MATHEMATICS OF COMPUTATION
Volume 67, Number 221, January 1998, Pages 369–398
S 0025-5718(98)00916-8

ON DIVISIBILITY OF THE CLASS NUMBER h^+ OF THE REAL CYCLOTOMIC FIELDS OF PRIME DEGREE l

STANISLAV JAKUBEC

ABSTRACT. In this paper, criteria of divisibility of the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$ of a prime conductor p and of a prime degree l by primes q the order modulo l of which is $\frac{l-1}{2}$, are given. A corollary of these criteria is the possibility to make a computational proof that a given q does not divide h^+ for any p (conductor) such that both $\frac{p-1}{2}$, $\frac{p-3}{4}$ are primes. Note that on the basis of Schinzel's hypothesis there are infinitely many such primes p.

INTRODUCTION

Let l, p be primes such that $p = 2l + 1$. To consider divisibility of the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ by primes q it is suitable to sort primes q according to their order modulo l. The simplest case is the case when the order of q modulo l is $l-1$, i.e. when q is a primitive root modulo l. In this case the problem is completely solved, because it is proved that q does not divide h^+. The proof for $q = 2$ can be found in [1] and for $q > 2$ in [4]. According to complexity, the further case is the case when the order of q modulo l is $\frac{l-1}{2}$, hence when q generates the group of quadratic residues modulo l.

In this case we have:

1) $q = 2$. If $l \equiv 3 \pmod 4$, then 2 does not divide h^+. (For the proof see [2].)

2) $q = 3$. The prime 3 does not divide h^+. (For the proof see [5].)

3) $q = 5$. If $l \equiv 3 \pmod 4$ then 5 does not divide h^+. (For the proof see [6].)

The divisibility of h^+ by a general prime q under the assumption $p \equiv -1 \pmod q$, $p \not\equiv -1 \pmod{q^3}$ was considered in the papers [7], [8].

The aim of this paper is to derive criteria for divisibility of h^+ by a prime q without any restriction imposed on $p \pmod q$. As an application of derived criteria we shall prove Theorem 7 .

Theorem 7. *Let q be prime, $q \leq 23$. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, and let the order of the prime q modulo l be $l-1$ or $\frac{l-1}{2}$. The prime q does not divide h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

Note that if $l = 2l_1 + 1$, where l_1 is a prime, then each $q \not\equiv 0, \pm 1 \pmod l$ satisfies the conditions of Theorem 5.

This implies the following Corollary.

Received by the editor March 16, 1995 and, in revised form, April 12, 1996.
1991 *Mathematics Subject Classification.* Primary 11R29.

Corollary. *Let l_1, l, p be primes such that $l = 2l_1 + 1$, $p = 2l + 1$. The prime q does not divide h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$, for $q \leq 23$.*

* * *

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

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

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:

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

Further, associate to the number n the quadratic form $Q_{m,n}(X_1, X_2, \ldots, X_{\frac{m-1}{2}})$,

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

The following theorem holds

Theorem 1. *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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then for each divisor n, $(n, q) = 1$, of the number $p + m$, the following congruence holds:*

(i)

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

(ii) *If $nq | \frac{p+m}{q}$, then*

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

where $t = \frac{m-1}{2}$.

Proof. To prove this theorem, the following assertion from [4] will be used:

Proposition 1. *Let l, p, q be primes, $p \equiv 1 \pmod l$, $q \neq 2$; $q \neq l$; $q < p$. Let K be a subfield of the field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$, $[K : \mathbf{Q}] = l$ and let h_K be the class number of the field K. If $q | h_K$, then $q | N_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\omega)$, where*

$$\omega = b_1 \sum_{i \equiv 1 \pmod q} \chi(i) + b_2 \sum_{i \equiv 2 \pmod q} \chi(i) + \cdots + b_{q-1} \sum_{i \equiv q-1 \pmod q} \chi(i),$$

with the sums all taken with $1 \leq i \leq p-1$, with $\chi(x)$ a Dirichlet character modulo p of order l, and b_j defined by the expressions

$$\frac{p}{q}\left(\frac{(\zeta_p - 1)^q}{\zeta_p^q - 1} - 1\right) \equiv b_1 \zeta_p + b_2 \zeta_p^2 + \cdots + b_{p-1} \zeta_p^{p-1} \pmod{q}.$$

The following lemma will determine the coefficients $b_1, b_2, \ldots, b_{q-1}$.

Lemma 1. *Let* $p \equiv z \pmod{q}$. *Then*

$$b_i = A_{\frac{-i}{z}}, \text{ for } i = 1, 2, \ldots, q-1.$$

Proof. We note that the b_j can be determined explicitly by multiplying the above expression through by $\zeta_p^q - 1$: In fact we get (taking $b_0 = 0$ and each $b_k = b_{k \pmod{p}}$)

$$\frac{1}{p}\sum_{j=0}^{p-1}(b_{j-q} - b_j)\zeta_p^j \equiv \left(\frac{(\zeta_p - 1)^q - (\zeta_p^q - 1)}{q}\right) = \sum_{i=1}^{q-1}\frac{1}{q}\binom{q}{i}(-1)^{q-i}\zeta_p^i$$

$$\equiv \sum_{i=1}^{q-1}\frac{\zeta_p^i}{i} \pmod{q},$$

since

$$\frac{1}{q}\binom{q}{i} = \frac{1}{i}\frac{(q-1)(q-2)\ldots(q-i+1)}{(i-1)!} \equiv \frac{(-1)^{i-1}}{i} \pmod{q}.$$

Comparing coefficients we see that $b_{j-q} - b_j \equiv b_{-q} - b_0 + p\delta_j \pmod{q}$, where $\delta_j = \frac{1}{j}$ if $1 \le j \le q-1$ and $\delta_j = 0$ otherwise. Adding these congruences together for $j = 0, -q, -2q, \ldots, -(n-1)q$ and noting that $b_0 = 0$, we obtain $b_{-nq} \equiv nb_{-q} + \frac{p}{(p)_p} + \frac{p}{(2p)_q} + \cdots + \frac{p}{(mp)_q} \pmod{q}$, where $(m+1)p \ge nq > mp$ and $(jp)_q$ is the least positive residue of $jp \pmod{q}$, by an easy induction. Taking $n = p$ gives that $0 = b_0 \equiv pb_{-q} + 1 + \frac{1}{2} + \cdots + \frac{1}{q-1} \equiv pb_{-q} \pmod{q}$ (since $\frac{1}{j} + \frac{1}{q-j} \equiv 0 \pmod{q}$ for each j), and thus $b_{-q} \equiv 0 \pmod{q}$. Therefore, if $1 \le j \le p-1$ we write $j = (m+1)p - nq$, so that

$$b_j = b_{-nq} \equiv 1 + \frac{1}{2} + \cdots + \frac{1}{m} \equiv 1 + \frac{1}{2} + \cdots + \frac{1}{(-j/p)_q} \pmod{q}.$$

Lemma 1 is proved. □

Let $p \equiv z \pmod{q}$. By Proposition 1 we have

$$\omega = \sum_{i=1}^{p-1} A_{\frac{-i}{z}}\chi(i).$$

Denote

$$\tau = \sum_{0<i<\frac{p}{2}} A_{\frac{-i}{z}}\chi(i).$$

It is easy to see that $\omega = 2\tau$.

Since the order of q modulo l is $\frac{l-1}{2}$, according to [10], Theorem 2.13, we have that q is splitting to two divisors in $\mathbf{Q}(\zeta_l)$. Because $l \equiv 3 \pmod{4}$, it holds that $\left(\frac{-1}{l}\right) = -1$, hence if $q|\mathrm{N}_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\omega)$, then q divides $\tau\overline{\tau}$.

The following formula holds

$$\tau\overline{\tau} = \sum_{i,j<\frac{p}{2}} A_{\frac{-i}{z}}A_{\frac{-j}{z}}\chi(ij^{-1}) = d_0 + d_1\zeta_l + d_2\zeta_l^2 + \cdots + d_{l-1}\zeta^{l-1}. \tag{1}$$

Then $q|\tau\overline{\tau}$ if and only if

$$d_0 \equiv d_1 \equiv \cdots \equiv d_{l-1} \pmod{q}.$$

Let $p \equiv -m \pmod{q}$, $m > 0$, $m \equiv 1 \pmod{2}$. Hence $b_i = A_{\frac{i}{m}}$. Denote by r such a number that $r < l$, $g^r \equiv \pm n \pmod{p}$. Let $\chi(ij^{-1}) = \zeta_l^r$. Then either

$\operatorname{ind}(ij^{-1}) = r$ or $r+l$, therefore

$$ij^{-1} \equiv \pm n \pmod p, \; i,j < \frac{p}{2}. \tag{2}$$

The following lemma determines the coefficient d_r of (1).

Lemma 2. *Let $p \equiv -m \pmod q$, $m > 0$, $m \equiv 1 \pmod 2$, $g^r \equiv \pm n \pmod p$. For the coefficient d_r, $r < l$, the following holds:*

$$d_r = \sum_{0<j<\frac{p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}} + \sum_{\frac{p}{n}<j<\frac{2p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+1} + \sum_{\frac{2p}{n}<j<\frac{3p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+2} + \cdots + \sum_{\frac{\frac{n-1}{2}p}{n}<j<\frac{p}{2}} A_{\frac{j}{m}} A_{\frac{jn}{m}+\frac{n-1}{2}},$$

for n odd,

$$d_r = \sum_{0<j<\frac{p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}} + \sum_{\frac{p}{n}<j<\frac{2p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+1} + \sum_{\frac{2p}{n}<j<\frac{3p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+2} + \cdots + \sum_{\frac{(\frac{n}{2}-1)p}{n}<j<\frac{p}{2}} A_{\frac{j}{m}} A_{\frac{jn}{m}+\frac{n}{2}-1},$$

for n even.

Proof. By (2), $ij^{-1} \equiv \pm n \pmod p$, $i,j < \frac{p}{2}$. Therefore either $i \equiv nj \pmod p$ or $i \equiv p - nj \pmod p$. Let $nj < p$. From (1) we get the term $A_{\frac{j}{m}} A_{\frac{nj}{m}} \chi(ij^{-1})$ if $nj < \frac{p}{2}$ and $A_{\frac{j}{m}} A_{\frac{p-nj}{m}} \chi(ij^{-1})$ if $nj > \frac{p}{2}$. Clearly $\frac{p-nj}{m} \equiv -1 - \frac{nj}{m} \pmod q$. From $\frac{p-nj}{m} + \frac{nj}{m} \equiv -1 \pmod q$ we get $A_{\frac{nj}{m}} = A_{\frac{p-nj}{m}}$. If $p < nj < 2p$, then the coefficient of $\chi(ij^{-1})$ is $A_{\frac{j}{m}} A_{\frac{nj-p}{m}}$ and hence $A_{\frac{j}{m}} A_{\frac{nj}{m}+1}$. Repeating this procedure we obtain

$$d_r = \sum_{0<j<\frac{p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}} + \sum_{\frac{p}{n}<j<\frac{2p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+1} + \sum_{\frac{2p}{n}<j<\frac{3p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+2} + \dots. \qquad \square$$

The following lemma determines the coefficient d_r, $g^r \equiv \pm n \pmod p$ in the special case when $n | \frac{p+m}{q}$. The reason why we restrict ourselves to such special coefficients is that in this case it is possible to give such criterion of divisibility h^+ that has a simple form (see Theorem 1). If n does not divide $\frac{p+m}{q}$, then things are more complicated and even in the most simple case when $n = 3$ and 3 does not divide $\frac{p+m}{q}$, the corresponding criteria have a more complicated form than Theorem 1 (see Theorem 2).

