63. *On the Class Number of an Abelian Field with Prime Conductor*

By Ken-ichi YOSHINO

Department of Mathematics, Kanazawa Medical University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 13, 1993)

1. Introduction. Let p be an odd prime. Let g be a primitive root modulo p and g_i the least positive residue of g^i modulo p for every $i \geq 0$. Let $\mu = (p-1)/2$ and let $\zeta = \zeta_p = \cos(2\pi/p) + i\sin(2\pi/p)$ be a primitive pth root of unity. For every $i \geq 0$, we put

$$\varepsilon_i = \frac{\zeta^{g_{i+1}} - \zeta^{-g_{i+1}}}{\zeta^{g_i} - \zeta^{-g_i}} = \frac{\sin\dfrac{2g_{i+1}\pi}{p}}{\sin\dfrac{2g_i\pi}{p}}.$$

These are cyclotomic units of $\boldsymbol{Q}(\zeta + \zeta^{-1})$ and $\varepsilon_{\mu+i} = \varepsilon_i$ for each $i \geq 0$. Let E_0 be the group of units of $\boldsymbol{Q}(\zeta + \zeta^{-1})$ and E_C the subgroup of E_0 generated by cyclotomic units, i.e., $E_C = \langle \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{\mu-1} \rangle$. Let h_0 be the class number of $\boldsymbol{Q}(\zeta + \zeta^{-1})$. Then it is well known that $h_0 = [E_0 : E_C]$. For every $i \geq 0$, we let $c_i = 0$ or 1 according as ε_i is positive or negative.

Let L be a real subfield of $Q(\zeta)$ of degree m. We denote by E_L the group of units of L and by E_{C_L} the subgroup of E_L generated by the cyclotomic units. We let $d_i = 0$ or 1 by

$$d_i \equiv \sum_{j=0}^{\frac{\mu}{m}-1} c_{i+mj} \pmod 2$$

for every $i \geq 0$. We note that if $L = \boldsymbol{Q}(\zeta + \zeta^{-1})$, then $c_i = d_i$ for every $i \geq 0$ and that $d_{m+i} = d_i$ for every $i \geq 0$. We then define the matrix

$$M_L = (d_{i+j})_{0 \leq i,\, j \leq m-1}$$

of degree m. Let $\rho_L = m - rank_{\boldsymbol{F}_2} M_L$, where $\boldsymbol{F}_2 = \boldsymbol{Z}/2\boldsymbol{Z}$. Then it is easily shown that $\# E_{C_L}^+ / E_{C_L}^2 = 2^{\rho_L}$, where $E_{C_L}^+$ denotes the group of totally positive units in E_{C_L}.

In this note we shall give a generalization of Theorem 3 in Uchida [5]. That is, we shall prove the following

Theorem. *Let l and p be two odd primes such that $p \equiv 1 \pmod l$. Let $a \geq 1$ be the integer such that $2^a \| (p-1)/l$. Let K be the imaginary subfield of $\boldsymbol{Q}(\zeta_p)$ of degree $2^a l$, K_0 the maximal real subfield of K and L the subfield of K_0 of degree l. Let h_K^* be the relative class number of K. Let h_{K_0} and h_L be the class numbers of K_0 and L, respectively. Suppose that 2 is a primitive root modulo l. Then the following are equivalent.*

(i) $2 \mid h_K^*$, (ii) $2 \mid h_{K_0}$, (iii) $2 \mid h_L$, (iv) $\rho_L = l - 1$.

2. Lemmas. To prove our theorem, we need the following three lemmas.

Lemma 1. *Let L be a real subfield of $\boldsymbol{Q}(\zeta_p)$ of odd prime degree l. Let f be the order of 2 modulo l. Then $\rho_L \equiv 0 \pmod f$.*

Lemma 2. *Let K be an imaginary subfield of $\boldsymbol{Q}(\zeta_p)$. Then h_K^* is even if and only if $\rho_{K_0} > 0$.*

Lemma 3. *Let L be a real subfield of $\boldsymbol{Q}(\zeta_p)$. Let F be a subfield of L such that L/F is a 2-extension. Then $\rho_L = 0$ if and only if $\rho_F = 0$.*

