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 $0 \leq \alpha < f$,*

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

(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 $q \| h(k)$ and $q \| h(K)$. 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 $r \| h(k)$, $r \| h(K)$. 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

$r \nmid h(k) \Rightarrow r \mid h(K)$. Now $f > 1$ is the order of $r \bmod q$. We will show that $r^f > p$.

In case $r \geqq 11$, $r^f - 1 = (r-1)(r^{f-1} + \cdots + 1)$ can not be $2nq$, where $n = 1$ or 2 or 3.

Let $r = 7$ and $7^f = 1 + 2nq$, where $n = 1$ or 2 or 3. Then f is even. Now let $f = 2m$ for some integer m. Hence $(7^m - 1)(7^m + 1) = 2nq$, where $n = 1$ or 2 or 3. This is a contradiction.

Let $r = 5$ and $5^f = 1 + 2nq$, where $n = 1$ or 3.

Let $5^f = 1 + 2q$. Then f is even. Now let $f = 2m$ for some integer m. Hence $(5^m - 1)(5^m + 1) = 2q$. This is a contradiciton.

Let $r = 5$ and $5^f = 1 + 6q$. Then f is even. Now let $f = 2m$ for some integer m. Hence $(5^m - 1)(5^m + 1) = 6q$. This is a contradiction.

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

Next $r = 2$ and $2^f = 1 + 3q$ or $2^f = 1 + 5q$ or $2^f = 1 + 7q$, 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 $2^f \neq 1 + 3q$. If $2^f = 1 + 5q$, then we have $f = 4m$ for some integer m. $2^f - 1 = (4^m - 1)(4^m + 1) = 5q$ and $3 \mid 4^m - 1$, we have that $2^f \neq 1 + 5q$.

Examples. Suppose $p = 857$ or 2153. Suppose $h^+(p) < p$. Then $h^+(p) = h(k(p)) = 5$ (see [1]).

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

References

[1] M. N. Gras: Table Numérique du Nombre de Classes et des Unités des Extensions Cycliques de Degré 4 de $\boldsymbol{Q}$. Publ. math. fasc., **2**, Fac. Sci. Besancon (1977/1978).

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

[3] H. Osada: A remark on the class-number of the maximal real subfield of a cyclotomic field. Proc. Japan Acad., **65A**, 318–319 (1989); ditto. II, III. ibid., **68A**, 41–42; 237–238 (1992).

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