Stanislav Jakubec
Schinzel's conjecture and divisibility of class number $h_p^+$


**Terms of use:**
© Mathematical Institute of the Slovak Academy of Sciences, 2003

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*
SCHINZEL’S CONJECTURE AND DIVISIBILITY OF CLASS NUMBER $h_p^+$

STANISLAV JAKUBEC

(Communicated by Pavol Zlatoš)

ABSTRACT. In this paper, we consider the class number of real cyclotomic fields for a prime conductor $p$ satisfying that both $\frac{p-1}{2}$ and $\frac{p-3}{4}$ are primes. According to Schinzel’s conjecture, for the polynomials $X$, $2X+1$, $4X+3$, there are infinitely many primes $p$ with this property. We investigate divisibility of the class number $h_p^+$.

In this paper we consider the class number of real cyclotomic fields for a prime conductor $p$ satisfying that both $\frac{p-1}{2}$ and $\frac{p-3}{4}$ are primes. According to Schinzel’s conjecture, for the polynomials $X$, $2X+1$, $4X+3$, there are infinitely many primes $p$ with this property. For this type of primes, the following theorem has been proved in [2].

THEOREM. ([2; Theorem 1]) Let $p = 8k(2m + 1)!! - 1$ be a prime with the property that $l = 4k(2m + 1)!! - 1$ and $2k(2m + 1)!! - 1$ are primes. Then $(h_p^+, (2m + 1)!!) = 1$.

The aim of this paper is to prove the following two theorems.

THEOREM 1. Let $m$, $M$, $A$ be any positive integers such that

(i) $(m, M) = 1$, $mM \equiv 1 \pmod{2}$, and $M$ is square-free;
(ii) $A \equiv \pm 1 \pmod{m}$, and $A^{q-1} \equiv 1 \pmod{q^2}$ for any prime divisor $q$ of $M$.

Then for each prime of the form $p = -m + MA + kmM^2$ for some integer $k$ satisfying $(k, M) = 1$, we have $(h_p^+, M) = 1$.

2000 Mathematics Subject Classification: Primary 11R29.
Keywords: class number.
THEOREM 2. Let $m$, $M$, $a$, $A$ be any positive integers such that

(i) $(m, M) = 1$, $mM \equiv 1 \pmod{2}$, and $M$ is square-free;
(ii) $aA \equiv \pm 1 \pmod{m}$, $(aA, M) = 1$ and $a^{q-1} \not\equiv 1 \pmod{q^2}$ for any prime divisor $q$ of $M$.

Then for each prime of the form $p = -m + kaAM$ for some integer $k$ satisfying $(k, M) = 1$, we have $(h^+_p, M) = 1$.

These theorems will be proved using [1; Theorem 1]. The following text is taken from [1].

Let $q$ be an odd prime. Define the numbers $A_0, A_1, A_2, \ldots, A_{q-1}$ as follows:

$$A_0 = 0, \quad A_j = \sum_{i=1}^{j} \frac{1}{i} \quad \text{for} \quad j = 1, 2, \ldots, q - 1.$$ 

Let $s$ be a rational $q$-integer. Put $A_s = A_j$ for an integer $j$, $0 \leq j < q$, $s \equiv j \pmod{q}$.

Let $m$, $n$ be natural numbers $m \equiv 1 \pmod{2}$, $(m, n) = 1$. Associate to the number $n$ the permutation $\phi_{m,n}$ of the numbers $1, 2, \ldots, \frac{m-1}{2}$ as follows:

$$\phi_{m,n}(x) \equiv \pm nx \pmod{m} \quad \text{for} \quad x = 1, 2, \ldots, \frac{m-1}{2}.$$ 

Further, associate to the number $n$ the following quadratic form:

$$Q_{m,n}(X_1, X_2, \ldots, X_{\frac{m-1}{2}}) = X_1^2 + X_2^2 + \cdots + X_{\frac{m-1}{2}}^2 - \sum_{i=1}^{\frac{m-1}{2}} X_i X_{\phi_{m,n}(i)}.$$ 

The following Theorem holds:

THEOREM. ([1; Theorem 1]) Let $q$ be an odd prime. Let $l$, $p$ be primes such that $p = 2l+1$, $l \equiv 3 \pmod{4}$, $p \equiv -m \pmod{q}$, $m \equiv 1 \pmod{2}$, $m > 0$, and let the order of the prime $q$ modulo $l$ be $\frac{l-1}{2}$. Suppose that $q$ divides $h^+$, the class number of the real cyclotomic field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Then for each divisor $n$, $(n, q) = 1$, of the number $p + m$, the following congruence holds

