^+ of certain imaginary abelian number field K over Q (Theorems 1, 2, § 3), by means of continuity of p-adic L-functions [4], [5] and the p-adic formulas for h_K^+ [6] and h_K^-. For this purpose, we use some results connected with p-adic L-functions which are derived by Fresnel [2] and simplified by Shiratani [10].

Denote by q a square-free integer >1 and by $d=3q$ the discriminant of a real quadratic number field. Consider the real field $Q(\sqrt{3q})$ and the imaginary field $Q(\sqrt{-q})$. As an application of our Theorems 1, 2, we shall obtain a classical result ((21), § 4) of Ankeny-Artin-Chowla [1], which states a congruence relation modulo 3 between the class numbers of $Q(\sqrt{3q})$ and $Q(\sqrt{-q})$ for $q\equiv 1 \pmod 3$. Furthermore in § 4 we shall give some similar results other than (21).

§ 2. Relations between $L_p(0, \chi)$ and $L_p(1, \chi)$.

Let p be an arbitrarily fixed prime number, Q_p the field of rational p-adic numbers and Z_p the ring of rational p-adic integers. Let χ be an even Dirichlet character and $L_p(s, \chi)$ the p-adic L-function for χ. The function $L_p(s, \chi)$ is a continuous function of $s\in Z_p$ $(s\neq 1)$, and if χ is not the principal character, then $L_p(s, \chi)$ is continuous at $s=1$ [4], [5]. A Dirichlet character

χ is called a character of the second kind (with respect to p) if it is an even character whose conductor f_χ and order n_χ are both some powers of p. We may suppose that the values of Dirichlet character χ are contained in an algebraic closure Ω_p of Q_p, and we set $\chi(x)=0$ if x is not prime to the conductor f_χ.

Now let $\mathfrak{X}$ be a finite abelian group of order g of even Dirichlet characters, p^m the number of characters of the second kind in $\mathfrak{X}$, $(m\geqq 0)$, and χ^0 the principal character. Then we have the following Propositions 1, 2.

PROPOSITION 1. *For $p\neq 2$, we have the congruence of rational p-adic integers:*

$$p^{m+1}\prod_{\chi\in\mathfrak{X}} L_p(0,\chi)\equiv p^m\prod_{\chi\in\mathfrak{X}-\{\chi^0\}} L_p(1,\chi)\qquad (\mathrm{mod}\ p)\,. \tag{2}$$

PROOF. Let $\mathfrak{X}_1$ denote the cyclic group of order p^m consisting of all characters of the second kind in $\mathfrak{X}$. By the definition of p-adic L-functions [2], [**10**] and Theorems 1, 2, 3, 4, 5 of [**10**], it holds that

$$L_p(0,\chi)\equiv L_p(1,\chi)\quad (\mathrm{mod}\ p)\qquad \text{for } \chi\in\mathfrak{X},\ \chi\notin\mathfrak{X}_1\,, \tag{3}$$

$$L_p(0,\chi)\equiv L_p(1,\chi)\quad (\mathrm{mod}\ p(1-\chi(1+p))^{-2})\qquad \text{for } \chi\in\mathfrak{X}_1,\ \chi\neq\chi^0\,, \tag{4}$$

$$pL_p(0,\chi)\equiv 1\quad (\mathrm{mod}\ p)\qquad \text{for } \chi=\chi^0\,. \tag{5}$$

By Theorem 5 of [**10**], we know that $L_p(0,\chi)$, $\chi\in\mathfrak{X}$, is not an integer in $Q_p(\chi)$ only if $\chi\in\mathfrak{X}_1$, and for every $\chi\in\mathfrak{X}_1$, $\chi\neq\chi^0$, $(1-\chi(1+p))L_p(0,\chi)$ is an integer in $Q_p(\chi)$.

