ACTA ARITHMETICA
XCIV.2 (2000)

Connection between Schinzel's conjecture and divisibility of the class number h_p^+

by

Stanislav Jakubec (Bratislava)

Notations

- $(2m+1)!! = 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2m+1)$,
- h_p^+—class number of the field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$,
- $Q_2 = (2^{q-1} - 1)/q$,
- $A_j = 1 + 1/2 + \ldots + 1/j, \qquad A_0 = 0$,
- B_k, $B_k(X)$—Bernoulli number and Bernoulli polynomial,
- E_k, $E_k(X)$—Euler number and Euler polynomial.

Introduction. The aim of this paper is to prove the following

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 $(h_p^+, (2m+1)!!) = 1$.*

It is easy to observe a connection between Theorem 1 and Schinzel's conjecture for the linear polynomials $8X(2m+1)!! - 1$, $4X(2m+1)!! - 1$ and $2X(2m+1)!! - 1$. If Schinzel's conjecture for the linear polynomials holds, then there are infinitely many prime numbers p which satisfy the assumptions of Theorem 1.

Schinzel's conjecture. Let $s \geq 1$, let $f_1(X), \ldots, f_s(X)$ be irreducible polynomials with integral coefficients; assume that the leading coefficient of $f_i(X)$ is positive and that no integer $n > 1$ divides all the numbers $f_1(m)f_2(m)\ldots f_s(m)$. Then there exists one (and then, as may be proved, necessarily infinitely many) natural number(s) m such that $f_1(m), \ldots, f_s(m)$ are all primes.

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11B68.

The proof of Theorem 1 will be based on Theorem 5 of [2]. Let j be an integer, $0 < j < 2q$, $j \equiv 0 \pmod 2$. Define

$$S_j = \sum_{i=1}^{(q-1)/2} A_i \sum_{\substack{k=1 \\ k\equiv 1 \,(\mathrm{mod}\, 2) \\ 2ji \not\equiv -k \,(\mathrm{mod}\, q)}}^{j-1} \frac{1}{2ji+k} - \sum_{i=(q+1)/2}^{q-1} A_i \sum_{\substack{k=1 \\ k\equiv 1 \,(\mathrm{mod}\, 2) \\ 2ji \not\equiv -k \,(\mathrm{mod}\, q)}}^{j-1} \frac{1}{2ji+k}.$$

Theorem (5 of [2]). *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -1 \pmod q$, and let the order of the prime q modulo l be $(l-1)/2$. Suppose that for each j such that $S_j \equiv 0 \pmod q$ there exists n, $(n, 2q) = 1$, $n \mid p+1$, such that $S_{j^*} \not\equiv 0 \pmod q$, where $j^* \equiv nj \pmod{2q}$. Then q does not divide h_p^+, the class number of the real cyclotomic field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.*

Lemma 1. *If $q > 3$, then*

$$S_j \equiv -Q_2 - \sum_{k=1}^{(q-3)/2} \frac{(2^{2k}-1)(2^{2k+1}-1)}{2k \cdot 2^{2k}} \binom{q-1}{2k} j^{2k} B_{2k} B_{q-1-2k} \pmod q.$$

Proof. Consider the sums $\sum_{i=1}^{(q-1)/2} (a+i)^{q-2} A_i$ modulo q, where $a \in \mathbb{Q}$, $a \not\equiv 0 \pmod q$ and a is a q-integer.