Lemma 3. *Let $p \equiv -m \pmod q$, $m > 0$, $m \equiv 1 \pmod 2$, $g^r \equiv \pm n \pmod p$. For the coefficient d_r, $r < l$, $n | \frac{p+m}{q}$ the following holds:*

$$\begin{aligned} d_r \equiv \frac{p+m}{qn} \Bigg(& \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}} + \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+1} \\ & + \cdots + \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+\frac{n-3}{2}} + \frac{1}{2} \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+\frac{n-1}{2}} \Bigg) \\ & - \sum_{i=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+[\frac{ni}{m}]} \pmod q, \end{aligned} \tag{3}$$

for $n \equiv 1 \pmod 2$,

$$d_r \equiv \frac{p+m}{qn}\left(\sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}} + \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+1} + \cdots + \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+\frac{n}{2}-1}\right)$$

$$- \sum_{i=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+[\frac{ni}{m}]} \pmod q,$$

for $n \equiv 0 \pmod 2$.

Proof. The following congruences hold

$$\sum_{0<j<\frac{p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}} \equiv \frac{p+m}{qn} \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}} - \sum_{[\frac{in}{m}]=0}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}},$$

$$\sum_{\frac{p}{n}<j<\frac{2p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+1} \equiv \frac{p+m}{qn} \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+1} - \sum_{[\frac{in}{m}]=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+1},$$

$$\sum_{\frac{p\frac{n-1}{2}}{n}<j<\frac{p}{2}} A_{\frac{j}{m}} A_{\frac{jn}{m}+\frac{n-1}{2}} \equiv \frac{p+m}{2qn} \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+\frac{n-1}{2}} - \sum_{[\frac{in}{m}]=\frac{n-1}{2}}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+\frac{n-1}{2}},$$

for n odd.

And

$$\sum_{0<j<\frac{p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}} \equiv \frac{p+m}{qn} \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}} - \sum_{[\frac{in}{m}]=0}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}},$$

$$\sum_{\frac{p}{n}<j<\frac{2p}{n}} A_{\frac{j}{m}} A_{\frac{jn}{m}+1} \equiv \frac{p+m}{qn} \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+1} - \sum_{[\frac{in}{m}]=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+1},$$

$$\sum_{\frac{p(\frac{n}{2}-1)}{n}<j<\frac{p}{2}} A_{\frac{j}{m}} A_{\frac{jn}{m}+\frac{n}{2}-1} \equiv \frac{p+m}{qn} \sum_{i=1}^{q-1} A_{\frac{i}{m}} A_{\frac{ni}{m}+\frac{n}{2}-1} - \sum_{[\frac{in}{m}]=\frac{n}{2}-1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+\frac{n}{2}-1},$$

for n even.

These congruences can be proved as follows. Let n be odd. If $s \equiv t \pmod q$, then $A_s \equiv A_t \pmod q$. On the basis of this fact it is enough to prove that for each $k = 1, 2, \ldots, \frac{n-1}{2}$ the following holds: the set $\{j \mid \frac{kp}{n} < j < \frac{(k+1)p}{n}\} \cup \{-i \mid \left[\frac{in}{m}\right] = k, i \le \frac{m-1}{2}\}$ gives $\frac{p+m}{qn}$ exemplars of the full residue system modulo q for $k =$

$1, 2, \dots, \frac{n-3}{2}$, and $\frac{p+m}{2qn}$ exemplars of the full residue system modulo q for $k = \frac{n-1}{2}$.

From $n|p+m$ we get that $(m,n) = 1$. Hence $\left[\frac{in}{m}\right] = k$, $k \neq 0$ if and only if

$$\frac{km}{n} < i < \frac{(k+1)m}{n}.$$

Denote $\frac{p+m}{nq} = v$, hence $m = nqv - p$. It implies

$$kqv - \frac{kp}{n} < i < (k+1)qv - \frac{(k+1)p}{n}.$$

Multiplying by -1 and adding $(k+1)qv$, we get

$$\frac{(k+1)p}{n} < -i + (k+1)qv < \frac{kp}{n} + qv.$$

Denote $i^* = -i + (k+1)qv$. Now we have

$$\frac{kp}{n} < i < \frac{(k+1)p}{n};\ \frac{(k+1)p}{n} < i^* < \frac{kp}{n} + qv.$$

This provides qv successive natural numbers, hence we have $v = \frac{p+m}{qn}$ exemplars of full residue systems modulo q. If $k = 0$, then the terms A_0 and A_{qv} will be missing. Since $A_0 = A_{qv} = 0$, the congruence will hold for $k = 0$ as well. For $k = \frac{n-1}{2}$, by the same method we get $\frac{p+m}{2qn}$ exemplars of the full residue system modulo q. Summing the congruences we get the required congruence. The same procedure applies for n even. Lemma 3 is proved. $\square$

In the formula for d_r, there is the sum

$$\sum_{i=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+\left[\frac{ni}{m}\right]}.$$

We shall prove that

$$\sum_{i=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-ni}{m}+\left[\frac{ni}{m}\right]} \equiv \sum_{i=1}^{\frac{m-1}{2}} X_i X_{\phi_{m,n}(i)} \pmod q,$$

for $X_i = A_{\frac{-i}{m}}$, for $i = 1, 2, \dots, \frac{m-1}{2}$.

Clearly

$$\frac{-ni}{m} + \left[\frac{ni}{m}\right] \equiv \frac{-1}{m}\left(ni - m\left[\frac{ni}{m}\right]\right) \pmod q.$$

The number $ni - m\left[\frac{ni}{m}\right]$ is equal to the residuum ni modulo m. It follows that if $ni - m\left[\frac{ni}{m}\right] < \frac{m}{2}$, then $ni - m\left[\frac{ni}{m}\right] = \phi_{m,n}(i)$. If $ni - m\left[\frac{ni}{m}\right] > \frac{m}{2}$, then $ni - m\left[\frac{ni}{m}\right] = m - \phi_{m,n}(i)$.

Consider the numbers

$$A_{-\frac{\phi_{m,n}(i)}{m}} \text{ resp. } A_{\frac{-1}{m}(m-\phi_{m,n}(i))}.$$

Since

$$\frac{-1}{m}\phi_{m,n}(i) + \frac{-1}{m}(m - \phi_{m,n}(i)) = -1,$$

there holds

$$A_{-\frac{\phi_{m,n}(i)}{m}} \equiv A_{\frac{-1}{m}(m-\phi_{m,n}(i))} \pmod q,$$

which implies the required relation.

Now we shall express the coefficient d_0 corresponding to the value $n = 1$. The substitution into (3) gives

$$d_0 = \frac{p+m}{2q}\sum_{i=1}^{q-1} A_i^2 - \sum_{i=1}^{\frac{m-1}{2}} A^2_{\frac{-i}{m}}.$$

If $q|h^+$, then $d_0 \equiv d_r \pmod q$ and hence for $n \equiv 1 \pmod 2$ there holds:

$$\frac{p+m}{qn}\left(\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}} + \sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+1} + \cdots + \sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+\frac{n-3}{2}} + \frac{1}{2}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+\frac{n-1}{2}}\right)$$

$$-\sum_{i=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}}A_{\frac{-\phi_{m,n}(i)}{m}} \equiv \frac{p+m}{2q}\sum_{i=1}^{q-1} A_i^2 - \sum_{i=1}^{\frac{m-1}{2}} A^2_{\frac{-i}{m}} \pmod q.$$

It is easy to prove that $\sum_{i=1}^{q-1} A_i^2 \equiv -2 \pmod q$. Therefore

$$\frac{p+m}{q}\left(\frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}} + \frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+1} + \cdots + \frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+\frac{n-3}{2}} + \frac{1}{2n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+\frac{n-1}{2}} + 1\right)$$

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

where $t = \frac{m-1}{2}$.

By [8] (proof of Theorem 1), the following holds:

$$\frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}} + \frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+1} + \cdots + \frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+\frac{n-3}{2}} + \frac{1}{2n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+\frac{n-1}{2}} + 1$$

$$\equiv -\frac{1}{2}\frac{n^{q-1}-1}{q} \pmod q.$$

The congruence (i) is now proved for $n \equiv 1 \pmod 2$. Analogically, the congruence (i) can be proved for $n \equiv 0 \pmod 2$, on the basis of the congruence

$$\frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}} + \frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+1} + \cdots + \frac{1}{n}\sum_{i=1}^{q-1} A_{\frac{i}{m}}A_{\frac{ni}{m}+\frac{n}{2}-1} + 1$$

$$\equiv -\frac{1}{2}\frac{n^{q-1}-1}{q} \pmod q.$$

Now we shall prove the congruence (ii). Substituting nq, where $nq|\frac{p+m}{q}$, instead of n into the formula for the computation d_r, we get for $n \equiv 1 \pmod 2$ the following sum:

$$A_1(A_1 + A_2 + \cdots + A_{q-1}) + A_2(A_1 + A_2 + \cdots + A_{q-1}) \\ + \cdots + \frac{1}{2}A_{\frac{nq-1}{2}}(A_1 + A_2 + \cdots + A_{q-1}).$$

It is easy to see that $A_1 + A_2 + \cdots + A_{q-1} \equiv 1 \pmod q$, therefore

$$A_1(A_1 + A_2 + \cdots + A_{q-1}) + A_2(A_1 + A_2 + \cdots + A_{q-1}) \\ + \cdots + \frac{1}{2}A_{\frac{nq-1}{2}}(A_1 + A_2 + \cdots + A_{q-1}) \equiv \frac{n}{2} \pmod q.$$

Analogously for $n \equiv 0 \pmod 2$ we get

$$A_1(A_1 + A_2 + \cdots + A_{q-1}) + A_2(A_1 + A_2 + \cdots + A_{q-1}) \\ + \cdots + A_{\frac{nq}{2}-1} \equiv \frac{n}{2} \pmod q.$$

Theorem 1 is proved. □

We shall show 12 corollaries of Theorem 1.

Corollary 1. *Let q be an odd prime. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, $p \equiv -3 \pmod q$, $p \not\equiv -3 \pmod{q^3}$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then $2^{q-1} \equiv 1 \pmod{q^2}$.*

Proof. By Theorem 1, (i) putting $n = 2$ we have

$$\frac{p+3}{2q}\frac{2^{q-1}-1}{q} \equiv Q_{3,2}(A_{\frac{-1}{3}}) \pmod q.$$

Clearly $Q_{3,2}(X_1) = 0$, hence

$$\frac{p+3}{2q}\frac{2^{q-1}-1}{q} \equiv 0 \pmod q.$$

If $\frac{p+3}{2q} \not\equiv 0 \pmod q$, then $\frac{2^{q-1}-1}{q} \equiv 0 \pmod q$. Suppose that $q|\frac{p+3}{q}$. By Theorem 1, (ii) we have

$$-\frac{p+3}{2q^2} \equiv Q_{3,q}(A_{\frac{-1}{3}}) \equiv 0 \pmod q,$$

hence $p + 3 \equiv 0 \pmod{q^3}$—a contradiction. □

Corollary 2. *Let q be an odd prime. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, $p \equiv -5 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*

$$F_{q-\left(\frac{5}{q}\right)} \equiv 0 \pmod{q^2},$$

where F_n is the nth Fibonacci number ($F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ for $0 \le n$).