Since $\prod_{\chi\in\mathfrak{X}_1-\{\chi^0\}}(1-\chi(1+p))=p^m$, it follows from (4) that

$$p^m\prod_{\chi\in\mathfrak{X}_1-\{\chi^0\}} L_p(0,\chi)\equiv p^m\prod_{\chi\in\mathfrak{X}_1-\{\chi^0\}} L_p(1,\chi)\qquad (\mathrm{mod}\ p(1-\zeta_p)^{-1})\,.$$

Here ζ_p means a primitive p-th root of unity in Ω_p. This congruence holds for modulo p since both sides are rational p-adic numbers. Therefore we immediately have the congruence with which we are concerned.

PROPOSITION 2. *For $p=2$, we have the congruence of rational 2-adic integers:*

$$2^{m-g+2}\prod_{\chi\in\mathfrak{X}} L_2(0,\chi)\equiv 2^{m-g+1}\prod_{\chi\in\mathfrak{X}-\{\chi^0\}} L_2(1,\chi)\qquad (\mathrm{mod}\ 2)\,. \tag{6}$$

Furthermore, if $\mathfrak{X}$ contains no character of the second kind except for χ^0, then the congruence (6) *holds for modulo* 4.

PROOF. Let $\mathfrak{X}_1$ be the cyclic group of order 2^m consisting of all characters of the second kind in $\mathfrak{X}$ as in the proof of Proposition 1. In this case where $p=2$, we obtain [**2**], [**10**] that

$$L_2(0,\chi)\equiv L_2(1,\chi)\quad (\mathrm{mod}\ 2^3)\qquad \text{for } \chi\in\mathfrak{X},\ \chi\notin\mathfrak{X}_1\,, \tag{7}$$

$$L_2(0,\chi)\equiv L_2(1,\chi)\quad (\mathrm{mod}\ 2^3(1-\chi(5))^{-2})\qquad \text{for } \chi\in\mathfrak{X}_1,\ \chi\neq\chi^0\,, \tag{8}$$

(9) $$L_2(0, \chi) \equiv \frac{1}{2} \pmod 2 \qquad \text{for } \chi = \chi^0 ,$$

where $\frac{1}{2}L_2(0, \chi)$ for $\chi \in \mathfrak{X}$, $\chi \notin \mathfrak{X}_1$ and $\frac{1-\chi(5)}{2}L_2(0, \chi)$ for $\chi \in \mathfrak{X}_1$, $\chi \neq \chi^0$ are integers in $Q_2(\chi)$.

Since $\prod_{\chi \in \mathfrak{X}_1 - \{\chi^0\}} (1-\chi(5)) = 2^m$, it follows from (8) that

$$2^{m-2m+1} \prod_{\chi \in \mathfrak{X}_1 - \{\chi^0\}} L_2(0, \chi) \equiv 2^{m-2m+1} \prod_{\chi \in \mathfrak{X}_1 - \{\chi^0\}} L_2(1, \chi) \pmod 2 .$$

On the other hand, it follows from (7) and (9) that

$$2^{2m-g} \prod_{\chi \in \mathfrak{X} - \mathfrak{X}_1} L_2(0, \chi) \equiv 2^{2m-g} \prod_{\chi \in \mathfrak{X} - \mathfrak{X}_1} L_2(1, \chi) \pmod 4$$

and

$$2L_2(0, \chi^0) \equiv 1 \pmod 4 .$$

Therefore we obtain the desired congruence.

§ 3. Relation between h_K^- and h_K^+.

In this section we shall prove our main theorems. Let K be an imaginary abelian number field of degree $2g$ over Q and $\mathfrak{X}$ the character group of K. Then $\mathfrak{X}$ is understood as an abelian group of Dirichlet characters in ordinary way. By $\mathfrak{X}^+$, $\mathfrak{X}^-$ we denote the two cosets of even and odd characters in $\mathfrak{X}$ respectively. The class number h_K of K can be written in the form $h_K = h_K^- h_K^+$ where h_K^+ is the class number of the maximal real subfield K^+ of K, and h_K^- is the relative class number of K/K^+.