Define $S_n(i) = 1^n + 2^n + \ldots + (i-1)^n$ for $n \geq 0$. The following formula will be used:

$$S_n(i) = \frac{1}{n+1}(B_{n+1}(i) - B_{n+1}).$$

The binomial theorem applied to $(a+i)^{q-2}$ yields

$$\sum_{i=1}^{(q-1)/2} (a+i)^{q-2} A_i \equiv A_{(q-1)/2} \sum_{n=0}^{q-2} \binom{q-2}{n} a^{q-2-n} S_n\left(\frac{q+1}{2}\right) - \sum_{n=0}^{q-2} \binom{q-2}{n} a^{q-2-n} \sum_{i=1}^{(q-1)/2} \frac{1}{i} S_n(i) \pmod q.$$

Since

$$S_n\left(\frac{q+1}{2}\right) \equiv \frac{1}{n+1}\left(B_{n+1}\left(\frac{1}{2}\right) - B_{n+1}\right) \equiv \frac{1}{n+1}(2^{-n} - 2)B_{n+1} \pmod q$$

for $0 < n \leq q-2$, it follows that

$$\sum_{n=0}^{q-2} \binom{q-2}{n} a^{q-2-n} S_n\left(\frac{q+1}{2}\right) \equiv -\frac{1}{a} + \sum_{n=0}^{q-2} \binom{q-2}{n} a^{q-2-n} \frac{1}{n+1}(2^{-n} - 2)B_{n+1} \pmod q.$$

Note that $(2^{q-1}-1)B_{q-1}$ is a q-integer; in fact $(2^{q-1}-1)B_{q-1} \equiv -Q_2 \pmod q$.

From the congruence

$$\binom{q-2}{n} \equiv -\binom{q-1}{n+1}(n+1) \equiv (-1)^n(n+1) \pmod q,$$

we get

$$\begin{aligned}\sum_{n=0}^{q-2}\binom{q-2}{n}a^{q-2-n}S_n\left(\frac{q+1}{2}\right) &\equiv -\frac{1}{a} - \sum_{k=1}^{q-1}\binom{q-1}{k}a^{-k}(2^{1-k}-2)B_k \\ &\equiv -\frac{1}{a} - 2\sum_{k=1}^{q-1}\binom{q-1}{k}\left(\frac{1}{2a}\right)^k B_k \\ &\quad + 2\sum_{k=1}^{q-1}\binom{q-1}{k}\left(\frac{1}{a}\right)^k B_k \pmod q.\end{aligned}$$

Using the formula ((50.5.33) of [1])

$$\sum_{k=0}^{n}\frac{(-n)_k}{k!}a^k B_k(X) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}a^k B_k(X) = (-a)^n B_n\left(X-\frac{1}{a}\right),$$

we altogether get

$$\begin{aligned}&A_{(q-1)/2}\sum_{n=0}^{q-2}\binom{q-2}{n}a^{q-2-n}S_n\left(\frac{q+1}{2}\right) \\ &\qquad \equiv A_{(q-1)/2}\left(2B_{q-1}(a) - 2B_{q-1}(2a) - 2Q_2 - \frac{1}{a}\right) \pmod q.\end{aligned}$$

Using the same procedure we get the following congruences modulo q:

$$\begin{aligned}&\sum_{n=0}^{q-2}\binom{q-2}{n}a^{q-2-n}\sum_{i=1}^{(q-1)/2}\frac{1}{i}S_n(i) \\ &\qquad \equiv \frac{1}{a}\sum_{i=1}^{(q-1)/2}\frac{i-1}{i} \\ &\qquad\quad + \sum_{n=1}^{q-2}(-1)^n(n+1)\frac{1}{a^{n+1}}\sum_{i=1}^{(q-1)/2}\frac{1}{i}\cdot\frac{1}{n+1}(B_{n+1}(i)-B_{n+1}) \\ &\qquad \equiv \frac{1}{a}\left(\frac{q-1}{2} - A_{(q-1)/2}\right) + \sum_{k=2}^{q-1}(-1)^{k+1}\frac{1}{a^k}\sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_k(i)-B_k)\end{aligned}$$

$$\equiv \frac{1}{a}\left(\frac{q-1}{2} - A_{(q-1)/2}\right) - \frac{1}{a}\sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_1(i) - B_1)$$

$$-\sum_{k=0}^{q-1}(-1)^k\binom{q-1}{k}\left(\frac{-1}{a}\right)^k\sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_k(i) - B_k).$$