Moreover, if $p \not\equiv -5 \pmod{q^3}$, then $2^{q-1} \equiv 1 \pmod{q^2}$.

Proof. The number $p+5$ has the divisors $n = 2, 4$. Therefore by Theorem 1 (i)

$$\frac{p+5}{2q}\frac{2^{q-1}-1}{q} \equiv Q_{5,2}(A_{\frac{-1}{5}}, A_{\frac{-2}{5}}) \pmod q,$$

$$\frac{p+5}{2q}\frac{4^{q-1}-1}{q} \equiv Q_{5,4}(A_{\frac{-1}{5}}, A_{\frac{-2}{5}}) \pmod q.$$

Clearly

$$\phi_{5,2} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \ \phi_{5,4} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}.$$

Hence

$$Q_{5,2}(X_1, X_2) = X_1^2 + X_2^2 - 2X_1X_2 = (X_1 - X_2)^2, \ Q_{5,4}(X_1, X_2) = 0.$$

It is easy to see that

$$(A_{\frac{-1}{5}} - A_{\frac{-2}{5}})^2 \equiv \left(\sum_{\frac{q}{5}<i<\frac{2q}{5}} \frac{1}{i} \right)^2 \pmod q.$$

Therefore

$$\frac{p+5}{2q}\frac{2^{q-1}-1}{q} \equiv \left(\sum_{\frac{q}{5}<i<\frac{2q}{5}} \frac{1}{i} \right)^2 \pmod q,$$

$$\frac{p+5}{2q}\frac{4^{q-1}-1}{q} \equiv 0 \pmod q.$$

Because $\frac{2^{q-1}-1}{q} \equiv 0 \pmod q$ if and only if $\frac{4^{q-1}-1}{q} \equiv 0 \pmod q$, we get that if $q|h^+$, then

$$\sum_{\frac{q}{5}<i<\frac{2q}{5}} \frac{1}{i} \equiv 0 \pmod q.$$

By [11], for $q > 5$ there holds

$$\frac{2}{5} \sum_{\frac{q}{5}<i<\frac{2q}{5}} \frac{1}{i} \equiv \frac{1}{q} F_{q-\left(\frac{5}{q}\right)} \pmod q,$$

which proves the first assertion of Corollary 2.

If $\frac{2^{q-1}-1}{q} \not\equiv 0 \pmod q$, then $\frac{p+5}{2q^2} \equiv 0 \pmod q$. By (ii) we get $\frac{p+5}{2q^2} \equiv 0 \pmod q$—a contradiction. □

Remark. P.L. Montgomery [9] reports no solution of $F_{q-\left(\frac{5}{q}\right)} \equiv 0 \pmod{q^2}$ with $q < 2^{32}$.

Corollary 3. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -7 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*

$$(*) \quad \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i} \right)^2 + \left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i} \right)^2 + \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i} \right) \left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i} \right) \equiv 0 \pmod q.$$

Moreover, if $p \not\equiv -7 \pmod{q^3}$, *then* $2^{q-1} \equiv 3^{q-1} \equiv 1 \pmod{q^2}$.

Proof. The number $p+7$ has the divisors $n = 2, 3, 6$. By Theorem 1 (i) the following holds

$$\frac{p+7}{2q}\frac{2^{q-1}-1}{q} \equiv Q_{7,2}(A_{\frac{-1}{7}}, A_{\frac{-2}{7}}, A_{\frac{-3}{7}}) \pmod{q},$$

$$\frac{p+7}{2q}\frac{3^{q-1}-1}{q} \equiv Q_{7,3}(A_{\frac{-1}{7}}, A_{\frac{-2}{7}}, A_{\frac{-3}{7}}) \pmod{q},$$

$$\frac{p+7}{2q}\frac{6^{q-1}-1}{q} \equiv Q_{7,6}(A_{\frac{-1}{7}}, A_{\frac{-2}{7}}, A_{\frac{-3}{7}}) \pmod{q}.$$

Clearly

$$\phi_{7,2} = \phi_{7,3} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \; \phi_{7,6} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Hence

$$Q_{7,2}(X_1, X_2, X_3) = Q_{7,3}(X_1, X_2, X_3), \;\; Q_{7,6}(X_1, X_2, X_3) = 0.$$

By rearrangement we get

$$Q_{7,2}(A_{\frac{-1}{7}}, A_{\frac{-2}{7}}, A_{\frac{-3}{7}})$$

$$\equiv \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)\left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right) \pmod{q},$$

Therefore we have

$$\frac{p+7}{2q}\frac{2^{q-1}-1}{q}$$

$$\equiv \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)\left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right) \pmod{q},$$

$$\frac{p+7}{2q}\frac{3^{q-1}-1}{q}$$

$$\equiv \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)\left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right) \pmod{q},$$

$$\frac{p+7}{2q}\frac{6^{q-1}-1}{q} \equiv 0 \pmod{q}.$$

If

$$\left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)\left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right) \not\equiv 0 \pmod{q},$$

then $\frac{p+7}{2q} \not\equiv 0 \pmod q$, $\frac{6^{q-1}-1}{q} \equiv 0 \pmod q$ and $\frac{2^{q-1}-1}{q} \equiv \frac{3^{q-1}-1}{q} \pmod q$ and $\frac{2^{q-1}-1}{q} \not\equiv 0 \pmod q$. This easily yields a contradiction.

If

$$\left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i}\right)\left(\sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i}\right) \equiv 0 \pmod q,$$

and $\frac{p+7}{2q} \not\equiv 0 \pmod q$, then

$$2^{q-1} \equiv 3^{q-1} \equiv 1 \pmod{q^2}.$$

If $\frac{p+7}{2q} \equiv 0 \pmod q$, then by Theorem 1 (ii) $\frac{p+7}{2q^2} \equiv 0 \pmod q$ and therefore $p \equiv -7 \pmod{q^3}$—a contradiction. □

Corollary 4. *Let q be an odd prime, $q \equiv 2 \pmod 3$. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -7 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*

$$\sum_{\frac{q}{7}<i<\frac{2q}{7}} \frac{1}{i} \equiv \sum_{\frac{2q}{7}<i<\frac{3q}{7}} \frac{1}{i} \equiv 0 \pmod q.$$

Proof. The left side of the congruence (*) can be expressed as the norm of the field $\mathbf{Q}(\zeta_3)$ into $\mathbf{Q}$. If $q \equiv 2 \pmod 3$, then q does not decompose in the field $\mathbf{Q}(\zeta_3)$, and it implies the assertion of Corollary 4. □

By [3] there holds: For $1 \le a \le 6$, and any odd prime $q \ne 7$,

$$B_{q-1}\left(\frac{a}{7}\right) - B_{q-1} \equiv \frac{7}{2q}(U_q(7,a,b) - 1) \pmod q,$$

where $b = 1, 2$ or 3 with $b \equiv \pm q \pmod 7$, and U_n satisfies the recurrence relation

$$U_{n+3} = 7U_{n+2} - 14U_{n+1} + 7U_n.$$

The values of U_1, U_2, U_3 are given in the table below

$\pm a$	$\pm b$	U_1	U_2	U_3
2	1	1	2	5
3	2	2	7	26
1	3	2	6	19
3	1	1	2	6
1	2	3	11	41
2	3	2	5	13
a	a	1	3	10

From Corollary 4 and the just mentioned result we get:

Corollary 5. *Let q be an odd prime, $b \equiv \pm q \pmod 7$ where $b = 1, 2$ or 3 and $q \equiv 2 \pmod 3$. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, $p \equiv -7 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*

$$U_q(7,1,b) \equiv U_q(7,2,b) \equiv U_q(7,3,b) \pmod{q^2}.$$

Corollary 6. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -9 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*

$$\left(\sum_{\frac{q}{9}<i<\frac{2q}{9}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{2q}{9}<i<\frac{4q}{9}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{q}{9}<i<\frac{2q}{9}} \frac{1}{i}\right)\left(\sum_{\frac{2q}{q}<i<\frac{4q}{9}} \frac{1}{i}\right) \equiv 0 \pmod q.$$

Moreover, if $p \not\equiv -9 \pmod{q^3}$, then $2^{q-1} \equiv 1 \pmod{q^2}$.

Proof. The number $p+9$ has the divisors $n = 2, 4, 8$, which follows from $p + 9 = 2l + 10 = 2(l+5) = 2(4k+3+5) = 8(k+2)$. Therefore, we have

$$\phi_{9,2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \ \phi_{9,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \ \phi_{9,8} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Hence

$$\begin{aligned} Q_{9,2}(X_1X_2, X_3, X_4) &= Q_{9,4}(X_1X_2, X_3, X_4) \\ &= X_1^2 + X_2^2 + X_4^2 - (X_1X_2 + X_1X_4 + X_2X_4), \end{aligned}$$

and

$$Q_{9,8}(X_1X_2, X_3, X_4) = 0.$$

By rearrangement we get

$$Q_{9,2}(A_{\frac{-1}{9}}, A_{\frac{-2}{9}}, A_{\frac{-3}{9}}, A_{\frac{-4}{9}})$$

$$\equiv \left(\sum_{\frac{q}{9}<i<\frac{2q}{9}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{2q}{9}<i<\frac{4q}{9}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{q}{9}<i<\frac{2q}{9}} \frac{1}{i}\right)\left(\sum_{\frac{2q}{q}<i<\frac{4q}{9}} \frac{1}{i}\right) \pmod q.$$

The rest of the proof is the same as in the case of Corollary 3. □

To prove the remaining corollaries, the following fact will be used.

1. If $n \equiv \pm 1 \pmod m$, then the permutation $\phi_{m,n}$ is identical and therefore $Q_{m,n}(X_1, X_2, \ldots, X_{\frac{m-1}{2}}) = 0$.