The value of h_K^+ as a p-adic integer is given by the Leopoldt's p-adic class number formula [4], [6] of real abelian number field K^+ in the form

(10) $$\frac{2^{g-1} h_K^+ R_p}{\sqrt{d}} \prod_{\chi \in \mathfrak{X}^+ - \{\chi^0\}} (1-\chi(p)p^{-1}) = \prod_{\chi \in \mathfrak{X}^+ - \{\chi^0\}} L_p(1, \chi) ,$$

where R_p, d are the p-adic regulator and the discriminant of K^+ respectively.

On the other hand, p-adic value of h_K^- is given by rewriting the analytic formula [3] for the relative class number of K/K^+ p-adically (Proposition 2, [9]; (26), (27), [10]), in the form

(11) $$h_K^- \prod_{\chi \in \mathfrak{X}^-} (1-\chi(p)) = Q_K w_K 2^{-g} \prod_{\chi \in \mathfrak{X}^-} L_p(0, \chi\omega) ,$$

where Q_K is the unit-index of K/K^+, w_K the number of roots of unity in K, and ω the Dirichlet character uniquely determined by $\omega(x) = \lim_{\rho \to \infty} x^{p^\rho}$ in Q_p for all p-adic units $x \in Z_p$ when $p \neq 2$ and $\omega(x) = \pm 1$ corresponding to that $x \equiv \pm 1 \pmod 4$ when $p = 2$. This formula (11) can be regarded as the p-adic relative class number formula for K/K^+.

In the following we assume that

$$\text{(12)}\qquad \left\{\begin{array}{l} K \text{ contains a primitive } p\text{-th root of unity if } p\neq 2 \\ K \text{ contains a primitive 4-th root of unity if } p=2 \end{array}\right\}.$$

This condition is equivalent to that $\mathfrak{X}$ contains the character ω, in other words, the preceding decomposition of $\mathfrak{X}$ into two cosets is expressed as $\mathfrak{X}=\mathfrak{X}^{+}+\mathfrak{X}^{+}\omega$. On the other hand, in this situation, the number w_K of roots of unity in K can be written as $w_K=p^{m+1}w'_K$, $m\geqq 0$, $(w'_K, p)=1$ if $p\neq 2$ and $w_K=2^{m+2}w'_K$, $m\geqq 0$, $(w'_K, 2)=1$ if $p=2$. Then, $\mathfrak{X}^{+}$ is an abelian group of order g of even characters with the cyclic subgroup of order p^m which consists of all characters of the second kind in $\mathfrak{X}^{+}$.

Since

$$\text{(13)}\qquad \prod_{\chi\in\mathfrak{X}^{-}} L_p(0, \chi\omega)=\prod_{\chi\in\mathfrak{X}^{+}} L_p(0, \chi)$$

under the assumption (12), combining this fact with the formulas (10), (11) and Proposition 1, we have the following

THEOREM 1. *If K contains a primitive p-th root of unity for $p\neq 2$, and we put $w_K=p^{m+1}w'_K$, $m\geqq 0$, $(w'_K, p)=1$, then it holds that*

$$\text{(14)}\qquad \frac{2h_K^{-}}{Q_K w'_K}\prod_{\chi\in\mathfrak{X}^{-}}(1-\chi(p))\equiv\frac{p^m R_p h_K^{+}}{\sqrt{d}}\prod_{\chi\in\mathfrak{X}^{+}-\{\chi^0\}}(1-\chi(p)p^{-1}) \pmod{p},$$

where R_p and d mean the p-adic regulator and the discriminant of K^{+} respectively.

For $p=2$, combining the relation (13) with (10), (11) and Proposition 2, we also obtain the following

THEOREM 2. *If K contains a primitive 4-th root of unity, and we put $w_K=2^{m+2}w'_K$, $m\geqq 0$, $(w'_K, 2)=1$, then it holds that*

$$\text{(15)}\qquad \frac{h_K^{-}}{Q_K w'_K}\prod_{\chi\in\mathfrak{X}^{-}}(1-\chi(2))\equiv\frac{2^m R_2 h_K^{+}}{\sqrt{d}}\prod_{\chi\in\mathfrak{X}^{+}-\{\chi^0\}}(1-\chi(2)2^{-1}) \pmod{2},$$

where R_2 and d are the 2-adic regulator and the discriminant of K^{+} respectively, and in particular, if $m=0$ i.e., $w_K=4w'_K$, $(w'_K, 2)=1$, then the congruence (15) is valid for modulo 4.