By switching the order of summation in the sum

$$\sum_{k=0}^{q-1}(-1)^k\binom{q-1}{k}\left(\frac{-1}{a}\right)^k\sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_k(i) - B_k),$$

using the above quoted formula (50.5.33) of [1] we get

$$\sum_{n=0}^{q-2}\binom{q-2}{n}a^{q-2-n}\sum_{i=1}^{(q-1)/2}\frac{1}{i}S_n(i)$$

$$\equiv -\frac{1}{a}A_{(q-1)/2} - \sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_{q-1}(i+a) - B_{q-1}(a)) \pmod q.$$

Altogether we get

$$(1)\quad \sum_{i=1}^{(q-1)/2}(a+i)^{q-2}A_i \equiv 2A_{(q-1)/2}(B_{q-1}(a) - B_{q-1}(2a) - Q_2)$$

$$+\sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_{q-1}(i+a) - B_{q-1}(a)) \pmod q.$$

The congruence (1) is thus proved for $a \not\equiv 0 \pmod q$. We now prove it for $a \equiv 0 \pmod q$. That is, for $a \equiv 0 \pmod q$ we claim that

$$\sum_{i=1}^{(q-1)/2}\frac{1}{i}A_i \equiv -2A_{(q-1)/2}Q_2 + \sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_{q-1}(i) - B_{q-1}) \pmod q.$$

Because $\sum_{i=1}^{(q-1)/2} 1/i^2 \equiv 0 \pmod q$, we have

$$\sum_{i=1}^{(q-1)/2}\frac{1}{i}A_i \equiv \sum_{i=1}^{(q-1)/2}\frac{1}{i}A_{i-1} \equiv \frac{1}{q-1}\sum_{i=1}^{(q-1)/2}\frac{1}{i}(B_{q-1}(i) - B_{q-1}) \pmod q.$$

It is sufficient to prove

$$\sum_{i=1}^{(q-1)/2}\frac{1}{i}A_{i-1} \equiv -A_{(q-1)/2}Q_2 \equiv \frac{1}{2}A_{(q-1)/2}^2 \pmod q.$$

This follows from the relation

$$A_{(q-1)/2}^2 = 1^2 + \left(\frac{1}{2}\right)^2 + \ldots + \left(\frac{1}{\frac{q-1}{2}}\right)^2 + 2\left(1\cdot\frac{1}{2} + 1\cdot\frac{1}{3} + \ldots + \frac{1}{\frac{q-3}{2}}\cdot\frac{1}{\frac{q-1}{2}}\right).$$

Now put

$$S^* = \sum_{i=1}^{(q-1)/2} (i+a)^{q-2} A_i - \sum_{i=(q+1)/2}^{q-1} (i+a)^{q-2} A_i.$$

For the numbers $A_0, A_1, \ldots, A_{q-1}$ we have

$$A_{(q-1)/2+k} \equiv A_{(q-1)/2-k} \pmod q \qquad \text{for } k = 1, 2, \ldots, (q-1)/2,$$

and so

$$\begin{aligned}
&- \sum_{i=(q+1)/2}^{q-1} (i+a)^{q-2} A_i \\
&\quad \equiv -\left(\frac{q-1}{2} + 1 + a\right)^{q-2} A_{(q-1)/2-1} \\
&\qquad - \left(\frac{q-1}{2} + 2 + a\right)^{q-2} A_{(q-1)/2-2} - \ldots - \left(\frac{q-1}{2} + \frac{q-3}{2} + a\right)^{q-2} A_1 \\
&\quad \equiv \left(\frac{q-3}{2} + 1 - a\right)^{q-2} A_{(q-3)/2} \\
&\qquad + \left(\frac{q-5}{2} + 1 - a\right)^{q-2} A_{(q-5)/2} + \ldots + (1+1-a)^{q-2} A_1 \\
&\quad \equiv \sum_{i=1}^{(q-1)/2} (i+1-a)^{q-2} A_i - \left(\frac{1}{2} - a\right)^{q-2} A_{(q-1)/2} \pmod q.
\end{aligned}$$

