PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 9, September 1998, Pages 2589–2591
S 0002-9939(98)04712-1

CLASS NUMBER PARITY FOR CYCLOTOMIC 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 nth 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^+ denote the group of totally positive units in E_C. Let g be the number of distinct prime factors of n. Let ρ_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 ρ_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 nth 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 $2 \mid h_n^+$ implies $2 \mid h_n^-$, 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 μ_n denote the non-negative integer defined by $\#E_C^+/E_C^2 \cap E_U/E_C^2 = 2^{\mu_n}$. To prove the Theorem, we need the following lemmas.

Lemma 1. $|1-\zeta_n|^2 \notin E_U$ *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 $E_U = \{\eta \in E_C\,;\, \eta^2 \equiv \eta^\tau \pmod 4\}$, where $\tau \in G(K_n/\mathbb{Q})$ is defined by $\zeta_n^\tau = \zeta_n^2$. 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 $\eta \notin K_n^2$. In fact, $\eta = -(\zeta_{2n} - \zeta_{2n}^{-1})^2 = (\zeta_{2n}^* + \zeta_{2n}^{*-1})^2$, where ζ_{2n} and $\zeta_{2n}^* = i\zeta_{2n}$ are primitive $2n$th roots of unity. Therefore $\eta \in K_n^2$ implies $\zeta_{2n}^* \in K_n$. This is impossible. Thus we obtain the quadratic extension $K_n^+(\sqrt{\eta})/K_n^+$. The above equation shows that $K_n^+(\sqrt{\eta}) = K_n^+(\zeta_{2n}^* + \zeta_{2n}^{*-1}) = K_n^+(\zeta_{2^{a+1}} + \zeta_{2^{a+1}}^{-1})$, where a is the positive integer such that $2^a \parallel n$. Now $K_{2n}^+ = K_n^+(\zeta_{2^{a+1}} + \zeta_{2^{a+1}}^{-1})$ and all the prime ideals in K_n^+ lying over 2 are ramified in K_{2n}^+/K_n^+. On the other hand we have $\eta \equiv \alpha^2 (\mathrm{mod}\ \ 4)$ for some integer α 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. □

Lemma 2. *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.*

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 $\phi\colon X \to X$ defined by $\phi(x) = x^{-1}f(x)$. Then $T = Ker\,\phi$. If T is trivial, then ϕ 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 $\phi^n(x) = \phi(x)^{(-1)^{n-1}2^{n-1}} (n = 1, 2, \cdots)$. Now we denote by $\mathcal{C}_n$ the ideal class group of K_n. Let j be the complex conjugate mapping. Then defining the involution f of $\mathcal{C}_n$ by $f(C) = C^j$ for any $C \in \mathcal{C}_n$, we have $a(K_n/K_n^+) = \#\{C \in \mathcal{C}_n;\, f(C) = C\}$. 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 $\mathcal{A}$ the 2-part of $\mathcal{C}_n$. Then $\mathcal{A}$ is nontrivial and $f(\mathcal{A}) = \mathcal{A}$. Hence $\#\{C \in \mathcal{A};\, f(C) = C\}$ is even. Thus $a(K_n/K_n^+)$ is even. The converse is obvious. This completes the proof. □

Lemma 3. *Suppose that $g \leq 3$. Then h_n^+ is even if and only if $\mu_n > 0$.*

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. □

Lemma 4. *$\mu_n \leq \rho_n$ for every positive integer $n \not\equiv 2\,(\mathrm{mod}\ \ 4)$.*

Proof. If $g = 1$, the assertion is trivial by definition of μ_n and ρ_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 $E_C^+ \cap E_U = E_C^+$, i.e., $E_C^+ \subseteq E_U$. This means $|1-\zeta_n|^2 \in E_U$, which contradicts Lemma 1. Thus we obtain the desired assertion. □

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_{2^a} is odd and $\rho_{2^a} = 0$ 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 $\#E_n^+/E_n^2 = 2^{q^*}$, where E_n^+ is the group of totally positive units in E_n. Then, since $E_n^+ = E_n \cap N_{K_n/K_n^+}(K_n^\times)$ 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 ρ_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 φ 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

1. G. Cornell and M. I. Rosen, *The l-rank of the real class group of cyclotomic fields*, Compositio Math. **53** (1984), 133–141. MR **86d:**10090
2. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952; Springer-Verlag, 1985. MR **14:**141a; MR **87j:**11122
3. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea Pub. Co., 1948. MR **16:**571b
4. K. Horie, *On the exponents of ideal class groups of cyclotomic fields*, Proc. Amer. Math. Soc. **119** (1993), 1049–1052. MR **94a:**11166
5. K. Horie and M. Horie, *On the* 2*-class groups of cyclotomic fields whose maximal real subfields have odd class numbers*, Proc. Amer. Math. Soc. **123** (1995), 2643–2649. MR **95k:**11136
6. 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*, Monatsber. Akad. Wiss. Berlin (1870), 855–880; *Collected Papers, I*, Springer-Verlag, 1975, pp. 919–944. MR **57:**5650a
7. J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256. MR **55:**2834
8. W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. **108** (1978), 107–134. MR **58:**5585
9. P. Stevenhagen, *Class number parity for the pth cyclotomic field*, Math. Comp. **63** (1994), 773–784. MR **95a:**11099
10. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982; Second edition 1997. MR **85g:**11001; MR **97h:**11130
11. K. Yoshino, *A criterion for the parity of the class number of an abelian field with prime power conductor*, Nagoya Math. J. **145** (1997), 163–177. CMP 97:10

Department of Mathematics, Kanazawa Medical University, Uchinada, Ishikawa 920-02, Japan

E-mail address: yoshino@kanazawa-med.ac.jp