REMARK. We can easily see, in the formula (14), that the quantity of the left hand side is a p-adic integer, since by the definition, Q_K, which is known to be always 1 or 2, and w'_K are p-adic units. Similarly, it follows that the left hand side in (15) is a 2-adic integer, because (15) is a congruence of 2-adic integers as we know in the proof of our Theorem 2.

Finally, we consider a special case where K is a cyclotomic field $k_0=Q(\zeta_p)$ generated by a primitive p-th root of unity ζ_p over Q, and $p>3$. Now let

R_p, d and h_0^+ denote the p-adic regulator, the discriminant and the class number of the maximal real subfield k_0^+ of k_0, and h_0^- the relative class number of k_0/k_0^+ respectively. Then, by Theorem 1 it immediately follows that

$$h_0^- \equiv \frac{R_p}{\sqrt{d}} h_0^+ \pmod{p}. \tag{16}$$

The p-adic regulator R_p for k_0^+ is the determinant of a matrix obtained by replacing the analytic logarithm of absolute values in regulator matrix of k_0^+ by the p-adic logarithm, which is defined over the multiplicative group $\Omega_p^\times$ of all invertible elements in Ω_p [4]. It is well-determined up to a factor ± 1. For the field k_0^+, we know that $\frac{R_p}{\sqrt{d}}\left(d=p^{m-1},\ m=\frac{p-1}{2}\right)$ is a p-adic integer [4], hence the formula (16) yields the result (1) of Metsänkylä [7], [8]. Let L be the closure of k_0^+ in the topological field Ω_p and Δ^2 the local discriminant of L/Q_p. A simple computation of a p-adic unit $\frac{\Delta}{\sqrt{p}^{m-1}}$ with a suitable basis for L/Q_p gives the explicit expression (mod p) of the constant factor G in (1):

$$\frac{\pm\Delta}{\sqrt{p}^{m-1}} \equiv 2^{1-m} D^{-1} \prod_{k=1}^{m-1} (-(2k)!) \pmod{p},$$

where $D=\det(r^{2(i-1)k})$ $(i, k=1, \cdots, m-1)$, r a primitive root modulo p.

§ 4. Application to quadratic fields.

In this section we shall apply Theorems 1, 2 to a relation of class numbers between real and imaginary quadratic fields.

1. Let q be a square-free integer $\neq 0, \pm 1, \pm 3$, and $K=Q(\sqrt{q}, \sqrt{-3q})$ an imaginary biquadratic field over Q containing cubic cyclotomic field $k_0=Q(\sqrt{-3})$. In $Q(\sqrt{q})$ and $Q(\sqrt{-3q})$ let k denote the real one and k' the imaginary one, and h, h' be the class numbers of k, k' respectively. Since k_0 has the class number one, we have [3]

$$h_K = \frac{1}{2} Q_K h h'. \tag{17}$$

Let ψ and ψ' be the generating characters belonging to quadratic fields k and k'. Since the imaginary biquadratic field K fulfils the condition (12) in § 3 for $p=3$, we obtain by Theorem 1

THEOREM 1′. *Let q be a square-free integer $\neq 0, \pm 1, \pm 3$. For the quadratic fields $Q(\sqrt{q})$ and $Q(\sqrt{-3q})$ we denote by h the class number of the real one and by h' the class number of the imaginary one. Then it holds that*

$$\frac{h'}{2}(1-\psi'(3)) \equiv \frac{h \log \varepsilon}{\sqrt{d}}(1-\psi(3)3^{-1}) \qquad (\mathrm{mod}\ 3)\,, \tag{18}$$

where d is the discriminant of k, the real one between $Q(\sqrt{q})$ and $Q(\sqrt{-3q})$, and $\varepsilon>1$ the fundamental unit of k.

In the above assertion, the 3-adic regulator R_3 for the real quadratic field k is normalized so that $R_3=\log \varepsilon$, $\varepsilon>1$, where "log" means the 3-adic logarithm mentioned in the end of § 3. The character factors in (18) are given as follows.