By congruence (1) we have

$$\begin{aligned}
S^* \equiv\ & 2A_{(q-1)/2}(B_{q-1}(a) - B_{q-1}(2a) - Q_2) \\
& + \sum_{i=1}^{(q-1)/2} \frac{1}{i}(B_{q-1}(a+i) - B_{q-1}(a)) \\
& + 2A_{(q-1)/2}(B_{q-1}(1-a) - B_{q-1}(2-2a) - Q_2) \\
& + \sum_{i=1}^{(q-1)/2} \frac{1}{i}(B_{q-1}(1-a+i) - B_{q-1}(1-a)) \\
& - \left(\frac{1}{2} - a\right)^{q-2} A_{(q-1)/2} \pmod q.
\end{aligned}$$

Since $B_{q-1}(X) = B_{q-1}(1-X)$, we have $B_{q-1}(2-2a) = B_{q-1}(2a-1)$, $B_{q-1}(1-a+i) = B_{q-1}(a-i)$ and $B_{q-1}(1-a) = B_{q-1}(a)$. Moreover, the formula

$$B_{q-1}(X) = B_{q-1}(-X) - (q-1)X^{q-2}$$

gives

$$\begin{aligned} B_{q-1}(2a-1) &= B_{q-1}(1-2a) + 2(q-1)B_1(2a-1)^{q-2} \\ &= B_{q-1}(2a) - (q-1)(2a-1)^{q-2}. \end{aligned}$$

So we obtain

$$\begin{aligned} (2)\quad S^* \equiv{}& 4A_{(q-1)/2}(B_{q-1}(a) - B_{q-1}(2a) - Q_2) \\ &+ \sum_{i=1}^{(q-1)/2} \frac{1}{i}(B_{q-1}(a+i) + B_{q-1}(a-i) - 2B_{q-1}(a)) \pmod q. \end{aligned}$$

Now using the congruence (2) let us start to compute the sums S_j defined in the introduction. We write

$$\begin{aligned} S_j \equiv{}& \sum_{i=1}^{(q-1)/2} A_i \sum_{\substack{k=1 \\ k\equiv 1 \,(\mathrm{mod}\, 2)}}^{j-1} (2ji+k)^{q-2} - \sum_{i=(q+1)/2}^{q-1} A_i \sum_{\substack{k=1 \\ k\equiv 1 \,(\mathrm{mod}\, 2)}}^{j-1} (2ji+k)^{q-2} \\ \equiv{}& (2j)^{q-2}\Bigg(\sum_{i=1}^{(q-1)/2} A_i \sum_{\substack{k=1 \\ k\equiv 1 \,(\mathrm{mod}\, 2)}}^{j-1} \left(i + \frac{k}{2j}\right)^{q-2} \\ &- \sum_{i=(q+1)/2}^{q-1} A_i \sum_{\substack{k=1 \\ k\equiv 1 \,(\mathrm{mod}\, 2)}}^{j-1} \left(i + \frac{k}{2j}\right)^{q-2}\Bigg) \pmod q. \end{aligned}$$

We now reverse the order of summations. For the inner summation (over i) we use (2) with $a = k/(2j)$. For the summation over k, the following formulas will be used. According to (50.7.2) of [1],

$$(3)\qquad \sum_{k=0}^{n-1} B_m\left(X + \frac{k}{n}\right) = n^{1-m}B_m(nX),$$

and by (50.7.4) of [1],

$$(4)\qquad \sum_{k=0}^{2n-1} (-1)^{k+1} B_m\left(X + \frac{k}{2n}\right) = 2^{-m}n^{1-m}mE_{m-1}(2nX).$$

Let us denote by $\sum'$ a summation over odd values of k. In view of the congruence (2) it is necessary to compute

$$\sum_{k=1}^{j-1}{}' \left(B_{q-1}\left(\frac{k}{2j} + i\right) + B_{q-1}\left(\frac{k}{2j} - i\right)\right).$$