2. If $n_1 n_2 \equiv \pm 1 \pmod m$, then the permutations ϕ_{m,n_1}, ϕ_{m,n_2} are inverse and therefore

$$Q_{m,n_1}(X_1, X_2, \ldots, X_{\frac{m-1}{2}}) = Q_{m,n_2}(X_1, X_2, \ldots, X_{\frac{m-1}{2}}).$$

Corollary 7. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -13 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*

$$\begin{aligned} &Q_{13,2}(A_{\frac{-1}{13}}, A_{\frac{-2}{13}}, A_{\frac{-3}{13}}, A_{\frac{-4}{13}}, A_{\frac{-5}{13}}, A_{\frac{-6}{13}}) \\ &\quad \equiv Q_{13,3}(A_{\frac{-1}{13}}, A_{\frac{-2}{13}}, A_{\frac{-3}{13}}, A_{\frac{-4}{13}}, A_{\frac{-5}{13}}, A_{\frac{-6}{13}}) \equiv 0 \pmod q. \end{aligned}$$

Moreover, if $p \not\equiv -13 \pmod{q^3}$, then

$$2^{q-1} \equiv 3^{q-1} \equiv 1 \pmod{q^2}.$$

Proof. The number $p+13$ has the divisors $n=2,3,4,6,12$. By Theorem 1 (i) we have

$$\frac{p+13}{2q}\frac{2^{q-1}-1}{q} \equiv Q_{13,2}(A_{\frac{-1}{13}},A_{\frac{-2}{13}},A_{\frac{-3}{13}},A_{\frac{-4}{13}},A_{\frac{-5}{13}},A_{\frac{-6}{13}}) \pmod q,$$

$$\frac{p+13}{2q}\frac{3^{q-1}-1}{q} \equiv Q_{13,3}(A_{\frac{-1}{13}},A_{\frac{-2}{13}},A_{\frac{-3}{13}},A_{\frac{-4}{13}},A_{\frac{-5}{13}},A_{\frac{-6}{13}}) \pmod q,$$

$$\frac{p+13}{2q}\frac{4^{q-1}-1}{q} \equiv Q_{13,3}(A_{\frac{-1}{13}},A_{\frac{-2}{13}},A_{\frac{-3}{13}},A_{\frac{-4}{13}},A_{\frac{-5}{13}},A_{\frac{-6}{13}}) \pmod q,$$

$$\frac{p+13}{2q}\frac{6^{q-1}-1}{q} \equiv Q_{13,2}(A_{\frac{-1}{13}},A_{\frac{-2}{13}},A_{\frac{-3}{13}},A_{\frac{-4}{13}},A_{\frac{-5}{13}},A_{\frac{-6}{13}}) \pmod q,$$

$$\frac{p+13}{2q}\frac{12^{q-1}-1}{q} \equiv 0 \pmod q.$$

If either

$$Q_{13,2}(A_{\frac{-1}{13}},A_{\frac{-2}{13}},A_{\frac{-3}{13}},A_{\frac{-4}{13}},A_{\frac{-5}{13}},A_{\frac{-6}{13}}) \not\equiv 0 \pmod q$$

or

$$Q_{13,3}(A_{\frac{-1}{13}},A_{\frac{-2}{13}},A_{\frac{-3}{13}},A_{\frac{-4}{13}},A_{\frac{-5}{13}},A_{\frac{-6}{13}}) \not\equiv 0 \pmod q,$$

then $\frac{p+13}{2q} \not\equiv 0 \pmod q$, hence $\frac{12^{q-1}-1}{q} \equiv 0 \pmod q$ and this yields a contradiction. □

Corollary 8. *Let q be an odd prime. Let l,p be primes such that $p=2l+1$, $l\equiv 3 \pmod 4$, $p\equiv -17 \pmod q$ 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 $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$. Then*

$$Q_{17,2}(A_{\frac{-1}{17}},A_{\frac{-2}{17}},A_{\frac{-3}{17}},A_{\frac{-4}{17}},A_{\frac{-5}{17}},A_{\frac{-6}{17}},A_{\frac{-7}{17}},A_{\frac{-8}{17}})$$

$$\equiv Q_{17,4}(A_{\frac{-1}{17}},A_{\frac{-2}{17}},A_{\frac{-3}{17}},A_{\frac{-4}{17}},A_{\frac{-5}{17}},A_{\frac{-6}{17}},A_{\frac{-7}{17}},A_{\frac{-8}{17}}) \equiv 0 \pmod q.$$

Moreover, if $p\not\equiv -17 \pmod{q^2}$, then $2^{q-1}\equiv 1 \pmod{q^2}$.

Proof. The number $p+17$ has the divisors $n=2,4,8$. By Theorem 1 (i) we have

$$\frac{p+17}{2q}\frac{2^{q-1}-1}{q} \equiv Q_{17,2}(A_{\frac{-1}{17}},A_{\frac{-2}{17}},A_{\frac{-3}{17}},A_{\frac{-4}{17}},A_{\frac{-5}{17}},A_{\frac{-6}{17}},A_{\frac{-7}{17}},A_{\frac{-8}{17}}) \pmod q,$$

$$\frac{p+17}{2q}\frac{4^{q-1}-1}{q} \equiv Q_{17,4}(A_{\frac{-1}{17}},A_{\frac{-2}{17}},A_{\frac{-3}{17}},A_{\frac{-4}{17}},A_{\frac{-5}{17}},A_{\frac{-6}{17}},A_{\frac{-7}{17}},A_{\frac{-8}{17}}) \pmod q,$$

$$\frac{p+17}{2q}\frac{8^{q-1}-1}{q} \equiv Q_{17,2}(A_{\frac{-1}{17}},A_{\frac{-2}{17}},A_{\frac{-3}{17}},A_{\frac{-4}{17}},A_{\frac{-5}{17}},A_{\frac{-6}{17}},A_{\frac{-7}{17}},A_{\frac{-8}{17}}) \pmod q.$$

If either $Q_{17,2} \not\equiv 0 \pmod q$ or $Q_{17,4} \not\equiv 0 \pmod q$, then $\frac{p+17}{2q} \not\equiv 0 \pmod q$ and $\frac{2^{q-1}-1}{q} \not\equiv 0 \pmod q$. The first and the third congruence imply that

$$\frac{2^{q-1}-1}{q} \equiv \frac{8^{q-1}-1}{q} \pmod q,$$

therefore $\frac{2^{q-1}-1}{q} \equiv 0 \pmod q$—a contradiction. □

From now on, the function values of quadratic forms will be omitted, i.e., instead of $Q_{19,2}(....)$ we shall write $Q_{19,2}$.

Corollary 9. *Let q be an odd prime. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, $p \equiv -19 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then $Q_{19,2} \equiv 0 \pmod q$. If $Q_{19,3} \not\equiv 0 \pmod q$, then $2^{q-1} \equiv 1 \pmod{q^2}$. Moreover, if $p \not\equiv -19 \pmod{q^2}$, then $2^{q-1} \equiv 1 \pmod{q^2}$.*

Proof. The number $p + 19$ has the divisors $n = 2, 3, 6$. Hence

$$\frac{p+19}{2q}\frac{2^{q-1}-1}{q} \equiv Q_{19,2} \pmod q,$$

$$\frac{p+19}{2q}\frac{3^{q-1}-1}{q} \equiv Q_{19,3} \pmod q,$$

$$\frac{p+19}{2q}\frac{6^{q-1}-1}{q} \equiv Q_{19,3} \pmod q.$$

If $Q_{19,2} \not\equiv 0 \pmod q$, then $\frac{2^{q-1}-1}{q} \not\equiv 0 \pmod q$. The second and the third congruence imply that

$$\frac{3^{q-1}-1}{q} \equiv \frac{6^{q-1}-1}{q} \pmod q,$$

which is not possible, because $\frac{2^{q-1}-1}{q} \not\equiv 0 \pmod q$. If $Q_{19,3} \not\equiv 0 \pmod q$, then

$$\frac{3^{q-1}-1}{q} \equiv \frac{6^{q-1}-1}{q} \pmod q,$$

and it follows that $2^{q-1} \equiv 1 \pmod{q^2}$. □

Corollary 10. *Let q be an odd prime. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, $p \equiv -25 \pmod q$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*

$$Q_{25,2} \equiv Q_{25,3} \equiv Q_{25,4} \equiv 0 \pmod q.$$

Moreover, if $p \not\equiv -25 \pmod{q^3}$, then $2^{q-1} \equiv 3^{q-1} \equiv 1 \pmod{q^2}$.

The proof is analogous as for $p \equiv -13 \pmod q$.

Corollary 11. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -m \pmod q$, $p \not\equiv -m \pmod{q^2}$, $m > 0$, $m \equiv 1 \pmod 2$ and let the order of the prime q modulo l be $\frac{l-1}{2}$. Suppose that there exist divisors n_1, n_2 of the number $p + m$ such that $n_1 n_2 \equiv \pm 1 \pmod m$ or $n_1 \equiv \pm n_2 \pmod m$. If $q | h^+$, then*

$$n_1^{q-1} \equiv n_2^{q-1} \pmod{q^2}.$$

Proof. Since $n_1n_2 \equiv \pm 1 \pmod{m}$ or $n_1 \equiv \pm n_2 \pmod{m}$, we have

$$Q_{m,n_1}(X_1, X_2, \dots, X_{\frac{m-1}{2}}) \equiv Q_{m,n_2}(X_1, X_2, \dots, X_{\frac{m-1}{2}}) \pmod{q},$$

and hence

$$\frac{p+m}{2q}\frac{n_1^{q-1}-1}{q} \equiv \frac{p+m}{2q}\frac{n_1^{q-1}-1}{q} \pmod{q}.$$

The Corollary now follows from $\frac{p+m}{2q} \not\equiv 0 \pmod{q}$. □

Corollary 12. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod{4}$, $p \equiv -m \pmod{q}$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then for arbitrary n_1, n_2 such that $n_1n_2|p+m$, $(n_1n_2, q) = 1$, the following congruence holds.*

$$Q_{m,n_1n_2}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{-\frac{t}{m}})$$

$$\equiv Q_{m,n_1}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{-\frac{t}{m}}) + Q_{m,n_2}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{-\frac{t}{m}}) \pmod{q},$$

where $t = \frac{m-1}{2}$.

Proof. Since $\frac{(n_1n_2)^{q-1}-1}{q} \equiv \frac{n_1^{q-1}-1}{q} + \frac{n_2^{q-1}-1}{q} \pmod{q}$, the preceding congruence implies Theorem 1 (i). □

The following example shows the possibility of applying the congruence of Corollary 12 in order to find out the divisibility of the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.

Example 1. Let $p \equiv -11 \pmod{43}$. If $p \not\equiv \pm 2 \pmod{11}$, then 43 does not divide the class number h^+. If $p \equiv \pm 2 \pmod{11}$ and $43|h^+$, then

$$p + 11 = 2.43^s.p_1^{s_1}p_2^{s_2}\dots p_n^{s_n},$$

where $p_i \equiv \pm 1 \pmod{11}$, for $i = 1, 2, \dots, n$.

Proof. Let $43^s|p+11$ and 43^{s+1} does not divide $p+11$, where $1 \le s$. Put $n_1 = \frac{p+11}{2.43^s}$, $n_2 = 2$. Then it holds:

$$Q_{11,2n_1}(A_{39}, A_{35}, A_{31}, A_{27}, A_{23})$$

$$\equiv Q_{11,n_1}(A_{39}, A_{35}, A_{31}, A_{27}, A_{23}) + Q_{11,2}(A_{39}, A_{35}, A_{31}, A_{27}, A_{23}) \pmod{43}.$$

In the following we shall write quadratic forms without arguments. Because $43 \equiv -1 \pmod{11}$ we have $2n_1 = \frac{p+11}{43^s} \equiv \pm p \pmod{11}$. Because $Q_{m,n} = Q_{m,-n}$, it is enough to consider the cases $p \equiv 1, 2, 3, 4, 5 \pmod{11}$.

1) $p \equiv 1 \pmod{11}$, then $Q_{11,1} = 0 \equiv Q_{11,\frac{1}{2}} + Q_{11,2} \pmod{43}$. From $Q_{11,\frac{1}{2}} = Q_{11,2}$ we have $Q_{11,2} \equiv 0 \pmod{43}$.

2) $p \equiv 2 \pmod{11}$, then $Q_{11,2} \equiv Q_{11,1} + Q_{11,2} \pmod{43}$, hence in this case we do not have any information, as $Q_{11,1} = 0$.

3) $p \equiv 3 \pmod{11}$, hence $Q_{11,3} \equiv Q_{11,\frac{3}{2}} + Q_{11,2} \pmod{43}$, $\frac{3}{2} \equiv 7 \pmod{11}$, $3.7 \equiv -1 \pmod{11}$ therefore $Q_{11,\frac{3}{2}} = Q_{11,3}$ and we get that $Q_{11,2} \equiv 0 \pmod{43}$.

4) $p \equiv 4 \pmod{11}$, then analogically as in the preceding cases we get the congruence $Q_{11,3} \equiv 2Q_{11,2} \pmod{43}$.