If $d\equiv 0 \pmod 3$,

$$1-\psi'(3)=\begin{cases} 2 & \text{if } \dfrac{d}{3}\equiv 1 \pmod 3\,, \\ 0 & \text{if } \dfrac{d}{3}\equiv -1 \pmod 3\,, \end{cases} \qquad 1-\psi(3)3^{-1}=1\,, \tag{19}$$

and if $d\not\equiv 0 \pmod 3$,

$$1-\psi'(3)=1, \qquad 1-\psi(3)3^{-1}=\begin{cases} \dfrac{2}{3} & \text{if } d\equiv 1 \pmod 3\,, \\ \dfrac{4}{3} & \text{if } d\equiv -1 \pmod 3\,. \end{cases} \tag{20}$$

Hence, in order to reduce the relation (18) to the form containing the coefficients of the fundamental unit ε of k, it is sufficient to approximate the 3-adic number $\log \varepsilon$ for modulo 3 (or for modulo 9).

I. The case $d\equiv 0 \pmod 3$. This corresponds to the case $k=Q(\sqrt{3q})$ and $k'=Q(\sqrt{-q})$, where q is a square-free integer >1 and $(q, 3)=1$. Let $\varepsilon=T+U\sqrt{d}>1$ $(T, U\in Q)$ be a fundamental unit of $k=Q\sqrt{3q})$. Here the rational numbers T and U are regarded as 3-adic integers in Z_3. In this case where the discriminant d contains the prime factor 3, it is easy to see that $3\nmid T$ and $N(\varepsilon)=T^2-U^2d=+1$.

If $\dfrac{d}{3}\equiv q\equiv 1 \pmod 3$, we have

$$\begin{aligned} \log \varepsilon &= \frac{1}{2}\log(T^2+2TU\sqrt{d}+U^2d) \\ &= \frac{1}{2}\log(1+2TU\sqrt{d}+2U^2d) \\ &\equiv \frac{1}{2}\left\{2TU\sqrt{d}+(2TU)^3\frac{d}{3}\sqrt{d}\right\} \qquad (\mathrm{mod}\ 3) \\ &\equiv -TU\sqrt{d} \qquad (\mathrm{mod}\ 3)\,. \end{aligned}$$

Since $T^2\equiv 1 \pmod 3$, we obtain from Theorem 1′ and (19) that

$$h'\equiv -\frac{U}{T}h \qquad (\mathrm{mod}\ 3) \tag{21}$$

to the case where $\frac{d}{3}\equiv q\equiv 1 \pmod 3$. This concludes a well-known result of Ankeny-Artin-Chowla [**1**].

II. The case $d\not\equiv 0 \pmod 3$. This corresponds to the case $k=Q(\sqrt{q})$ and $k'=Q(\sqrt{-3q})$, where q is a square-free integer >1 and $(q, 3)=1$. Let $\varepsilon=T+U\sqrt{d}>1$ be a fundamental unit of $k=Q(\sqrt{q})$. If $d\equiv q\equiv 1 \pmod 3$, it occurs that $3\nmid T$, $3\mid U$ or $3\mid T$, $3\nmid U$ corresponding to that $N(\varepsilon)=+1$ or $N(\varepsilon)=-1$. Calculating $\log\varepsilon$ for modulo 9, we obtain in the same manner as in I

$$h'\equiv\frac{1}{3}TUh \pmod 3\,. \tag{22}$$

If $d\equiv q\equiv -1 \pmod 3$ we put $\varepsilon^4=\bar{T}+\bar{U}\sqrt{d}$, where $\bar{T}$ and $\bar{U}$ are rational numbers, and $3\mid\bar{U}$. Then it follows that

$$h'\equiv -\frac{1}{3}\bar{T}\bar{U}h \pmod 3\,. \tag{23}$$

2. Let q be a square-free integer >3, and put $K=Q(\sqrt{-1}, \sqrt{q})$, $k_0=Q(\sqrt{-1})$, $k=Q(\sqrt{q})$ and $k'=Q(\sqrt{-q})$. As in **1**, we denote by h and h' the class numbers of real quadratic field k and imaginary quadratic field k' respectively. Since k_0 has the class number one, it follows [**3**] that