By the identity $B_{q-1}(X) = B_{q-1}(1-X)$ we have

$$\sum_{k=1}^{j-1}{}' \left(B_{q-1}\left(\frac{k}{2j}+i\right) + B_{q-1}\left(\frac{k}{2j}-i\right)\right) = \sum_{k=1}^{2j-1}{}' B_{q-1}\left(\frac{k}{2j}+i\right).$$

Using (3) and (4), we altogether obtain

$$\sum_{k=1}^{j-1}{}' \left(B_{q-1}\left(\frac{k}{2j}+i\right) + B_{q-1}\left(\frac{k}{2j}-i\right)\right)$$
$$= \frac{1}{2}((2j)^{1-(q-1)}B_{q-1}(2ji) + (q-1)2^{-(q-1)}j^{1-(q-1)}E_{q-2}(2ji)).$$

Using the identity

$$E_{q-2}(2ji) = \frac{2}{q-1}(B_{q-1}(2ji) - 2^{q-1}B_{q-1}(ji)),$$

we get

$$\sum_{k=1}^{j-1}{}' \left(B_{q-1}\left(\frac{k}{2j}+i\right) + B_{q-1}\left(\frac{k}{2j}-i\right)\right) = j^{2-q}(2^{2-q}B_{q-1}(2ji) - B_{q-1}(ji)). \tag{5}$$

Consider now the sums

$$\sum_{k=1}^{j-1}{}' B_{q-1}\left(\frac{k}{2j}\right), \quad \sum_{k=1}^{j-1}{}' B_{q-1}\left(\frac{k}{j}\right).$$

The identity (5) for $i = 0$ implies

$$\sum_{k=1}^{j-1}{}' B_{q-1}\left(\frac{k}{2j}\right) = \frac{1}{2}j^{2-q}(2^{2-q}-1)B_{q-1},$$

and using (3) and (4) we obtain, since j is even,

$$\sum_{k=0}^{j-1} B_{q-1}\left(\frac{k}{j}\right) = j^{1-(q-1)}B_{q-1},$$
$$\sum_{k=0}^{j-1}(-1)^{k+1}B_{q-1}\left(\frac{k}{j}\right) = 2^{-(q-1)}\left(\frac{j}{2}\right)^{1-(q-1)}(q-1)E_{q-2}(0).$$

By summing the last two identities using the previous formula for a relation between Euler and Bernoulli polynomials we have

$$\sum_{k=1}^{j-1}{}' B_{q-1}\left(\frac{k}{j}\right) = (1-2^{q-1})2^{1-q}\left(\frac{j}{2}\right)^{2-q}B_{q-1} + \frac{1}{2}j^{2-q}B_{q-1}.$$

Using the formula for S^* we get

$$S_j \equiv 2^{q-1}A_{(q-1)/2}((2^{2-q}-1)B_{q-1} - (1-2^{q-1})B_{q-1} - B_{q-1} - Q_2) + 2^{q-2}\sum_{i=1}^{(q-1)/2}\frac{1}{i}((2^{2-q}B_{q-1}(2ij) - B_{q-1}(ij)) - (2^{2-q}-1)B_{q-1}) \pmod q.$$

This shows that if $q > 3$ then

$$S_j \equiv \sum_{i=1}^{(q-1)/2}\frac{1}{i}\left(B^*_{q-1}(2ji) - \frac{1}{2}B^*_{q-1}(ji)\right) \pmod q,$$

where $B^*_{q-1}(X) = B_{q-1}(X) - B_{q-1}$.