Proof of Lemma 1. Let $\# E_{C_L}/E_{C_L}^+ = 2^b$. Then $b = l - \rho_L$, because $\# E_{C_L}^+/E_{C_L}^2 = 2^{\rho_L}$ as noted above. Let σ be a generator of the Galois group of L over $\boldsymbol{Q}$. Here we consider the homomorphism φ from E_{C_L} into the direct sum of l copies of $\{\pm 1\}$, which is defined by

$$\eta \mapsto (sign(\eta),\ sign(\eta^{\sigma}), \dots, sign(\eta^{\sigma^{l-1}})),$$

where $sign(\eta^{\sigma^i}) = |\eta^{\sigma^i}|/\eta^{\sigma^i}$ for each i. Clearly the kernel of φ is $E_{C_L}^+$. So $\# \varphi(E_{C_L}) = 2^b$. Now $G(L/\boldsymbol{Q})$ naturally acts on $\varphi(E_{C_L})$, that is, $\varphi(\eta)^{\tau} = \varphi(\eta^{\tau})$ for any $\eta \in E_{C_L}$ and $\tau \in G(L/\boldsymbol{Q})$. Therefore $(a_0, a_1, \dots, a_{l-1})^{\sigma} = (a_1, a_2, \dots, a_{l-1}, a_0)$ for any $(a_0, a_1, \dots, a_{l-1}) \in \varphi(E_{C_L})$. It easily follows that the orbit of every element of $\varphi(E_{C_L})$ except $(1, 1, \dots, 1)$ and $(-1, -1, \dots, -1)$ has l elements. Hence $2^b \equiv 2 \pmod l$. Thus we obtain $b \equiv 1 \pmod f$. Since f is a divisor of $l-1$, we have the desired congruence.

Proof of Lemma 2. We shall show that $h_K^* \equiv det\, M_{K_0} \pmod 2$. First we deal with the case $K = \boldsymbol{Q}(\zeta)$. Let θ be a primitive $(p-1)$th root of unity. It is well known that

$$h_K^* = \frac{1}{(2p)^{\mu-1}} |F(\theta)F(\theta^3)\cdots F(\theta^{p-2})|,$$

where F denotes the polynomial $F(X) = \sum_{j=0}^{p-2} g_j X^j$ (cf. [1] p.358). Since $\theta^{\mu} = -1$, we have $F(\theta^k) = \sum_{j=0}^{\mu-1} (g_j - g_{\mu+j})\theta^{kj}$ for odd k. Noting that $(1-\theta^{-k})F(\theta^k) = 2\sum_{j=0}^{\mu-1}(g_j - g_{j+1})\theta^{kj}$ for odd k and that $\Pi_{j=0}^{\mu-1}(1-\theta^{-2j-1}) = 2$, we obtain

$$p^{\mu-1} h_K^* = |G(\theta)G(\theta^3)\cdots G(\theta^{p-2})|,$$

where $G(X) = \sum_{j=0}^{\mu-1} (g_j - g_{j+1})X^j$. We set $b_j = g_j - g_{j+1}$. Then $b_{\mu+j} = -b_j$. Therefore it follows from a well known calculation that

$$G(\theta)G(\theta^3)\cdots G(\theta^{p-2}) = \pm\, det(b_{i+j})_{0 \le i,\, j \le \mu-1}.$$

On the other hand we have

$$2b_j = b_{j+s} \pm pc_j,$$

where s denotes the integer such that $g_s = 2$ (cf. Kummer [3]). So $c_j \equiv b_{j+s} \pmod 2$. Therefore we obtain $det(b_{i+j}) \equiv det(b_{i+j+s}) \equiv det(c_{i+j}) \pmod 2$. Thus we get the desired congruence in the case $K = \boldsymbol{Q}(\zeta)$.

In the case $K \neq \boldsymbol{Q}(\zeta)$, using a similar argument as above, we get the congruence.

Proof of Lemma 3. We may assume that L/F is an extension of degree 2. We define d_i' for F just as d_i were defined for L. Putting $[L:\boldsymbol{Q}] = 2n$ and $\mu = 2nt$, we have

$$d_i' \equiv \sum_{j=0}^{2t-1} c_{i+nj} \pmod 2.$$

Therefore $d_i' \equiv d_i + d_{i+n} \pmod 2$. Here we put two matrices A and B of degree n as follows:

$$A = (d_{i+j})_{0 \leq i,\, j \leq n-1}, \quad B = (d_{i+j})_{0 \leq i \leq n-1,\, n \leq j \leq 2n-1}.$$

Then

$$M_L = \begin{pmatrix} A & B \\ B & A \end{pmatrix}.$$

Hence, since $M_F \equiv A + B \pmod 2$, we obtain

$$det\, M_L \equiv \begin{vmatrix} M_F & B \\ M_F & A \end{vmatrix} \equiv \begin{vmatrix} M_F & B \\ 0 & M_F \end{vmatrix} \pmod 2.$$

On the other hand, by definition of ρ, we see that $\rho_L = 0$ (resp. $\rho_F = 0$) is equivalent to $det\, M_L \equiv 1$ (resp. $det\, M_F \equiv 1$) $\pmod 2$. Therefore Lemma 3 is proved.