$$h_K=\frac{1}{2}Q_K hh'\,. \tag{24}$$

Let ψ and ψ' be the generating characters belonging to k and k'. In the following we denote by "log" the 2-adic logarithm. Since the imaginary biquadratic fields K fulfils the condition (12) in § 3 for $p=2$, and since $w_K=4$ i. e., $m=0$, $w'_K=1$ in Theorem 2, we obtain

THEOREM 2′. *Let q be a square-free integer >3, h and h' the class numbers of quadratic fields $Q(\sqrt{q})$ and $Q(\sqrt{-q})$ respectively. Then it holds that*

$$\frac{h'}{2}(1-\psi'(2))\equiv\frac{h\log\varepsilon}{\sqrt{d}}\Big(1-\frac{\psi(2)}{2}\Big) \pmod 4\,, \tag{25}$$

where d and $\varepsilon>1$ are the discriminant and a fundamental unit of $Q(\sqrt{q})$.

The character factors in (25) are given as follows.

$$1-\psi'(2)=\begin{cases}1 & \text{if } q\equiv 1 \text{ or } 2 \pmod 4,\\ 2 & \text{if } q\equiv 3 \pmod 8,\\ 0 & \text{if } q\equiv 7 \pmod 8,\end{cases}\qquad 1-\frac{\psi(2)}{2}=\begin{cases}1 & \text{if } q\equiv 2 \text{ or } 3 \pmod 4,\\ \frac{1}{2} & \text{if } q\equiv 1 \pmod 8\,,\\ \frac{3}{2} & \text{if } q\equiv 5 \pmod 8\,.\end{cases} \tag{26}$$

We notice that (25) is a congruence of rational 2-adic integers. So we can immediately conclude from (25), (26) that the class number of an imaginary quadratic field $Q(\sqrt{-q})$ is even, if q is a square-free integer >3 and $q\not\equiv -1 \pmod 4$.

Considering the 2-adic value $\log\varepsilon$ for modulo 8, we have the following various consequences.

I. The case $q\equiv 1 \pmod 8$. It is easy to see that ε can be written in the form $\varepsilon=t+u\sqrt{q}$ where t and u are rational integers and necessarily $2\nmid t$, $4|u$ or $4|t$, $2\nmid u$. As the former corresponds to that $N(\varepsilon)=+1$ and the latter corresponds to that $N(\varepsilon)=-1$, we have

$$\begin{aligned}\log\varepsilon &= \frac{1}{2}\log(t^2+2tu\sqrt{q}+u^2q)\\ &\equiv \frac{1}{2}\log(1+2tu\sqrt{q}) \qquad \pmod 8\\ &\equiv tu\sqrt{q} \qquad \pmod 8\,.\end{aligned}$$

Hence we obtain from (25), (26)

$$\frac{1}{2}h'\equiv\frac{1}{2}tuh \qquad \pmod 4\,. \tag{27}$$

In particular, $h\equiv 0 \pmod{2^\rho}$ implies $h'\equiv 0 \pmod{2^{\rho+2}}$ for $\rho=0,\ 1$.

II. The case $q\equiv 5 \pmod 8$. We put $\varepsilon^3=\bar{t}+\bar{u}\sqrt{q}$. Then $\bar{t}$ and $\bar{u}$ are rational integers and $2\nmid\bar{t}$, $4|\bar{u}$ or $2\,\|\,\bar{t}$, $2\nmid\bar{u}$, corresponding to that $N(\varepsilon)=+1$ or -1. Hence it follows that if $N(\varepsilon)=+1$,

$$\begin{aligned}\log\varepsilon &= \frac{1}{6}\log(\bar{t}^2+2\bar{t}\bar{u}\sqrt{q}+\bar{u}^2q)\\ &\equiv \frac{1}{6}\log(1+2\bar{t}\bar{u}\sqrt{q})\equiv\frac{1}{3}\bar{t}\bar{u}\sqrt{q} \qquad \pmod 8\,,\end{aligned}$$

