CLASS NUMBER PARITY FOR CYCLOMATIC FIELDS

KEN-ICHI YOSHINO

(Communicated by David E. Rohrlich)

Abstract. We give a simple criterion for the parity of the class number of the cyclotomic field.

1. Introduction

Let $n$ be a positive integer such that $n \not\equiv 2 \pmod{4}$. Let $h_n$ be the class number of the $n$th cyclotomic field $\mathbb{Q}(\zeta_n)$. Let $h_n^-$ and $h_n^+$ be the first and second factor of the class number $h_n$ respectively. It is well known that if $n$ is divisible by at least four primes, then $h_n^-$ is even (cf. [7]) and so is $h_n$. In this paper, we shall give a simple criterion for the parity of $h_n$ when $n$ is divisible by at most three primes. Let $E_C$ be the group of cyclotomic units of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Let $E_C^\pm$ denote the group of totally positive units in $E_C$. Let $g$ be the number of distinct prime factors of $n$. Let $\rho_n$ be the non-negative integer which is defined by $\#E_C^+/E_C^2 = 2^{\rho_n}$ or $\#E_C^+/E_C^2 = 2^{\rho_n+1}$ according as $g = 1$ or $g \geq 2$. We note that $\rho_n$ is in fact non-negative in the case $g \geq 2$, since $|1-\zeta_n|^2 \in E_C^+ \setminus E_C^2$. Here we present a criterion for the parity of the class number $h_n$ of the $n$th cyclotomic field $\mathbb{Q}(\zeta_n)$.

Theorem. Let $n$ be a positive integer $\not\equiv 2 \pmod{4}$. Then

(i) $h_n$ is even in the case $g \geq 4$,
(ii) $h_n$ is even if and only if $\rho_n > 0$ in the case $g \leq 3$.

Remark 1. Since $2|h_n^+$ implies $2|h_n^-$, the parity of $h_n$ coincides with that of $h_n^-$.

2. Proof of the Theorem

Put $K_n = \mathbb{Q}(\zeta_n)$ and $K_n^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Let $E_U$ be the group of primary units in $E_C$, that is, $E_U = \{\eta \in E_C : \alpha^2 \equiv \eta \pmod{4}\}$ for some integer $\alpha \in K_n^+$ (cf. [3], §59, §61). Let $\mu_n$ denote the non-negative integer defined by $\#E_U^+/E_U^2 \cap E_U/E_U^2 = 2^{\mu_n}$.

To prove the Theorem, we need the following lemmas.

Lemma 1. $|1-\zeta_n|^2 \not\in E_U$ if $g \geq 2$.

Proof. In the case where $n$ is odd, the same argument in the proof of Lemma 2 in [11] shows that $E_U = \{\eta \in E_C : \eta^2 \equiv \eta \pmod{4}\}$, where $\tau \in G(K_n/\mathbb{Q})$ is defined by $\zeta_n^2 = \zeta_n^2$. Since $(-2 + \zeta_n + \zeta_n^{-1})^2 \equiv -2 + \zeta_n^2 + \zeta_n^{-2} \pmod{4}$, we have $-|1-\zeta_n|^2 \in E_U$. So, if $|1-\zeta_n|^2 \in E_U$, then $-1 \in E_U$, which implies that $1 \equiv -1 \pmod{4}$. This is a contradiction. Next consider the case where $n$ is even.

Received by the editors February 12, 1997.
1991 Mathematics Subject Classification. Primary 11R29, 11R18; Secondary 11R27.
Then $4 \mid n$. Put $\eta = |1 - \zeta_n|^2$. Assume that $\eta \in E_U$. Here we note that $\eta \not\in K_n^\times$. In fact, $\eta = - (\zeta_n - \zeta_n^{-1})^2 = (\zeta_n + \zeta_n^{-1})^2$, where $\zeta_n$ and $\zeta_n^{-1}$ are primitive $2n$th roots of unity. Therefore $\eta \in K_n^\times$ implies $\zeta_n \in K_n$. This is impossible. Thus we obtain the quadratic extension $K_n^+(\sqrt{\eta})/K_n^+$. The above equation shows that $K_n^+(\sqrt{\eta}) = K_n^+(\zeta_n + \zeta_n^{-1}) = K_n^+(\zeta_n + \zeta_n^{-1})$, where $a$ is the positive integer such that $2^n \parallel n$. Now $K_n^+ = K_n^+(\zeta_n + \zeta_n^{-1})$ and all the prime ideals in $K_n^+$ lying over 2 are ramified in $K_n^+/K_n^+$. On the other hand we have $\eta \equiv \alpha^2 (\text{mod } 4)$ for some integer $\alpha$ in $K_n^+$ by the assumption $\eta \in E_U$. Therefore the extension $K_n^+(\sqrt{\eta})/K_n^+$ is also generated by the roots of the equation $x^2 + x + (1 - \alpha^2 \eta^{-1})/4 = 0$, where $(1 - \alpha^2 \eta^{-1})/4$ is an integer in $K_n^+$. Thus $K_n^+(\sqrt{\eta})/K_n^+$ is unramified at 2. This is a contradiction.

\begin{lemma}
Let $a(K_n^+/K_n^+)$ be the ambiguous class number of $K_n^+/K_n^+$. Then $h_n$ is even if and only if $a(K_n^+/K_n^+)$ is even.