(i) $\frac{p + m}{2q} n^{q-1} - 1 \equiv Q_{m,n}(A_{-\frac{1}{m}}, A_{-\frac{2}{m}}, \ldots, A_{-\frac{t}{m}}) \pmod{q}.$ 

If $nq \mid \frac{p+m}{q}$, then

(ii) $\frac{p + m}{2q^2} \equiv -Q_{m,qn}(A_{-\frac{1}{m}}, A_{-\frac{2}{m}}, \ldots, A_{-\frac{t}{m}}) \pmod{q},$ \quad where $t = \frac{m-1}{2}.$
Proof of Theorem 1. Because for a prime $p$, both $\frac{p-1}{2}$ and $\frac{p-3}{4}$ are primes, it follows that every prime $q$, $q \not\equiv \pm 1 \pmod{l}$ ($l = \frac{p-1}{2}$) either is a primitive root modulo $l$ or generates a group of quadratic residues modulo $l$. Hence either $q$ does not divide $h_p^+$ according to [3; Example 1] or the assumptions of [1; Theorem 1] are satisfied.

Put $n = A + kmM$, hence $n$ divides $p+m$. Now we shall apply [1; Theorem 1] for prime $q$ and $n = A + kmM$. Since $n \equiv \pm 1 \pmod{m}$, the permutation $\phi_{m,n}(x)$ is identical and hence $Q_{m,n}(X_1, X_2, \ldots, X_t) = 0$. If $q$ divides the class number $h_p^+$, then

$$\frac{p+m}{2q} \equiv 0 \pmod{q}.$$ 

Hence

$$\left( \frac{AM}{q} + km \frac{M^2}{q} \right) \frac{(A + kmM)^{q-1} - 1}{q} \equiv 0 \pmod{q}.$$ 

Clearly $\frac{AM}{q} + km \frac{M^2}{q} \not\equiv 0 \pmod{q}$. The number $A + kmM$ has the form $A + Kq$, where $K \not\equiv 0 \pmod{q}$. Since

$$\frac{A^{q-1} - 1}{q} \equiv 0 \pmod{q},$$ 

we have

$$\frac{(A + Kq)^{q-1} - 1}{q} \not\equiv 0 \pmod{q}.$$ 

This implies that $q$ does not divide the class number $h_p^+$. \qed

Proof of Theorem 2. We apply [1; Theorem 1] to the prime $q$. Let $n = aA$. Since $aA \equiv \pm 1 \pmod{m}$, the permutation $\phi_{m,aA}(x)$ is identical, hence $Q_{m,aA}(X_1, X_2, \ldots, X_t) = 0$. Now, we will apply [1; Theorem 1] again; first for $n = a$ and in the next turn for $n = A$. Since $aA \equiv \pm 1 \pmod{m}$, it follows that the permutations $\phi_{m,a}(x)$ and $\phi_{m,A}(x)$ are mutually inverse, hence $Q_{m,a}(X_1, X_2, \ldots, X_t) = Q_{m,A}(X_1, X_2, \ldots, X_t)$. Therefore for the Fermat quotient we have $Q_q(a) \equiv Q_q(A) \pmod{q}$ and hence

$$0 \equiv Q_q(aA) \equiv Q_q(a) + Q_q(A) \equiv 2Q_q(a) \pmod{q}.$$ 

This implies that $Q_q(a) \equiv 0 \pmod{q}$, a contradiction. \qed
COROLLARY 1. Let \( m, M, s \) be any positive integers such that

(i) \((m, M) = 1\), \(mm \equiv 1 \pmod{2}\), and \( M \) is square-free;
(ii) \( s \equiv 1 \pmod{2}\), \((sm \pm 1, M) = 1\) and \(2^{q-1} \not\equiv 1 \pmod{q^2}\) for any prime divisor \( q \) of \( M \).

Then for each prime of the form \( p = -m + 2k\frac{(ms+1)}{2}M \) for some integer \( k \) satisfying \((M, k) = 1\), we have \((h^+_p, M) = 1\).

Remark. Two primes are known such that \( Q_q(2) \equiv 0 \pmod{q} \). They are \( q = 1093 \) and 3511.

REFERENCES

