11. A Remark on the Class-Number of the Maximal Real Subfield of a Cyclotomic Field. II

By Hiroyuki OSADA
Department of Mathematics, National Defence Academy

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

For any number field K of finite degree, we denote by $h(K)$ the class number of K. ζ_q denotes a primitive q-th root of 1. In this article, we show the following.

Theorem. *Let p and $q=4p+1$ be both primes. Suppose $p+1$ is not a power of 2, and $2p+1$ is not a power of 3. Then*

$$h^+(q)<q \Rightarrow h^+(q)=h(\mathbf{Q}(\sqrt{q})),$$

where, $h^+(q)$ denotes $h(\mathbf{Q}(\zeta_q+\zeta_q^{-1}))$, namely the class number of the maximal real subfield of $\mathbf{Q}(\zeta_q)$.

To show the above theorem, we prepare some propositions.

Proposition 1. *Let p be a prime. Suppose L/k is a Galois p-extention. Assume there is at most one prime which ramifies in L/k. If $p\mid h(L)$, then $p\mid h(k)$ (see [2]).*

Proposition 2. *Let p and q be distinct primes. Let F be a finite algebraic field. Suppose E/F is a Galois q-extention and f is the order of $p \bmod q$. Then, for any α with $0\leqq\alpha<f$,*

$$p^\alpha\| h(E) \Rightarrow p^\alpha \| h(F).$$

Proof. Let $P(E)$ be the maximal abelian unramified p-extention of E. Since $p^\alpha\|h(E)$, $[P(E):E]=p^\alpha$. Since E/F is Galois, $(P(E)/F)$ is Galois because of the uniqueness of $P(E)$. Suppose $G=\mathrm{Gal}(P(E)/F)$. We can write the order of G as $p^\alpha q^\beta$ for some non-negative integer β.

To go further, we need the following:

Lemma. *Let p, 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.*

Proof of lemma. Let S be the number of q-Sylow subgroups of G. Then $s=mq+1$ for some non-negative integer m and s divides $p^\alpha q^\beta$. We can write $s=mq+1=p^t$ for $0\leqq t\leqq\alpha$. Especially, $p^t\equiv 1 \bmod q$. Since f is the order of $p \bmod q$, $t=0$ holds. Therefore, $s=1$.

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 Proposition 2 holds.

Corollary. *Let p, q, E, F and f be as in Proposition 2. Then*

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

and

$$p^{\alpha}\| h(F) \Rightarrow p^{\alpha}\| h(E) \quad or \quad p^{j} \mid h(E).$$

Proof of the theorem. Put $K=\boldsymbol{Q}(\zeta_q+\zeta_q^{-1})$ and $k=\boldsymbol{Q}(\sqrt{q})$. By the assumption on q and p, K/k is a p-extention.

Since $h(k)<\sqrt{q}=\sqrt{4p+1}$ (see [3]), we have $h(k)<p$. Therefore, $p\nmid h(k)$. By Proposition 1, $p\nmid h(K)$. Now let r be any prime $\neq p$. We shall show that $r\nmid h(k)\Rightarrow r\nmid h(K)$. In fact, $r\nmid h(k)$ and $r\mid h(K)$ would imply $r^f\mid h(K)$ by Corollary of Proposition 2, where f is the order of $r \pmod p$. Thus $r^f \leqq h(K)<q$, which is in contradiction to our assumptions on p, q shown as follows.

In fact, $r^f\equiv 1 \pmod p$ implies $r^f-1=mp$ for some $m\geqq 1$, and $m\geqq 4$ means $r^f\geqq 4p+1=q$ in contradiction to $r^f<q$.

In case $r\geqq 5$, $r^f-1=(r-1)(r^{f-1}+\cdots+1)$ can not be $=2p$ because $r-1$ is an even number $\geqq 4$, and $r^{f-1}+\cdots+1\geqq 2$. Thus $r^f-1\geqq 4p$, i.e. $m\geqq 4$.

In case $r=2$, 3, our assumptions on $p+1$ and $2p+1$ enable us also to show $m\geqq 4$.

First let $r=2$. We have $2^f\equiv 1 \pmod 3$. It follows $f=2l$ for some l. Since $2^f-1=(2^l-1)(2^l+1)=3p$, we should have $l=2$. But $4p+1=21$ is not a prime, so $m=3$ is impossible. The case $r=3$ is clear.

In view of the well-known fact $h(k)\mid h(K)$ (see [4]), we see thus that the conclusion of our Theorem holds.

Examples. Suppose $q=1229$ or 4493. Suppose $h^+(q)<q$. Then $h^+(q)=3$.

Remark 1. Suppose p, $q=4p+1$ are prime. Then we have only 5 examples {3, 7, 13, 127, 1093} for $p<10^8$, which satisfy the condition that $p+1=2^f$ or $2p+1=3^f$.

Remark 2. Let q be a prime. We know no example for $h^+(q)>1$ such that $h^+(q)$ is completely determined. We have only one example $h^+(163)=4$ (see [1]) under the generalized Rimannian hypothesis by van der Linden.

References

[1] F. van der. Linden: Class numbers computations of real abelian number fields. Math Comp., **39**, 693–707 (1982).

[2] J. Masley: Class numbers of real cyclic number fields with small conductors. Compositio Math., **37**, 297–319 (1978).

[3] W. Narkiewicz: Elementary and Analytic Theory of Algebraic Numbers. Polish Scientific Publishers (1973).

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