5) $p \equiv 5 \pmod{11}$, then we get $Q_{11,3} \equiv 0 \pmod{43}$.

By substituting $A_{39}, A_{35}, A_{31}, A_{27}, A_{23}$ we have $Q_{11,2}(A_{39}, A_{35}, A_{31}, A_{27}, A_{23}) \equiv Q_{11,2}(9, 33, 15, 20, 10) \equiv 11 \pmod{43}$ and $Q_{11,3}(9, 33, 15, 20, 10) \equiv 39 \pmod{43}$.

Hence $Q_{11,2} \not\equiv 0 \pmod{43}$, $Q_{11,3} \not\equiv 0 \pmod{43}$, and $Q_{11,3} \not\equiv 2Q_{11,2} \pmod{43}$. By this we proved that if $p \not\equiv \pm 2 \pmod{11}$, then 43 does not divide h^+.

The preceding calculations show that if $p+11$ had another divisor than 2 different from $\pm 1 \pmod{11}$, then 43 would not divide h^+. Therefore $p + 11$ must have the above mentioned form. □

Throughout the rest of the paper, we shall consider the divisibility of h^+ by the concrete primes $q = 7, 11, 13, 17, 19, 23$. Theorem 1 and its corollaries would not sufficiently solve this task. The reason is that for some m (e.g. $m = 11$), only one suitable divisor of $p + m$ is known, namely $n = 2$.

In what follows, B_j resp. $B_j(X)$ will denote a Bernoulli number resp. a Bernoulli polynomial.

Theorem 2. *Let q be an odd prime. Let l, p be primes such that $p = 2l + 1$; $l \equiv 3 \pmod{4}$, $p \equiv -m \pmod{q}$, for $m = 1, 3, 5, \dots 2q - 3$, $m \equiv 0, 2 \pmod{3}$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then the following holds:*

I. $m \equiv 0 \pmod{3}$.

(i) *if* $q \equiv 1 \pmod{3}$, *then*

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} + \frac{1}{9}B_{q-2}\left(\frac{1}{3}\right) \equiv C_m \pmod{q}.$$

(ii) *if* $q \equiv 2 \pmod{3}$, $m + 2 < q$, *then*

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} + \frac{2}{9}B_{q-2}\left(\frac{1}{3}\right) \equiv C_m \pmod{q}.$$

(iii) *if* $q \equiv 2 \pmod{3}$ *and* $m + 2 \geq q$, *then*

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} - \frac{1}{9}B_{q-2}\left(\frac{1}{3}\right) \equiv C_m \pmod{q}.$$

II. $m \equiv 2 \pmod{3}$

(i) *if* $q \equiv 2 \pmod{3}$, *then*

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} + \frac{1}{9}B_{q-2}\left(\frac{1}{3}\right) \equiv C_m \pmod{q}.$$

(ii) *if* $q \equiv 1 \pmod{3}$, $m + 2 < q$, *then*

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} + \frac{2}{9}B_{q-2}\left(\frac{1}{3}\right) \equiv C_m \pmod{q}.$$

(iii) *if* $q \equiv 1 \pmod{3}$, $m + 2 \geq q$, *then*

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} - \frac{1}{9}B_{q-2}\left(\frac{1}{3}\right) \equiv C_m \pmod{q},$$

where

$$C_m = \sum_{i=1}^{\frac{m-1}{2}} A^2_{\frac{-i}{m}} - \sum_{i=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-3i}{m}+1} + \sum_{\substack{i=1 \\ 3i \not\equiv m \pmod{q}}}^{k-1} \frac{1}{\frac{-3i}{m}+1} A_{\frac{-i}{m}},$$

and $k \equiv \frac{m+2}{3} \pmod{q}$, $0 \leq k < q$.

Proof. By Lemma 2, for the coefficient d_r, where $g^r \equiv \pm 3 \pmod p$, we get

$$d_r \doteq \sum_{0<i<\frac{p}{3}} A_{\frac{i}{m}} A_{\frac{3i}{m}} + \sum_{\frac{p}{3}<i<\frac{p}{2}} A_{\frac{i}{m}} A_{\frac{3i}{m}+1}.$$

Then we proceed similarly as in the proof of Lemma 3. The corresponding congruence will be obtained from the fact that $q|h^+$ implies $d_0 \equiv d_r \pmod q$, using the following results of [8]. $\square$

Theorem 3. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -m \pmod q$, for $m = 1, 3, 5, \dots 2q-3$, $m \equiv 0, 2 \pmod 3$ 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then the following holds:*

(i) $m \equiv 0 \pmod 3$, $q \equiv 1 \pmod 3$, *then*

$$\frac{p+m+4q}{2q}\frac{3^{q-1}-1}{q} \equiv Q_{m+4q,3}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{-\frac{t}{m}}) \pmod q,$$

where $t = \frac{4q+m-1}{2}$.

(ii) $m \equiv 0 \pmod 3$, $q \equiv 2 \pmod 3$, *then*

$$\frac{p+m+2q}{2q}\frac{3^{q-1}-1}{q} \equiv Q_{m+2q,3}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{-\frac{t}{m}}) \pmod q,$$

where $t = \frac{2q+m-1}{2}$.

(iii) $m \equiv 2 \pmod 3$, $q \equiv 1 \pmod 3$, *then*

$$\frac{p+m+2q}{2q}\frac{3^{q-1}-1}{q} \equiv Q_{m+2q,3}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{-\frac{t}{m}}) \pmod q,$$

where $t = \frac{2q+m-1}{2}$.

(iv) $m \equiv 2 \pmod 3$, $q \equiv 2 \pmod 3$, *then*

$$\frac{p+m+4q}{2q}\frac{3^{q-1}-1}{q} \equiv Q_{m+4q,3}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{-\frac{t}{m}}) \pmod q,$$

where $t = \frac{4q+m-1}{2}$.

Proof. (i) If $m \equiv 0 \pmod 3$ and $q \equiv 1 \pmod 3$, then because $p \equiv 2 \pmod 3$ we have $p+m+4q \equiv 0 \pmod 3$ and the assertion (i) follows from Theorem 1 (i). Further we proceed analogously. $\square$

Lemma 2 of [8]**.** *Let n, k be integers such that $nk \not\equiv 0 \pmod q$. Then*

$$\sum_{\substack{i=1 \\ ni \not\equiv -k \pmod q}}^{q-1} \frac{A_i}{ni+k} \equiv \frac{1}{n} B_{q-2}\left(\frac{k}{n}\right) \pmod q.$$

Lemma 3 of [8]**.** *Let n be an odd number. Then*

$$\sum_{i=1}^{q-1} A_i A_{ni} \equiv \frac{-1}{n^2}(n-2)B_{q-2}\left(\frac{1}{n}\right) + \frac{-1}{n^2}(n-4)B_{q-2}\left(\frac{2}{n}\right) + \dots + \frac{-1}{n^2}B_{q-2}\left(\frac{\frac{n-1}{2}}{n}\right) - 2 - \frac{n^{q-1}-1}{q} \pmod q.$$

By Lemma 2 of [8] we get

$$\sum_{i=1}^{q-1} A_i A_{ni+1} \equiv \sum_{i=1}^{q-1} A_i A_{ni} + \frac{1}{n} B_{q-2}\left(\frac{1}{n}\right) \pmod{q},$$

$$\sum_{i=1}^{q-1} A_i A_{ni+2} \equiv \sum_{i=1}^{q-1} A_i A_{ni} + \frac{1}{n} B_{q-2}\left(\frac{1}{n}\right) + \frac{1}{n} B_{q-2}\left(\frac{2}{n}\right) \pmod{q},$$

$$\vdots$$

$$\begin{aligned}\sum_{i=1}^{q-1} A_i A_{ni+\frac{n-1}{2}} \equiv &\sum_{i=1}^{q-1} A_i A_{ni} + \frac{1}{n} B_{q-2}\left(\frac{1}{n}\right) + \frac{1}{n} B_{q-2}\left(\frac{2}{n}\right) \\ &+ \cdots + \frac{1}{n} B_{q-2}\left(\frac{\frac{n-1}{2}}{n}\right) \pmod{q}.\end{aligned}$$

Theorem 4. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -m \pmod q$, for $m = 1, 3, 5, \ldots, 2q-3$, $m \equiv 3 \pmod 4$, 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 $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then the following holds:*

(i) *if $\frac{m+3}{2} < q$, then*

$$\frac{p+m}{2q}\frac{4^{q-1}-1}{q} - \frac{1}{8} B_{q-2}\left(\frac{1}{4}\right) \equiv C_m \pmod{q}.$$

(ii) *if $\frac{m+3}{2} \geq q$, then*

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} + \frac{1}{8} B_{q-2}\left(\frac{1}{4}\right) \equiv C_m \pmod{q},$$

where

$$C_m = \sum_{i=1}^{\frac{m-1}{2}} A^2_{\frac{-i}{m}} - \sum_{i=1}^{\frac{m-1}{2}} A_{\frac{-i}{m}} A_{\frac{-4i}{m}+1} + \sum_{\substack{i=1 \\ 4i \not\equiv m \pmod q}}^{k-1} \frac{1}{\frac{-4i}{m}+1} A_{\frac{-i}{m}},$$

and $k \equiv \frac{m+3}{4} \pmod q$, $0 \leq k < q$.

Proof. Analogous to the proof of Theorem 2. □

To prove that q does not divide h^+ for $p \equiv -1 \pmod q$, the following Theorem 5 will be necessary.

Let j be an integer, $0 < j < 2q$, $j \equiv 0 \pmod 2$. Define the sums

$$S_j = \sum_{i=1}^{\frac{q-1}{2}} A_i \sum_{\substack{k=1 \\ k \equiv 1 \pmod 2 \\ 2ji \not\equiv -k \pmod q}}^{j-1} \frac{1}{2ji+k} - \sum_{i=\frac{q+1}{2}}^{q-1} A_i \sum_{\substack{k=1 \\ k \equiv 1 \pmod 2 \\ 2ji \not\equiv -k \pmod q}}^{j-1} \frac{1}{2ji+k}.$$

Theorem 5. *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 $\frac{l-1}{2}$. Suppose that for each j such that $S_j \equiv 0 \pmod q$ there exists n, $(n, 2q) = 1$, $n | p+1$ such that $S_{j^*} \not\equiv 0 \pmod q$, where $j^* \equiv nj \pmod{2q}$. Then q does not divide h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

Proof. Let $2^v|p+1$ and let 2^{v+1} not divide $p+1$. Let n be a divisor of $p+1$, $(n,2q)=1$. Denote $M=2^{v+1}n$. We shall compute the coefficient d_r, $r<l$ in (2), where $g^r\equiv \pm M \pmod p$. By Lemma 2 we have

$$d_r=\sum_{0<i<\frac{p}{M}} A_iA_{Mi}+\sum_{\frac{p}{M}<i<\frac{2p}{M}} A_iA_{Mi+1}+\dots.$$

It implies that

$$d_r\equiv S+\left(\frac{p+1}{qN}-\frac{1}{2}\right)\sum_{k=0}^{\frac{M}{2}-1}\sum_{i=1}^{q-1}A_iA_{Mi+k} \pmod q,$$

where

$$S=\sum_{i=1}^{\frac{q-1}{2}}A_iA_{Mi}+\sum_{i=\frac{q+1}{2}}^{q-1}A_iA_{Mi+1}+\sum_{i=1}^{\frac{q-1}{2}}A_iA_{Mi+2}+\sum_{i=\frac{q+1}{2}}^{q-1}A_iA_{Mi+3}$$

$$+\dots+\sum_{i=1}^{\frac{q-1}{2}}A_iA_{Mi+\frac{M}{2}-2}+\sum_{i=\frac{q+1}{2}}^{q-1}A_iA_{Mi+\frac{M}{2}-1}.$$