3. Proof of Theorem. It is well known that (iii) implies (ii) and that (ii) implies (i). By Lemma 2 we see that if h_K^* is even, then $\rho_{K_0} > 0$, so that $\rho_L > 0$ by Lemma 3. Since 2 is a primitive root modulo l, $\rho_L = 0$ or $l - 1$ by Lemma 1. Therefore it is shown that (i) implies (iv), so that it suffices to prove that if $\rho_L = l - 1$, then h_L is even.

Suppose that $\rho_L = l - 1$ and h_L is odd. Let h_L^+ be the narrow class number of L. Then $h_L^+/h_L = [E_L^+ : E_L^2] = [E_{C_L}^+ : E_{C_L}^2] = 2^{l-1}$, where E_L^+ is the group of totally positive units of E_L. Let $\bar{L}$ be the narrow Hilbert 2-class field of L. Since $G(\bar{L}/L)$ is an elementary 2-group, $\bar{L}$ is written in the form:

$$\bar{L} = L(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_{l-1}}),$$

where each α_i is an integer of L. Since $L(\sqrt{\alpha_i})/L$ is unramified at all prime ideals of L, there exists an ideal $\mathfrak{a}_i$ such that $(\alpha_i) = \mathfrak{a}_i^2$. Therefore $2 \nmid h_L$ implies that $\mathfrak{a}_i$ is principal. So we may replace α_i by a unit of L for each i. Moreover, noting that $h_L = [E_L : E_{C_L}]$ (cf. [2]), we may assume that each α_i is a cyclotomic unit of L. We denote by E_1 the subgroup of E_{C_L} generated by $\alpha_1, \alpha_2, \ldots, \alpha_{l-1}$ and by the elements of $E_{C_L}^2$. Then $E_1/E_{C_L}^2 \cap E_{C_L}^+/E_{C_L}^2 \neq \{1\}$, because $\# E_1/E_{C_L}^2 = \# E_{C_L}^+/E_{C_L}^2 = 2^{l-1}$ and $\# E_{C_L}/E_{C_L}^2 = 2^l$. Thus we can find a cyclotomic unit α in $E_1 \cap E_{C_L}^+$ which is not contained in $E_{C_L}^2$. Obviously $L \neq L(\sqrt{\alpha}) \subseteq \bar{L}$. Since α is totally positive, $L(\sqrt{\alpha})/L$ is also unramified at all infinite prime divisors of L. This implies that h_L is even, which is a contradiction. This completes the proof.

Numerical example. Let $l = 3$. Then, among positive integers < 10000, there are 70 primes $p \equiv 1 \pmod 3$ which satisfy the condition of Theorem (cf. [4]). Next let $l = 5$. Then, among positive integers < 50000, we have the following 18 primes $p \equiv 1 \pmod 5$ which satisfy the condition of Theorem: $p = 941$, 2161, 3301, 3931, 8831, 10181, 12671, 13411, 16831, 18661, 21391, 24421, 26141, 32371, 35851, 39821, 43151, 44531.

References

[1] Z. I. Borevich and I. R. Shafarevich: Number Theory. Academic Press (1966).

[2] H. Hasse: Über die Klassenzahl abelscher Zahlkörper. Akademie-Verlag, Berlin (1952).

[3] E. E. Kummer: Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^{\lambda}=1$ gebildeten complexen Zahlen, und über den zweiten Factor der Klassenzahl. Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, pp. 855–880 (1870). Reprinted in Collected Papers, vol. I, Springer-Verlag, Berlin, pp. 919–944 (1975).
[4] M.-N. Montouchet (M.-N. Gras): Sur le nombre de classes de sous-corps cubique cyclique de $\boldsymbol{Q}^{(p)}$, $p\equiv 1 \bmod 3$. Proc. Japan Acad., **47**, 585–586 (1971).
[5] K. Uchida: On a cubic cyclic field with discriminant 163^2. J. of Number Theory, **8**, 346–349 (1976).