20. *On the Class-number of the Maximal Real Subfield of a Cyclotomic Field*

By Hiroyuki OSADA

Department of Mathematics, National Defense Academy
(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1993)

Let p be a prime. $h^+(p)$ will denote as usual the class-number of the maximal real subfield $\boldsymbol{Q}(\zeta_p + \zeta_p^{-1})$ of the cyclotomic field $\boldsymbol{Q}(\zeta_p)$, $\zeta_p = e^{\frac{2\pi i}{p}}$. Under the generalized Riemann Hypothesis $h^+(163)$ can be proved to be 4, but all values of $h^+(p)$ hitherto determined are 1 (see [4]). In a series of papers [3], we have obtained some results on $h^+(p)$ under the assumption:
(H) $\quad h^+(p) < p.$
In particular, we have shown under (H) that
$$h^+(1229) = h^+(4493) = 3$$
and
$$h^+(607) = h^+(1894) = 4,$$
so that, in any case, $h^+(p) > 1$ for $p = 1229, 4493, 607$ or 1879. We recall furthermore that the results of [3] were derived from the following proposition:

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 $0 \leq \alpha < f$,*
$$p^\alpha \parallel h(E) \Rightarrow p^\alpha \parallel h(F).$$
(See [3]).

Here and in what follows, $h(L)$ means the class-number of the algebraic number field L.

We shall prove in this note, which will be the last paper of this series, that the following theorem follows also from the above proposition:

Theorem. *Let q be an odd prime such that $p = 8q + 1$ 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, $4q + 1$ is not a power of 5 and $7q + 1$ is not a power of 2. Then*
$$h^+(p) < p \text{ and } h(k(p)) \geqq 5 \Rightarrow h^+(p) = h(k(p))$$
where $k(p)$ is the unique quartic subfield of $\boldsymbol{Q}(\zeta_p)$ over $\boldsymbol{Q}$.

Proof. Since $8 \cdot 3 + 1 = 25$, we may assume $q \geqq 5$. Put $K = \boldsymbol{Q}(\zeta_p + \zeta_p^{-1})$ and $k = k(p)$. Then K/k is a q-extension and the above proposition can be applied.

If $q \nmid h(k)$, then $q \nmid h(K)$ (see [2]). Since $h(K) < p$, $h(k) < p$. It is easy to show that if $q \mid h(k)$, then $q \parallel h(k)$ and $q \parallel h(K)$. Now let r be an odd prime. If $r \equiv 1 \pmod q$, $r \mid h(k)$ and $r \mid h(K)$, then $r = 1 + 2nq$, where $n = 1$ or 2 or 3. Since $r^2 > p$, we have that $r \parallel h(k)$, $r \parallel h(K)$. If $r \equiv 1 \pmod q$ and $r \nmid h(k)$, $r \mid h(K)$, then $h(K) \geqq r \cdot h(k) \geqq 5r > p$. Hence we have that