Therefore

$$S=\sum_{k=0}^{\frac{M}{4}-1}\sum_{i=1}^{q-1}A_iA_{Mi+2k}+\sum_{i=\frac{q+1}{2}}^{q-1}A_i\sum_{\substack{k=1\\ k\equiv 1 \pmod 2\\ Mi\not\equiv -k \pmod q}}^{\frac{M}{2}-1}\frac{1}{Mi+k}.$$

By Lemma 2 of [8] and Lemma 3 of [8] we get

$$\sum_{k=0}^{\frac{M}{4}-1}\sum_{i=1}^{q-1}A_iA_{Mi+2k}\equiv -\frac{M}{4}\left(2+\frac{M^{q-1}-1}{q}\right)$$
$$-\frac{1}{2M}\sum_{\substack{k=1\\ k\equiv 1 \pmod 2}}^{\frac{M}{2}-1}B_{q-2}\left(\frac{k}{M}\right) \pmod q.$$

If $q|h^+$ then $d_r\equiv d_0 \pmod q$, hence

$$S+\frac{p+1}{q}\left(1+\frac{1}{M}\sum_{k=0}^{\frac{M}{2}-1}\sum_{i=1}^{q-1}A_iA_{Mi+k}\right)-\frac{1}{2}\sum_{k=0}^{\frac{M}{2}-1}\sum_{i=1}^{q-1}A_iA_{Mi+k}\equiv -\frac{p+1}{q} \pmod q.$$

By [8] we have

$$1+\frac{1}{M}\sum_{k=0}^{\frac{M}{2}-1}\sum_{i=1}^{q-1}A_iA_{Mi+k}\equiv -\frac{1}{2}\frac{M^{q-1}-1}{q} \pmod q.$$

The congruence

$$-\frac{p+1}{2q}\frac{M^{q-1}-1}{q}+\frac{M}{2}\left(\frac{1}{2}\frac{M^{q-1}-1}{q}+1\right)+S\equiv 0 \pmod q.$$

follows.

Substituting for S we get

$$-\frac{p+1}{2q}\frac{M^{q-1}-1}{q}+\sum_{i=\frac{q+1}{2}}^{q-1}A_i\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)\\ Mi\not\equiv -k\ (\mathrm{mod}\ q)}}^{\frac{M}{2}-1}\frac{1}{Mi+k}\equiv\frac{1}{2M}\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)}}^{\frac{M}{2}-1}B_{q-2}\left(\frac{k}{M}\right).$$

By Theorem 1, $q|h^+$ implies that

$$\frac{p+1}{2q}\frac{M^{q-1}-1}{q}\equiv 0 \pmod q.$$

Therefore

$$\sum_{i=\frac{q+1}{2}}^{q-1}A_i\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)\\ Mi\not\equiv -k\ (\mathrm{mod}\ q)}}^{\frac{M}{2}-1}\frac{1}{Mi+k}\equiv\frac{1}{2M}\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)}}^{\frac{M}{2}-1}B_{q-2}\left(\frac{k}{M}\right) \pmod q.$$

By Lemma 2 of [8] and Lemma 3 of [8] we get

$$\sum_{i=\frac{q+1}{2}}^{q-1}A_i\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)\\ Mi\not\equiv -k\ (\mathrm{mod}\ q)}}^{\frac{M}{2}-1}\frac{1}{Mi+k}\equiv\sum_{i=1}^{\frac{q-1}{2}}A_i\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)\\ Mi\not\equiv -k\ (\mathrm{mod}\ q)}}^{\frac{M}{2}-1}\frac{1}{Mi+k} \pmod q. \tag{4}$$

Clearly

$$\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)\\ Mi\not\equiv -k\ (\mathrm{mod}\ q)}}^{2q-1}\frac{1}{Mi+k}\equiv 0 \pmod q.$$

Therefore the congruence (4) can be rewritten as follows

$$\sum_{i=\frac{q+1}{2}}^{q-1}A_i\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)\\ 2ji\not\equiv -k\ (\mathrm{mod}\ q)}}^{j-1}\frac{1}{2ji+k}-\sum_{i=1}^{\frac{q-1}{2}}A_i\sum_{\substack{k=1\\ k\equiv 1\ (\mathrm{mod}\ 2)\\ 2ji\not\equiv -k\ (\mathrm{mod}\ q)}}^{j-1}\frac{1}{2ji+k}\equiv 0 \pmod q,$$

where $j\equiv 2^v n \pmod{2q}$.

Let $2^v|p+1$ and let 2^{v+1} not divide $p+1$. If p runs through all primes of the form $2l+1$, then the numbers $2^v \pmod{2q}$ run through the set $\{j|j=2,4,6,\dots,2q-2\}$. If $S_j\not\equiv 0 \pmod q$ for all $j=2,4,6,\dots,2q-2$, then q does not divide h^+. Let $S_j\equiv 0 \pmod q$ for some j. For this j there exists the corresponding coefficient d_r, $r<l$, where $g^r\equiv \pm 2^{v+1} \pmod p$. Consider the coefficient $d_{r'}$, $r'<l$, where $g^{r'}\equiv \pm 2^{v+1}n \pmod q$, $n|p+1$, $(n,2q)=1$. If $q|h^+$, then $d_r\equiv d_{r'}\equiv d_0 \pmod q$. Hence $S_{j^*}\equiv 0 \pmod q$, where $j^*\equiv nj \pmod{2q}$. Theorem 5 is proved. □

Theorem 6. *Let q be an odd prime. Let l,p be primes such that $p=2l+1$, $l\equiv 3 \pmod 4$, $p\equiv -1 \pmod q$, the order of the prime q modulo l be $\frac{l-1}{2}$ and let the congruence $2^{q-1}\equiv 3^{q-1}\equiv 1 \pmod{q^2}$ not hold.*

Suppose that q divides h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$. Then for each k, $(k,q)=1$, the following congruence holds:

$$k\frac{k^{q-1}-1}{q} \equiv Q_{1+2kq,\frac{p}{2q}}(A_{-1},A_{-2},\dots,A_{-t}) \pmod{q},$$

where $t=kq$.

Proof. By Theorem 1 (i) put $n=\frac{p+1+2kq}{2q}=\frac{p+1}{2q}+k$ If $q|h^+$, then similarly as in the proof of Corollary 1 we get $\frac{p+1}{2q}\equiv 0 \pmod{q^2}$ and hence $n\equiv k \pmod{q^2}$. Clearly $n=\frac{p+1+2kq}{2q}\equiv\frac{p}{2q} \pmod{1+2kq}$ and Theorem 6 is proved. □

Theorem 7. *Let q be prime, $q\le 23$. Let l,p be primes such that $p=2l+1$, $l\equiv 3 \pmod 4$, and let the order of the prime q modulo l be $l-1$ or $\frac{l-1}{2}$. The prime q does not divide h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$.*

Proof. If the order of q modulo l is $l-1$, then q does not divide h^+ by [1] and [3]. Suppose that the order of q modulo l is $\frac{l-1}{2}$. For $q=2,3,5$, Theorem 7 was proved in the papers [2],[5],[6].

Now we shall prove that q does not divide h^+ for $q=7,11,13,17,19,23$.

Let $p\equiv -1 \pmod q$. By a computation we get that $S_j\equiv 0 \pmod q$ if and only if either $j=q-1$ or $j=q+1$. Since $3|p+1$, by Theorem 5 we get that q does not divide h^+. On the basis of the Remark after Corollary 2, the case $m=5$ need not be considered.

I. Case $q=7$

By the assumption of Theorem 1, we have that the order of q modulo l is $\frac{l-1}{2}$. Therefore

$$1=\left(\frac{7}{l}\right)=-\left(\frac{l}{7}\right).$$

Since $l\equiv 3,5,6 \pmod 7$, then $p=2l+1\equiv 4,6 \pmod 7$. Therefore $m=1,3$, i.e. either $p\equiv -1 \pmod 7$ or $p\equiv -3 \pmod 7$.

For $p\equiv -3 \pmod 7$ by Corollary 1 we get

$$\frac{p+3}{14}\frac{2^6-1}{7}\equiv 0 \pmod 7.$$

By Theorem 2, I,(i) we have

$$\frac{p+3}{14}\frac{3^6-1}{7}+\frac{1}{9}B_5\left(\frac{1}{3}\right)\equiv C_3 \pmod 7.$$

By computation,

$$\frac{3^6-1}{7}\equiv 6 \pmod 7,\ C_3\equiv 6 \pmod 7,\ B_5\left(\frac{1}{3}\right)\equiv 6 \pmod 7.$$

Hence

$$6\frac{p+3}{14}+\frac{6}{9}\equiv 6 \pmod 7,$$

which is a contradiction

$$\frac{p+3}{14}\frac{2^6-1}{7}\equiv 0 \pmod 7.$$

II. Case $q=11$

Analogously for $q=7$ we get $m=1,5,7,9,17$.

1. $m=7$, $p\equiv -7 \pmod{11}$.
By Corollary 3, if $11|h^+$, then

$$\left(\sum_{\frac{11}{7}<i<\frac{22}{7}}\frac{1}{i}\right)^2+\left(\sum_{\frac{22}{7}<i<\frac{33}{7}}\frac{1}{i}\right)^2+\left(\sum_{\frac{11}{7}<i<\frac{22}{7}}\frac{1}{i}\right)\left(\sum_{\frac{22}{7}<i<\frac{33}{7}}\frac{1}{i}\right)\equiv 0 \pmod{11}.$$

By computation, we get that this sum is $10^2+3^2+3.10\equiv 7 \pmod{11}$, therefore 11 does not divide h^+.

2. $m=9$, $p\equiv -9 \pmod{11}$.
By Corollary 6, we have

$$\left(\sum_{\frac{11}{9}<i<\frac{22}{9}}\frac{1}{i}\right)^2+\left(\sum_{\frac{22}{9}<i<\frac{44}{9}}\frac{1}{i}\right)^2+\left(\sum_{\frac{11}{9}<i<\frac{22}{9}}\frac{1}{i}\right)\left(\sum_{\frac{22}{q}<i<\frac{44}{9}}\frac{1}{i}\right)$$
$$\equiv 6^2+7^2+6.7\equiv 6 \pmod{11}.$$

Therefore 11 does not divide h^+.

3. $m=17$, $p\equiv -17 \pmod{11}$.
By Corollary 8, it is enough to prove that

$$Q_{17,4}(A_{\frac{-1}{17}},A_{\frac{-2}{17}},A_{\frac{-3}{17}},A_{\frac{-4}{17}},A_{\frac{-5}{17}},A_{\frac{-6}{17}},A_{\frac{-7}{17}},A_{\frac{-8}{17}})\not\equiv 0 \pmod{11}.$$

By computation we have

$$Q_{17,4}(A_{\frac{-1}{17}},A_{\frac{-2}{17}},A_{\frac{-3}{17}},A_{\frac{-4}{17}},A_{\frac{-5}{17}},A_{\frac{-6}{17}},A_{\frac{-7}{17}},A_{\frac{-8}{17}})\equiv 3 \pmod{11},$$

therefore 11 does not divide h^+.

III. Case $q=13$

In this case we have $m=1,5,7,17,19,23$.