and if $N(\varepsilon)=-1$,

$$\begin{aligned}\log\varepsilon &= \frac{1}{6}\log(\bar{t}^2+2\bar{t}\bar{u}\sqrt{q}+\bar{u}^2q)=\frac{1}{6}\log(1+2\bar{t}\bar{u}\sqrt{q}+2\bar{t}^2)\\ &\equiv \frac{1}{6}\{2\bar{t}\bar{u}\sqrt{q}+2\bar{t}^2-2(\bar{t}\bar{u}\sqrt{q}+\bar{t}^2)^2\} \qquad \pmod 8\\ &\equiv \frac{1}{3}(\bar{t}\bar{u}\sqrt{q}+\bar{t}^2-\bar{t}^2\bar{u}^2q)\equiv\frac{1}{3}\bar{t}\bar{u}\sqrt{q} \qquad \pmod 8\,.\end{aligned}$$

Therefore we obtain from (25), (26)

$$\frac{1}{2}h'\equiv\frac{1}{2}\bar{t}\bar{u}h \qquad \pmod 4\,. \tag{28}$$

In particular, if $N(\varepsilon)=+1$, $h\equiv 0 \pmod{2^\rho}$ implies $h'\equiv 0 \pmod{2^{\rho+2}}$ for $\rho=0,1$, and if $N(\varepsilon)=-1$, $h\equiv 0 \pmod{2^\rho}$ implies $h'\equiv 0 \pmod{2^{\rho+1}}$ for $\rho=0, 1, 2$.

III. The case $q\equiv 2 \pmod 4$. The number ε is written as $\varepsilon=t+u\sqrt{q}$ where

t and u are rational integers. Then t is always odd, and u is even or odd corresponding to that $N(\varepsilon)=+1$ or -1.

If $N(\varepsilon)=+1$, we obtain $\frac{1}{2}h' \equiv \frac{1}{2}tuh \pmod 4$ in the same manner as in the case I of **2**. On the other hand if $N(\varepsilon)=-1$, we put $\varepsilon^2=\bar{t}+\bar{u}\sqrt{q}$. Then $\bar{t}$ and $\bar{u}$ are rational integers and $2\|\bar{u}$. Hence

$$\begin{aligned}\log\varepsilon &= \frac{1}{4}\log(\bar{t}^2+2\bar{t}\bar{u}\sqrt{q}+\bar{u}^2q)=\frac{1}{4}\log(1+2\bar{t}\bar{u}\sqrt{q}+2\bar{u}^2q)\\ &\equiv \frac{1}{4}\{2\bar{t}\bar{u}\sqrt{q}+2\bar{u}^2q-2(\bar{t}\bar{u}\sqrt{q}+\bar{u}^2q)^2\} \qquad \pmod 8\\ &\equiv \frac{1}{2}\bar{t}\bar{u}\sqrt{q}\equiv tu(1+q)\sqrt{q} \qquad \pmod 8,\end{aligned}$$

and we have

$$\frac{\log\varepsilon}{\sqrt{d}} \equiv \frac{1}{2}tu(1+q) \qquad (\mathrm{mod}\ 4\sqrt{q}^{\,-1}).$$

Since $\frac{\log\varepsilon}{\sqrt{d}}$ is a rational 2-adic number, it follows from (25), (26) that

$$\frac{1}{2}h' \equiv \frac{1}{2}tu(1+q)h \qquad \pmod 4.$$

Now the right hand side of the above congruence is a 2-adic integer, so in this case where $q\equiv 2 \pmod 4$, $q>3$ and $N(\varepsilon)=-1$, we see that the class number h of $Q(\sqrt{q})$ must be even. Therefore we obtain

$$\frac{1}{2}h' \equiv \pm\frac{1}{2}tuh \qquad \pmod 4. \tag{29}$$

Here the factor ± 1 is corresponding to that $N(\varepsilon)=\pm 1$. In particular, if $N(\varepsilon)=+1$, $h\equiv 0 \pmod{2^\rho}$ implies $h'\equiv 0 \pmod{2^{\rho+1}}$ for $\rho=0, 1, 2$. On the other hand if $N(\varepsilon)=-1$, $2^\rho\|h$ is equivalent to $2^\rho\|h'$ for $\rho=1, 2$, and in this case, h is even as well as h'.