For $c \in \mathbb{Z}$, we have

$$\sum_{k=1}^{(q-1)/2}\frac{1}{k}B^*_{q-1}(kc) \equiv \sum_{k=1}^{(q-1)/2}k^{q-2}(B_{q-1}(kc) - B_{q-1}) = \sum_{k=1}^{(q-1)/2}k^{q-2}B_{q-1}(kc) - B_{q-1}\sum_{k=1}^{(q-1)/2}k^{q-2}.$$

Using the formula (50.7.14) of [1]:

$$\sum_{k=1}^{n}k^rB_m(kX) = \sum_{k=0}^{m}\frac{(-m)_k}{(r+k+1)k!}(-X)^kB_{m-k}(B_{r+k+1}(n+1) - B_{r+k+1}),$$

we have

$$\sum_{k=1}^{(q-1)/2}k^{q-2}B_{q-1}(kc) = \sum_{k=0}^{q-1}\binom{q-1}{k}\frac{(-1)^k}{q-1+k}(-c)^kB_{q-1-k}\left(B_{q-1+k}\left(\frac{q+1}{2}\right) - B_{q-1+k}\right).$$

For the term with $k = 0$ on the right-hand side, note that

$$\frac{1}{q-1}\left(B_{q-1}\left(\frac{q+1}{2}\right) - B_{q-1}\right) = \sum_{k=1}^{(q-1)/2}k^{q-2}.$$

Thus we have

$$\sum_{k=1}^{(q-1)/2}\frac{1}{k}B^*_{q-1}(kc) \equiv \sum_{k=1}^{q-1}\binom{q-1}{k}\frac{1}{q-1+k}c^kB_{q-1-k}\left(B_{q-1+k}\left(\frac{q+1}{2}\right) - B_{q-1+k}\right) \pmod q.$$

For $k = q-1$ we have

$$\frac{1}{2(q-1)}c^{q-1}B_0\bigg(B_{2(q-1)}\bigg(\frac{q+1}{2}\bigg)-B_{2(q-1)}\bigg) \equiv \sum_{k=1}^{(q-1)/2}\frac{1}{k} \equiv -2Q_2 \pmod q,$$

hence

$$\sum_{k=1}^{(q-1)/2}\frac{1}{k}B^*_{q-1}(kc) \equiv -2Q_2 + \sum_{k=1}^{q-2}\binom{q-1}{k}\frac{1}{q-1+k} \times c^k B_{q-1-k}\bigg(B_{q-1+k}\bigg(\frac{q+1}{2}\bigg) - B_{q-1+k}\bigg) \pmod q.$$

Clearly

$$B_{q-1+k}\bigg(\frac{q+1}{2}\bigg) \equiv B_{q-1+k}\bigg(\frac{1}{2}\bigg) \pmod q,$$
$$B_{q-1+k}\bigg(\frac{1}{2}\bigg) = (2^{2-q-k}-1)B_{q-1+k}.$$

By Kummer's congruence $B_{q-1+k} \equiv (q-1+k)B_k/k \pmod q$. Hence

$$\sum_{k=1}^{(q-1)/2}\frac{1}{k}B^*_{q-1}(kc) \equiv -2Q_2 + \sum_{k=1}^{(q-3)/2}\binom{q-1}{2k}\frac{1}{2k}c^{2k}\bigg(\frac{2}{2^{2k}}-2\bigg)B_{q-1-2k}B_{2k} \pmod q. \tag{6}$$

Define

$$F(X) = \sum_{k=1}^{(q-3)/2}\binom{q-1}{2k}\frac{X^{2k}}{2k}B_{2k}B_{q-1-2k}.$$

By (6) we have

$$\sum_{k=1}^{(q-1)/2}\frac{1}{k}B^*_{q-1}(kc) \equiv -2Q_2 + 2F\bigg(\frac{c}{2}\bigg) - 2F(c) \pmod q.$$

Hence if $q > 3$, then

$$\begin{aligned} S_j &\equiv \sum_{i=1}^{(q-1)/2}\frac{1}{i}\bigg(B^*_{q-1}(2ji) - \frac{1}{2}B^*_{q-1}(ji)\bigg) \\ &\equiv -2Q_2 + 2F\bigg(\frac{2j}{2}\bigg) - 2F(2j) - \frac{1}{2}\bigg(-2Q_2 + 2F\bigg(\frac{j}{2}\bigg) - 2F(j)\bigg) \\ &\equiv -Q_2 + 3F(j) - 2F(2j) - F\bigg(\frac{j}{2}\bigg) \pmod q, \end{aligned}$$

hence

$$S_j \equiv -Q_2 - \sum_{k=1}^{(q-3)/2} \frac{(2^{2k}-1)(2^{2k+1}-1)}{2k \cdot 2^{2k}} \binom{q-1}{2k} j^{2k} B_{2k} B_{q-1-2k} \pmod{q}.$$