1. $m=7$, $p\equiv -7 \pmod{13}$. By Corollary 3,

$$\left(\sum_{\frac{13}{7}<i<\frac{26}{7}}\frac{1}{i}\right)^2+\left(\sum_{\frac{26}{7}<i<\frac{39}{7}}\frac{1}{i}\right)^2+\left(\sum_{\frac{13}{7}<i<\frac{26}{7}}\frac{1}{i}\right)\left(\sum_{\frac{26}{7}<i<\frac{39}{7}}\frac{1}{i}\right)$$
$$\equiv 3^2+5^2+3.5\equiv 10 \pmod{13},$$

therefore 13 does not divide h^+.

2. $m=17$, $p\equiv -17 \pmod{13}$.
By computation, using Corollary 8, we get that
$A_1=1, A_2=8, A_3=4, A_4=1, A_5=9, A_6=7, A_7=9, A_8=1, A_9=4, A_{10}=8, A_{11}=1, A_{12}=0$.

For the permutation $\phi_{17,2}$ we have

$$\phi_{17,2}=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&4&6&8&7&5&3&1\end{pmatrix},$$

hence

$$Q_{17,2}(X_1,X_2,\dots,X_8)=X_1^2+X_2^2+\cdots+X_8^2-(X_1X_2+X_2X_4+\cdots+X_8X_1).$$

By computation modulo 13 we get
$A_{\frac{-1}{17}}=A_3=4, A_{\frac{-2}{17}}=A_6=7, A_{\frac{-3}{17}}=A_9=4, A_{\frac{-4}{17}}=A_{12}=0, A_{\frac{-5}{17}}=A_2=8, A_{\frac{-6}{17}}=A_5=9, A_{\frac{-7}{17}}=A_8=1, A_{\frac{-8}{17}}=A_{11}=1$.

Hence

$$Q_{17,2}(4,7,4,0,8,9,1,1) \equiv 11 \pmod{13},$$

therefore 13 does not divide h^+.

3. $m = 19$, $p \equiv -19 \pmod{13}$.

By Corollary 9 we have that

$$Q_{19,2}(8,1,7,1,8,0,1,4,9) \equiv 6 \pmod{13},$$

therefore 13 does not divide h^+.

4. $m = 23$, $p \equiv -23 \pmod{13}$.

By Theorem 1 (i), putting $n = 2$, we get

$$\frac{p+23}{26}\frac{2^{12}-1}{13} \equiv Q_{23,2}(A_{\frac{-1}{23}}, \dots, A_{\frac{-11}{23}}) \pmod{13}.$$

By computation we have

$$\frac{p+23}{26} \equiv 1 \pmod{13}.$$

Further we proceed using Theorem 2, III, (iii). The congruence (iii) can be rewritten as

$$\frac{p+m}{2q}\frac{3^{q-1}-1}{q} \equiv -\frac{1}{9}B_{q-2}\left(\frac{1}{3}\right) + \frac{3^{q-1}-1}{q} - A_{\frac{-1}{3}} + \sum_{i=1}^{\frac{q-4}{3}} \frac{1}{1+i}A_{\frac{i}{3}} \pmod{q}.$$

By substitution $m = 23$, $q = 13$ and by computation we get $\frac{3^{12}-1}{13} \equiv 8 \pmod{13}$, $B_{11}\left(\frac{1}{3}\right) \equiv 7 \pmod{13}$, $A_{\frac{-1}{3}} = A_4 = 1$, $\sum_{i=1}^{3} \frac{1}{1+i}A_{\frac{i}{3}} \equiv 2 \pmod{13}$.

This implies the congruence

$$8\frac{p+23}{26} \equiv 1 \pmod{13},$$

which is a contradiction with the congruence

$$\frac{p+23}{26} \equiv 1 \pmod{13}.$$

The case III, $q = 13$ is solved.

IV. Case $q = 17$

By computation we get that the corresponding values of m are $m = 1, 3, 7, 15, 25, 29, 31$.

1. $m = 3$, $p \equiv -3 \pmod{17}$.

By Theorem 1 (i) and Theorem 2 I.(ii), the following congruences hold:

$$\frac{p+3}{34}\frac{2^{16}-1}{17} \equiv 0 \pmod{17},$$

$$\frac{p+3}{34}\frac{3^{16}-1}{17} + \frac{2}{9}B_{15}\left(\frac{1}{3}\right) \equiv C_3 \pmod{17},$$

where

$$C_3 = A_{11}^2 + \sum_{i=2}^{12} \frac{1}{1-i}A_{\frac{-1}{3}}.$$

By computation we get that $C_3 = 5$, $B_{15}\left(\frac{1}{3}\right) \equiv 8 \pmod{17}$. Therefore

$$10\frac{p+3}{34} \equiv 7 \pmod{17},$$

$$\frac{p+3}{34}\frac{2^{16}-1}{17} \equiv 0 \pmod{17},$$

—a contradiction.

2. $m = 7$, $p \equiv -7 \pmod{17}$.

By Corollary 3 it is enough to prove that

$$\left(\sum_{\frac{17}{7}<i<\frac{34}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{34}{7}<i<\frac{51}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{17}{7}<i<\frac{34}{7}} \frac{1}{i}\right)\left(\sum_{\frac{34}{7}<i<\frac{51}{7}} \frac{1}{i}\right) \not\equiv 0 \pmod{17}.$$

3. $m = 15$, $p \equiv -15 \pmod{17}$.

In this case by Theorem 1 (i) we have

$$\frac{p+15}{34}\frac{2^{16}-1}{17} \equiv Q_{15,2}(A_{\frac{-1}{15}}, \dots, A_{\frac{-7}{15}}) \pmod{17}.$$

By computation we get

$$\frac{p+15}{34}\frac{2^{16}-1}{17} \equiv Q_{15,2}(10,1,5,10,2,16,12) \pmod{17},$$

hence

$$13\frac{p+15}{34} \equiv 2 \pmod{17}.$$

By Theorem 2 I, (i) we have

$$10\frac{p+15}{34} \equiv 7 \pmod{17},$$

—a contradiction.

4. $m = 25$, $p \equiv -25 \pmod{17}$.

By Corollary 10, it is enough to prove that

$$Q_{25,2}(10,12,5,8,5,12,10,0,1,16,2,10) \not\equiv 0 \pmod{17}.$$

By computation we get

$$Q_{25,2}(10,12,5,8,5,12,10,0,1,16,2,10) \equiv 6 \pmod{17}.$$

5. $m = 29$, $p \equiv -29 \pmod{17}$.

By Theorem 1 (i) we have

$$\frac{p+29}{34}\frac{2^{16}-1}{17} \equiv Q_{29,2}(A_{\frac{-1}{29}}, \dots, A_{\frac{-14}{29}}) \pmod{17},$$

$$\frac{p+29}{34}\frac{4^{16}-1}{17} \equiv Q_{29,2}(A_{\frac{-1}{29}}, \dots, A_{\frac{-14}{29}}) \pmod{17}.$$

By computation we get

$$13\frac{p+29}{34} \equiv 11 \pmod{17},$$

$$9\frac{p+29}{34} \equiv 8 \pmod{17},$$

—a contradiction.

6. $m = 31$, $p \equiv -31 \pmod{17}$.
By Theorem 1 (i) we have

$$\frac{p+31}{34}\frac{2^{16}-1}{17} \equiv Q_{31,2}(A_{\frac{-1}{31}},\dots,A_{\frac{-15}{31}}) \pmod{17},$$

$$\frac{p+31}{34}\frac{3^{16}-1}{17} \equiv Q_{31,3}(A_{\frac{-1}{31}},\dots,A_{\frac{-15}{31}}) \pmod{17}.$$

By computation we get two congruences

$$\frac{p+31}{34}\frac{2^{16}-1}{17} \equiv 13 \pmod{17},$$

$$\frac{p+31}{34}\frac{3^{16}-1}{17} \equiv 13 \pmod{17},$$

—a contradiction.

V. Case $q = 19$

By computation we get that $m = 1, 7, 9, 11, 13, 17, 21, 31, 33$.

1. $m = 7$, $p \equiv -7 \pmod{19}$.
By Corollary 3 it is enough to prove

$$\left(\sum_{\frac{19}{7}<i<\frac{38}{7}}\frac{1}{i}\right)^2 + \left(\sum_{\frac{38}{7}<i<\frac{57}{7}}\frac{1}{i}\right)^2 + \left(\sum_{\frac{19}{7}<i<\frac{38}{7}}\frac{1}{i}\right)\left(\sum_{\frac{38}{7}<i<\frac{57}{7}}\frac{1}{i}\right) \not\equiv 0 \pmod{19}.$$

By computation we have that the left side is equal to $13 \pmod{19}$.

2. $m = 9$, $p \equiv -9 \pmod{19}$.
By Corollary 6 it is enough to prove that

$$\left(\sum_{\frac{19}{9}<i<\frac{38}{9}}\frac{1}{i}\right)^2 + \left(\sum_{\frac{38}{9}<i<\frac{76}{9}}\frac{1}{i}\right)^2 + \left(\sum_{\frac{19}{9}<i<\frac{38}{9}}\frac{1}{i}\right)\left(\sum_{\frac{38}{q}<i<\frac{76}{9}}\frac{1}{i}\right) \not\equiv 0 \pmod{19}.$$

By computation we have that the left side is equal to $2 \pmod{19}$.

3. $m = 11$, $p \equiv -11 \pmod{19}$.
By Theorem 1 (i) we have

$$\frac{p+11}{38}\frac{2^{18}-1}{19} \equiv Q_{11,2}(A_{\frac{-1}{11}},\dots A_{\frac{-5}{11}}) \pmod{19}.$$

By computation we get that

$$Q_{11,2}(A_{\frac{-1}{11}},\dots,A_{\frac{-5}{11}}) \equiv Q_{11,2}(11,14,1,15,5) \equiv 15 \pmod{19}.$$

By Theorem 2 II, (ii) we have

$$\frac{p+11}{38}\frac{3^{18}-1}{19} + \frac{2}{9}B_{17}\left(\frac{1}{3}\right) \equiv C_{11} \pmod{19},$$

where

$$C_{11} = \sum_{i=1}^{5} A_{\frac{-i}{11}} - \sum_{i=1}^{5} A_{\frac{-1}{11}} A_{\frac{-3}{11}+1} + \sum_{i=1}^{16} \frac{1}{\frac{-3i}{11}+1} A_{\frac{-i}{11}} \equiv 17 \pmod{19},$$

$$B_{17}\left(\frac{1}{3}\right) \equiv 13 \pmod{19}.$$

Therefore

$$3\frac{p+11}{38} \equiv 15 \pmod{19},$$

$$18\frac{p+11}{38} \equiv 12 \pmod{19},$$

—a contradiction.

4. $m = 13$, $p \equiv -13 \pmod{19}$.

By Corollary 7 it is enough to prove

$$Q_{13,2}(A_{\frac{-1}{13}}, \dots, A_{\frac{-6}{13}}) \not\equiv 0 \pmod{19}.$$

But

$$Q_{13,2}(11, 14, 15, 3, 10, 1) \equiv 3 \pmod{19}.$$

5. $m = 17$, $p \equiv -17 \pmod{19}$.

By Corollary 8 it is enough to prove

$$Q_{17,2}(A_{\frac{-1}{17}}, \dots, A_{\frac{-8}{17}}) \not\equiv 0 \pmod{19},$$

but

$$Q_{17,2}(15, 1, 3, 11, 11, 5, 14, 10) \equiv 18 \pmod{19}.$$

6. $m = 21$, $p \equiv -21 \pmod{19}$.