\begin{proof}
Let $X$ be an abelian group of order $m$. Let $f$ be an involution of $X$, that is, $f$ is an automorphism of $X$ of order 2. Let $T = \{ x \in X ; f(x) = x \}$. Then if $m$ is even, $T$ is nontrivial. Indeed, we consider the homomorphism $\phi : X \rightarrow X$ defined by $\phi(x) = x^{-1}f(x)$. Then $T = \ker \phi$. If $T$ is trivial, then $\phi$ is surjective. For any $y \in X$, there is an element $x$ which satisfies $y = x^{-1}f(x)$. Hence $yf(y) = x^{-1}f(x)f(x^{-1}f(x)) = 1$. This shows that $f(y) = y^{-1}$ for any $y \in X$. Since $m$ is even, an element of $X$ of order 2 is fixed by $f$. This contradicts the assumption $T = \{1\}$. We can also derive a contradiction from the identity $\phi^n(x) = \phi(x)^{-1}n^{-1}2\zeta_1^{-1}= (n = 1, 2, \ldots)$. Now we denote by $C_n$ the ideal class group of $K_n$. Let $j$ be the complex conjugate mapping. Then defining the involution $f$ of $C_n$ by $f(C) = C^j$ for any $C \in C_n$, we have $a(K_n^+/K_n^+) = \# \{ C \in C_n; f(C) = C \}$. Suppose that $h_n$ is even. Then using the above argument in this case, we have $a(K_n^+/K_n^+)$ is even. In fact, we denote by $A$ the 2-part of $C_n$. Then $A$ is nontrivial and $f(A) = A$. Hence $\# \{ C \in A; f(C) = C \}$ is even. Thus $a(K_n^+/K_n^+)$ is even. The converse is obvious. This completes the proof.

\begin{lemma}
Suppose that $g \leq 3$. Then $h_n^+$ is even if and only if $\mu_n > 0$.

\begin{proof}
In the case $g \leq 3$, it is well known that the class number $h_n^+$ of $K_n^+$ is represented by $h_n^+ = [E_n : E_C]$, where $E_n$ is the group of units of $K_n^+$ (cf. Sinnott [8]). The argument of the proof of Lemma 4 in [11] can be applied to show that our assertion is valid. This completes the proof.

\begin{lemma}
$\mu_n \leq \rho_n$ for every positive integer $n \not\equiv 2 (\text{mod } 4)$.

\begin{proof}
If $g = 1$, the assertion is trivial by definition of $\mu_n$ and $\rho_n$. Consider the case that $g \geq 2$. Then $\mu_n \leq \rho_n + 1$ by definition. Suppose that $\mu_n = \rho_n + 1$. Then we get $E_n^\times \cap E_U = E_n^\times$, i.e., $E_n^\times \subseteq E_U$. This means $[1 - \zeta_n]^2 \in E_U$, which contradicts Lemma 1. Thus we obtain the desired assertion.

\begin{proof}[Proof of the Theorem]
The assertion (i) is obvious from Lemma 6 of [7]. As to (ii), we showed in [11] that when $n$ is an odd prime power, $h_n^-$ is even if and only if $\rho_n > 0$. And it is well known that $h_n^+$ is odd and $\rho_2 = 0$ for any $a \geq 2$. Therefore it suffices to show that the equivalence of (ii) is valid in the case $g = 2$ or 3. Let $q^*$ be the integer defined by $\# E_n^\times / E_n^\times \cap \mathbb{Z}^* = 2q^*$, where $E_n^\times$ is the group of totally positive units in $E_n$. Then, since $E_n^\times = E_n \cap N_{K_n^+/K_n^+}(K_n^\times)$ by the norm residue theorem and the product formula, it follows from the formula for the ambiguous class number
that \( a(K_n/K_n^+) = h_n^+2^{q^*-1} \). We notice here that \( q^* \geq 1 \) in this case by Satz 12 in [2], and that \( q^*-1 \leq \rho_n \). Suppose that \( h_n \) is even. Then \( a(K_n/K_n^+) \) is even by Lemma 2. Therefore \( h_n^+ \) is even or \( 0 < q^*-1 \leq \rho_n \). Combining Lemma 3 with Lemma 4, we have \( \rho_n > 0 \). Conversely we suppose that \( \rho_n > 0 \). If \( \mu_n > 0 \), then \( h_n \) is even. This implies that \( a(K_n/K_n^+) \) is even and so is \( h_n \) by Lemma 2. If \( \mu_n = 0 \), then \( h_n \) is odd by Lemma 3. Then we have \( E_n/E_n^+ \cong E_C/E_C^+ \), i.e., \( q^*-1 = \rho_n \), so that \( a(K_n/K_n^+) \) is even. Thus \( h_n \) is even by Lemma 2. This completes the proof of the Theorem.

Remark 2. Since the generators of \( E_C \) are concretely given in [5], the values of \( \rho_n \) are calculated by using the \( \mathbb{F}_2 \)-ranks \( d \) of certain matrices as shown in [5], where \( \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} \). That is, \( \rho_n = \varphi(n)/2 - d \) or \( \rho_n = \varphi(n)/2 - d - 1 \) according as \( g = 1 \) or \( g \geq 2 \), where \( \varphi \) is the Euler function and \( d \) is the 2-rank of \( E_C/E_C^+ \).

ACKNOWLEDGMENT

The author thanks the referee for valuable comments and suggestions.

REFERENCES


Department of Mathematics, Kanazawa Medical University, Uchinada, Ishikawa 920-02, Japan
E-mail address: yoshino@kanazawa-med.ac.jp

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use