Lemma 1 is proved. ∎

Proof of Theorem 1. If $q = 3$ then from [3] it follows that $(h_p^+, 3) = 1$. Let q be a prime, $3 < q \le 2m+1$. By the quadratic reciprocity law we have

$$\left(\frac{q}{l}\right) = \left(\frac{-1}{q}\right)\left(\frac{l}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{4k(2m+1)!! - 1}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{-1}{q}\right) = 1.$$

The number $(l-1)/2 = 2k(2m+1)!! - 1$ is prime, and so the order of q modulo l is $(l-1)/2$. Let j be such that $S_j \equiv 0 \pmod{q}$. Now we use Theorem 5 of [2]. The number $p+1$ has divisors $n = 1, 3, \ldots, q-2$. For some n we have $S_{nj} \not\equiv 0 \pmod{q}$. To prove this, note that S_j is a polynomial in j of degree at most $q-3$. Suppose that S_j has roots $j, 3j, \ldots, (q-2)j$; then $-j, -3j, \ldots, -(q-2)j$ are also roots of S_j. Thus the number of roots of S_j is $q-1$, which is a contradiction.

To complete the proof it is necessary to prove that S_j is non-zero modulo q. For this we shall use the bound for the first factor h_q^- from [4] and [5],

$$h_q^- < 2q\left(\frac{q}{24}\right)^{(q-1)/4}.$$

Let $\mathrm{ii}(q)$ be the index of irregularity and d be the order (mod q) of 2. If S_j is a zero polynomial modulo q, then

$$\frac{(2^{2k}-1)(2^{2k+1}-1)}{2k \cdot 2^{2k}} \binom{q-1}{2k} B_{2k} B_{q-1-2k} \equiv 0 \pmod{q}$$

for $k = 1, 2, \ldots, (q-3)/2$, and then

$$\mathrm{ii}(q) > \frac{1}{2}\left(\frac{q-3}{2} - 2\frac{q-1}{d}\right) > \frac{1}{2}\left(\frac{q-3}{2} - 2\frac{q-1}{\log_2 q}\right).$$

This yields

$$q^{\frac{1}{2}\left(\frac{q-3}{2} - 2\frac{q-1}{\log_2 q}\right)} < 2q\left(\frac{q}{24}\right)^{(q-1)/4},$$

and so

$$1 < 4q^3\left(\frac{2}{3}\right)^{(q-1)/2},$$

which is not true for $q > 67$. For primes q, $3 < q \le 67$, the polynomial S_j is non-zero modulo q. Theorem 1 is proved. ∎

Acknowledgements. The author thanks the referee for the important remarks to the proof of Lemma 1.

References

[1] E. R. Hansen, *A Table of Series and Products*, Prentice-Hall, 1973.
[2] S. Jakubec, *Divisibility of the class number* h^+ *of the real cyclotomic fields of prime degree* l, Math. Comp. 67 (1998), 369–398.
[3] —, *On divisibility of* h^+ *by the prime* 3, Rocky Mountain J. Math. 24 (1994), 1467–1473.
[4] T. Lepistö, *On the growth of the first factor of the class number of the prime cyclotomic field*, Ann. Acad. Sci. Fenn. Ser. A I Math. 577 (1974).
[5] T. Metsänkylä, *Class numbers and* μ*-invariants of cyclotomic fields*, Proc. Amer. Math. Soc. 43 (1974), 299–300.

Matematický ústav SAV
Štefánikova 49
814 73 Bratislava, Slovakia
E-mail: jakubec@mat.savba.sk

Received on 27.7.1999
and in revised form on 6.12.1999 (3659)