IV. The case $q\equiv 3 \pmod 8$. We put $\varepsilon=t+u\sqrt{q}$ with rational integers t and u. Then $2\|t$, $2\nmid u$ or $2\nmid t$, $4|u$ and in this case we know that always $N(\varepsilon)=+1$. So we have

$$\begin{aligned}\log\varepsilon &= \frac{1}{2}\log(t^2+2tu\sqrt{q}+u^2q)=\frac{1}{2}\log(1-2tu\sqrt{q}-2t^2)\\ &\equiv -\frac{1}{2}\{2tu\sqrt{q}+2t^2+2(tu\sqrt{q}+t^2)^2\} \qquad \pmod 8\\ &\equiv -tu\sqrt{q} \qquad \pmod 8\end{aligned}$$

for $2\|t$, $2\nmid u$. And for $2\nmid t$, $4|u$, we have $\log\varepsilon\equiv tu\sqrt{q}\equiv -tu\sqrt{q} \pmod 8$ too.

Hence it follows from (25), (26) that

$$h' \equiv -\frac{1}{2} tuh \qquad (\mathrm{mod}\ 4). \tag{30}$$

In particular, if $4|u$, $h \equiv 0 \pmod{2^\rho}$ implies $h' \equiv 0 \pmod{2^{\rho+1}}$ for $\rho = 0, 1$, namely we see that h' is even. On the contrary, if $2 \nmid u$, h' is even if and only if h is even.

V. The case $q \equiv 7 \pmod 8$. We put $\varepsilon = t + u\sqrt{q}$ with rational integers t and u. Then $4|t$, $2 \nmid u$ or $2 \nmid t$, $4|u$, and in this case, we know that always $N(\varepsilon) = +1$. Hence it follows that

$$\log \varepsilon = \frac{1}{2} \log (t^2 + 2tu\sqrt{q} + u^2 q)$$

$$\equiv \frac{1}{2} \log (1 \pm 2tu\sqrt{q}) \equiv tu\sqrt{q} \qquad (\mathrm{mod}\ 8).$$

Then we have from (25), (26), for the class number h of $Q(\sqrt{q})$,

$$tuh \equiv 0 \qquad (\mathrm{mod}\ 8). \tag{31}$$

References

[1] N.C. Ankeny, E. Artin and S. Chowla, The class-number of real quadratic number fields, Ann. of Math., **56** (1952), 479–493.

[2] J. Fresnel, Nombres de Bernoulli et fonctions L p-adiques, Ann. Inst. Fourier, **17** (2) (1967), 281–333.

[3] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Berlin, 1952.

[4] K. Iwasawa, Lectures on p-adic L-functions, Princeton Univ., 1972.

[5] T. Kubota and H.W. Leopoldt, Eine p-adische Theorie der Zetawerte, I, J. Reine Angew. Math., **214/215** (1964), 328–339.

[6] H.W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, J. Reine Angew. Math., **206** (1962), 54–71.

[7] T. Metsänkylä, A congruence for the class number of a cyclic field, Ann. Acad, Sci. Fenn. Ser. A I, **472** (1970), 1–11.

[8] T. Metsänkylä, A class number congruence for cyclotomic fields and their subfields, Acta Arith., **23** (1973), 107–116.

[9] K. Shiratani, A generalization of Vandiver's congruence, Mem. Fac. Sci. Kyushu Univ., **25** (1971), 144–151.

[10] K. Shiratani, Kummer's congruence for generalized Bernoulli numbers and its application, Mem. Fac. Sci. Kyushu Univ., **26** (1972), 119–138.

Aichi KUDO
Department of Mathematics
Faculty of Science
Kyushu University
Hakozaki-cho, Fukuoka
Japan