58. *A Remark on the Class-number of the Maximal Real Subfield of a Cyclotomic Field. III*

By Hiroyuki OSADA

Department of Mathematics, National Defence Academy

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1992)

For any number field K of finite degree, we denote by $h(K)$ the class number of K. For a prime p, ζ_p denotes a primitive p-th root of unity. In this note, we show the following:

Theorem. *Let q be an odd prime such that $p = 6q + 1$ is also a prime. We assume the following condition.*

(c) *$q + 1$ is not a power of 2, $2q + 1$ is not a power of 3, and $4q + 1$ is not a power of 5. Then*

$$h^+(p) < p \text{ and } \quad h(k(p)) > 1 \Rightarrow h^+(p) = h(k(p)),$$

where $h^+(p)$ denotes $h(Q(\zeta_p + \zeta_p^{-1}))$ and $k(p)$ is the unique cubic subfield of $Q(\zeta_p)$ over Q of a prime conductor p.

We need the following:

Proposition. *Let p and q be distinct primes. Let F be a finite algebraic number field. Suppose E/F is a Galois q-extension and f is the order of p mod q. Then, for any α with $0 \leqq \alpha < f$,*

$$p^\alpha \parallel h(E) \Rightarrow p^\alpha \parallel h(F)$$

(see [3]).

Proof. First of all, we need the following:

Lemma. *Let p and q be distinct primes. Let G be a finite group of order $p^\alpha q^\beta$. Let f be the order of $p \bmod q$. Let H be a q-Sylow subgroup of G and $\alpha < f$. Then H is a normal subgroup of G* (see [3]).

Let $P(E)$ be the maximal abelian unramified p-extention of F contained E and $G = G(P(E)/F)$. By the above lemma, the q-Sylow subgroup H of G is a normal subgroup of G. Let M be the subfield of $P(E)$ which corresponds to H. Then M/F is a Galois extention and $G(M/F) \cong G(P(E)/E)$. Therefore M/F is an abelian unramified extention of degree p^α. Therefore we have $p^\alpha \mid h(F)$. If $p^{\alpha+1} \mid h(F)$, then $p^{\alpha+1} \mid h(E)$. We conclude the above Proposition.

Corollary. *Let p, q, E, F and f be as in Proposition. Then*

$$p \nmid h(F),\ p \mid h(E) \Rightarrow p^f \mid h(E),$$

and

$$p^\alpha \parallel h(F) \Rightarrow p^\alpha \parallel h(E) \text{ or } p^f \mid h(E).$$

Proof of the theorem. Since $h^+(6\cdot 5 + 1) = h^+(31) = 1$, we may assume $q > 5$. Put $K = \mathrm{Q}(\zeta_p + \zeta_p^{-1})$ and $k = k(p)$. By the assumption on p and q, K/k is a q-extention. If $q \nmid h(k)$, then $q \nmid h(K)$ (see [1]). Since $h(k) < \dfrac{2}{3}p$ (see [2]) and $h(K) < p$, it is easy to show that if $q \mid h(k)$, then

$q \| h(k)$ and $q \| h(K)$. Now let r be an odd prime. If $r \equiv 1 (\bmod q)$, $r | h(k)$ and $r | k(K)$, then $r = 1 + 2nq$, where $n = 1$ or 2. Since $r^2 > p$, we have that $r \| h(k)$, $r \| h(K)$. If $r \equiv 1 (\bmod q)$ and $r \nmid h(k)$, $r | h(K)$, then $h(K) \geqq r \cdot h(k) \geqq 4r > p$, where $h(k) > 1 \Rightarrow h(k) \geqq 4$(see[5]). Hence we have that $r \nmid h(k) \Rightarrow r \nmid h(K)$. Now $f > 1$ is the order of r mod q. We will show that $r^f > p$.

In case $r \geqq 7$, $r^f - 1 = (r-1)(r^{f-1} + \cdots + 1)$ can not be $2nq$, where $n = 1$ or 2.

Let $r = 5$ and $5^f = 1 + 2q$. Since $5^f - 1 = 2q$, $4(5^{f+1} + \cdots + 1) = 2q$. This is a contradiction.

Let $r = 3$ and $3^f = 4q + 1$. Then f is even. Now let $f = 2m$ for some integer m. Hence $(3^m - 1)(3^m + 1) = 4q$. This is a contradiction.

Next let $r = 2$. Then $2^f = 1 + 3q$ or $2^f = 1 + 5q$. If $2^f = 1 + 3q$, then we have that $f = 2m$ for some integer m. Since $(2^m - 1)(2^m + 1) = 3q$, we should have $m = 2$, $q = 5$. Therefore we have that $2^f \neq 1 + 3q$. If $2^f = 1 + 5q$, then $f = 4m$ for some integer m. Since $2^f - 1 = (4^m - 1)(4^m + 1) = 5q$ and $3 | 4^m - 1$, we have that $2^f \neq 1 + 5q$.

Hence we have $r^f > p$. By Corollary, we have that $r \nmid h(k) \Rightarrow r \nmid h(K)$ and if $r^m \| h(k)$, for some integer m, then $r^m \| h(k)$. This completes the proof.

Examples. Suppose $p = 607$ or 1879. Suppose $h^+(p) < p$. Then $h^+(p) = h(k(p)) = 4$ (see [5]).

Remark 1. Let q and $p = 6q + 1$ be primes. Then we have only 5 example {3, 7, 13, 127, 1093,} for $q < 10^8$, which do not satisfy the condition (c) in the theorem.

Remark 2. Let p be a prime. We have no example for $h^+(p) > 1$ such that $h^+(p)$ is completely determined.

References

[1] J. Masely: Class numbers of real cyclic field with small conductors. Compositio Math., **37**, 297–319 (1978).

[2] C. Moser and J. J. Rayan: Majoration du nombre de classes d'un corps cubique cyclique de conducteur premier. J. Math. Soc. Japan, **33**, 701–706 (1981).

[3] H. Osada: A remark on the class-number of the maximal real subfield of a cyclotomic field. II. Proc. Japan Acad., **68** A, 41–42 (1992).

[4] L. C. Washington: Introduction to Cyclotomic Field. Springer (1982).

[5] M. N. Gras: Méthodes et algorithmes pour le calcul numérique du nombre de classes et umités des extentions cubiques cycliques de $\boldsymbol{Q}$. J. reine angew. Math., **277**, 89–116 (1975).