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 $\rho_L = m - \mathit{rank}_{\boldsymbol{F}_2} M_L$, where $\boldsymbol{F}_2 = \boldsymbol{Z}/2\boldsymbol{Z}$. Then it is easily shown that $\# E^+_{C_L}/E^2_{C_L} = 2^{\rho_L}$, 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.