87. A Remark on the Class-number of the Maximal Real Subfield of a Cyclotomic Field

By Hiroyuki OSADA
Department of Mathematics, Rikkyo University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 13, 1989)

For an integer $m>2$, we denote by $h^+(m)$ the class-number of the field

$$K=\boldsymbol{Q}(\zeta_m+\zeta_m^{-1})$$

where ζ_m is a primitive m-th root of unity.

It is conjectured that $p\nmid h^+(p)$ for all primes p. The Theorem 2 of [2] says $h^+(p)=1$ for all $p<163$, $h^+(163)=4$ if we assume the generalized Riemann hypothesis.

In this note, we shall show that

Theorem. *Let p and $(p-1)/2=q$ be primes. If $h^+(p)<p$, then $h^+(p)=1$.*

follows easily from the following proposition (see Washington [3], Theorem 10.8).

Proposition. Let q be a prime and $K/\boldsymbol{Q}$ be a cyclic extension of degree q. Let $C(K)$ be the ideal class group of K. Let r be a prime such that $r=q$. Further let f be the order of r mod q.

If $C(K)$ has a subgroup which is isomorphic to $\boldsymbol{Z}/r^n\boldsymbol{Z}$ for some integer $n\geq 1$, then $C(K)$ has a subgroup which is isomorphic to $(\boldsymbol{Z}/r^n\boldsymbol{Z})^f$.

Proof of Theorem. We may, and shall, suppose q to be odd, as $q=2$ implies $p=5$ and $h^+(5)=1$.

Let $h^+(p)>1$, and r be a prime factor of $h^+(p)$. Then we have $r\neq q$ (see Iwasawa [1]), and the above proposition says $r^f\mid h^+(p)$, where f is the order of r mod q. If r is odd, then $r^f=2kq+1$ for some integer $k\geq 1$. Then $h^+(p)\geq 2q+1=p$ contrary to the hypothesis $h^+(p)<p$, so we should have $r=2$. Then $2^f=(2k-1)q+1$ for some integer k, but $k>1$ would be contrary as above to the hypothesis $h^+(p)<p$, so $2^f=q+1$, and f must be a prime. From $2^{f+1}-1=2q+1=p$ follows that $f+1$ is also a prime. Hence $f=2$. Therefore we get $p=7$ and $h^+(p)=1$. This completes the proof.

Remark. Professor Iwasawa has kindly communicated to me that we could prove the following lemma just as above:

Lemma. *Let $K/\boldsymbol{Q}$ be a cyclic extension of degree q, and denote the class number of K by h_K. If*

(1) *$q\geq 5$ and both q and $2q+1$ are prime,*

(2) *$(h_K, q)=1$, $h_K<2q+1$,*

then $h_K=1$.

This is a little more general result than our theorem, which follows immediately from this lemma using $h^+(5)=h^+(7)=1$. q is assumed to be ≥ 5

in this lemma, because for $q=2,3$, our statement does not hold as the following examples show:

$$q=2,\ 2q+1=5:\quad K=\boldsymbol{Q}(\sqrt{-23})\quad \text{or}\quad \boldsymbol{Q}(\sqrt{79}),\ h_K=3<5.$$
$$q=3,\ 2q+1=7:\quad K=\text{cubic subfield of } \boldsymbol{Q}(\zeta_{163}),\ h_K=4<7.$$

References

[1] K. Iwasawa: A note on class numbers of algebraic number fields. Abh. Math. Sem. Univ. Hamburg, **20**, 257–258 (1956).
[2] F. J. van der Linden: Class Number Computations of Real Abelian Number Fields. Math. Comp., vol. 39, no. 160, pp. 693–707 (1982).
[3] L. C. Washington: Introduction to cyclotomic fields. Graduate Texts in Math., **83**, Springer, Berlin, Heidelberg, New York (1982).