By Theorem 1 (i) we have

$$\frac{p+21}{38}\frac{2^{18}-1}{19} \equiv Q_{21,2}(A_{\frac{-1}{21}}, \dots, A_{\frac{-10}{21}}) \pmod{19},$$

$$\frac{p+21}{38}\frac{4^{18}-1}{19} \equiv Q_{21,4}(A_{\frac{-1}{21}}, \dots, A_{\frac{-10}{21}}) \pmod{19}.$$

By computation we get

$$Q_{21,2}(13, 0, 15, 1, 3, 11, 11, 5, 10) \equiv 4 \pmod{19},$$

$$Q_{21,4}(13, 0, 15, 1, 3, 11, 11, 5, 14, 10) \equiv 3 \pmod{19},$$

which gives a contradiction.

7. $m = 31$, $p \equiv -31 \pmod{19}$.

By Theorem 1 (i) we have

$$\frac{p+31}{38}\frac{2^{18}-1}{19} \equiv Q_{31,2}(A_{\frac{-1}{31}}, \dots, A_{\frac{-15}{31}}) \pmod{19},$$

$$\frac{p+31}{38}\frac{3^{18}-1}{19} \equiv Q_{31,3}(A_{\frac{-1}{31}}, \dots, A_{\frac{-15}{31}}) \pmod{19},$$

$$Q_{31,2}(3, 5, 10, 11, 1, 13, 1, 11, 10, 5, 3, 0, 15, 11, 14) \equiv 4 \pmod{19},$$

$$Q_{31,3}(3, 5, 10, 11, 1, 13, 1, 11, 10, 5, 3, 0, 15, 11, 14) \equiv 3 \pmod{19}.$$

By computation we get

$$3\frac{p+31}{38} \equiv 3 \pmod{19},$$

$$18\frac{p+31}{38} \equiv 7 \pmod{19},$$

—a contradiction.

8. $m = 33$, $p \equiv -33 \pmod{19}$.

By Theorem 1 (i) we have

$$\frac{p+33}{38}\frac{2^{18}-1}{19} \equiv Q_{33,2}(A_{\frac{-1}{33}}, \dots, A_{\frac{-16}{33}}) \pmod{19},$$

$$\frac{p+33}{38}\frac{4^{18}-1}{19} \equiv Q_{33,2}(A_{\frac{-1}{33}}, \dots, A_{\frac{-16}{33}}) \pmod{19}.$$

By computation we get

$$Q_{33,2}(10,15,11,11,1,14,13,14,1,11,11,15,10,0,5,3) \equiv 18 \pmod{19},$$

$$Q_{33,4}(10,15,11,11,1,14,13,14,1,11,11,15,10,0,5,3) \equiv 1 \pmod{19},$$

—a contradiction.

VI. Case $q = 23$

The possible values for m are $m = 1,3,5,7,11,15,17,25,31,35$.

1. $m = 3$, $p \equiv -3 \pmod{23}$.

By Theorem 1 (i) we have

$$\frac{p+3}{46}\frac{2^{22}-1}{23} \equiv 0 \pmod{23}.$$

By Theorem 2 I.(ii) we get

$$\frac{p+3}{46}\frac{3^{22}-1}{23} + \frac{2}{9}B_{21}\left(\frac{1}{3}\right) \equiv C_3 \pmod{23}.$$

By computation we obtain that $C_3 \equiv 19 \pmod{23}$, $B_{21}\left(\frac{1}{3}\right) \equiv 13 \pmod{23}$, —a contradiction.

2. $m = 7$, $p \equiv -7 \pmod{23}$.

By Corollary 3 it is enough to prove

$$\left(\sum_{\frac{23}{7}<i<\frac{46}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{46}{7}<i<\frac{69}{7}} \frac{1}{i}\right)^2 + \left(\sum_{\frac{23}{7}<i<\frac{46}{7}} \frac{1}{i}\right)\left(\sum_{\frac{46}{7}<i<\frac{69}{7}} \frac{1}{i}\right) \not\equiv 0 \pmod{23}.$$

By computation we get that the sum is different from zero $\pmod{23}$.

3. $m = 11$, $p \equiv -11 \pmod{23}$.

By Theorem 2 II.(i) we have

$$\frac{p+11}{46}\frac{3^{22}-1}{23} + \frac{1}{9}B_{21}\left(\frac{1}{3}\right) \equiv C_{11} \pmod{23},$$

where

$$C_{11} = \sum_{i=1}^{5} A_{\frac{-i}{11}} - \sum_{i=1}^{5} A_{\frac{-1}{11}} A_{\frac{-3}{11}+1} + \sum_{i=1}^{11} \frac{1}{\frac{-3i}{11}+1} A_{\frac{-i}{11}} \equiv 3 \pmod{23}.$$

Hence

$$\frac{p+11}{46}\frac{3^{22}-1}{23} \equiv 22 \pmod{23}.$$

By Theorem 1 (i) we have

$$\frac{p+11}{46}\frac{2^{22}-1}{23} \equiv Q_{11,2}(A_{\frac{-1}{11}}, \dots A_{\frac{-5}{11}}) \pmod{23}.$$

Therefore

$$\frac{p+11}{38}\frac{2^{18}-1}{19} \equiv 17 \pmod{23},$$

$$\frac{p+11}{46}\frac{3^{22}-1}{23} \equiv 22 \pmod{23},$$

—a contradiction.

4. $m = 15$, $p \equiv -15 \pmod{23}$.

By Theorem 1 (i) we have

$$\frac{p+15}{46}\frac{2^{22}-1}{23} \equiv Q_{15,2}(A_{\frac{-1}{15}}, \dots A_{\frac{-7}{15}}) \equiv 4 \pmod{23}.$$

By Theorem 2 I.(ii)

$$\frac{p+15}{46}\frac{3^{22}-1}{23} + \frac{2}{9}B_{21}\left(\frac{1}{3}\right) \equiv C_{15} \pmod{23}.$$

By computation we get a contradiction.

5. $m = 17$, $p \equiv -17 \pmod{23}$.

By Corollary 8 it is enough to prove

$$Q_{17,4}(A_{\frac{-1}{17}}, \dots, A_{\frac{-8}{17}}) \not\equiv 0 \pmod{23},$$

$$Q_{17,4}(A_{\frac{-1}{17}}, \dots, A_{\frac{-8}{17}}) \equiv 8 \pmod{23}.$$

6. $m = 25$, $p \equiv -25 \pmod{23}$.

By Corollary 10 it is enough to prove

$$Q_{25,4}(A_{\frac{-1}{25}}, \dots, A_{\frac{-12}{25}}) \not\equiv 0 \pmod{23},$$

$$Q_{25,4}(A_{\frac{-1}{25}}, \dots, A_{\frac{-12}{25}}) \equiv 11 \pmod{23}.$$

7. $m = 31$, $p \equiv -31 \pmod{23}$.

By Theorem 1 (i) we have

$$\frac{p+31}{46}\frac{2^{22}-1}{23} \equiv Q_{31,2}(A_{\frac{-1}{31}}, \dots A_{\frac{-15}{31}}) \equiv 13 \pmod{23},$$

$$\frac{p+31}{46}\frac{3^{22}-1}{23} \equiv Q_{31,2}(A_{\frac{-1}{31}}, \dots A_{\frac{-15}{31}}) \equiv 15 \pmod{23},$$

—a contradiction.

8. $m = 35$, $p \equiv -35 \pmod{23}$.

By Theorem 2 II. (i) we have

$$\frac{p+35}{46}\frac{3^{22}-1}{23} + \frac{1}{9}B_{21}\left(\frac{1}{3}\right) \equiv C_{35} \pmod{23},$$

by computation we get the congruence

$$\frac{p+15}{46}\frac{3^{22}-1}{23} \equiv 10 \pmod{23}.$$

By Theorem 1 (i) we have

$$\frac{p+35}{46}\frac{2^{22}-1}{23} \equiv Q_{35,2}(A_{\frac{-1}{35}}, \dots A_{\frac{-17}{35}}) \equiv 0 \pmod{23},$$

—a contradiction. Theorem 7 is proved. □

Now we give the values of j such that $S_j \equiv 0 \pmod q$ for $q \leq 173$ (see Theorem 5)

1. $q = 29$, $j = 4, 28, 30, 54$
2. $q = 31$, $j = 30, 32$
3. $q = 37$, $j = 36, 38$
4. $q = 41$, $j = 40, 42$
5. $q = 43$, $j = 34, 42, 44, 52$
6. $q = 47$, $j = 46, 48$
7. $q = 53$, $j = 14, 48, 52, 54, 58, 92$
8. $q = 61$, $j = 36, 60, 62, 86$
9. $q = 67$, $j = 66, 68$
10. $q = 71$, $j = 70, 72$
11. $q = 73$, $j = 72, 74$
12. $q = 79$, $j = 78, 80$
13. $q = 83$, $j = 82, 84$
14. $q = 89$, $j = 88, 90$
15. $q = 97$, $j = 96, 98$
16. $q = 101$, $j = 38, 100, 102, 164$
17. $q = 103$, $j = 102, 104$
18. $q = 107$, $j = 68, 92, 106, 108, 122, 146$
19. $q = 109$, $j = 108, 110$
20. $q = 113$, $j = 112, 114$
21. $q = 127$, $j = 12, 26, 116, 126, 128, 138, 228, 242$
22. $q = 131$, $j = 130, 132$
23. $q = 137$, $j = 76, 80, 136, 138, 194, 198$
24. $q = 139$, $j = 56, 138, 140, 222$
25. $q = 149$, $j = 2, 126, 148, 150, 172, 196$
26. $q = 151$, $j = 84, 150, 152, 218$
27. $q = 157$, $j = 12, 156, 158, 302$
28. $q = 163$, $j = 162, 164$
29. $q = 167$, $j = 166, 168$
30. $q = 173$, $j = 80, 172, 174, 266$

By Theorem 5, putting $n = 3$, we obtain that q does not divide h^+ for $q \leq 173$.

By computation it was verified that the assumption of Theorem 5 (putting $n = 3$) is satisfied for all $q \leq 857$.

Acknowledgement

The author thanks the referee of this article for the important suggestions and for the short proof of Lemma 1.

References

[1] D. Davis, Computing the number of totally positive circular units which are squares, J. Number Theory **10** (1978), p. 1-9. MR **57:**16254

[2] D.R. Estes, On the parity of the class number of the field of q-th roots of unity, The Rocky Mountain J. of Math. **19** (1989), p.675-681. MR **92b:**11078

[3] A. Granville and Zhi-Wei Sun, Values of Bernoulli Polynomials, Pacific Journal of Mathematics, Vol. 172 No. 1, (1996) 117-137. CMP 96:09

[4] S. Jakubec, On divisibility of class number or real Abelian fields of prime conductor, Abh. Math. Sem. Univ. Hamburg **63** (1993), p. 67-86. MR **95a:**11098

[5] S.Jakubec, On divisibility of h^+ by the prime 3. The Rocky Mountain J. of Math, Volume 24, Number 4 (1994) 1467-1473. MR **95m:**11119

[6] S. Jakubec, On divisibility of h^+ by the prime 5. Math. Slovaca 44,5,(1994) 650-700. MR **96f:**11140

[7] S. Jakubec, Connection between Wiefferich congruence and divisibility of h^+. Acta Arithmetica 71.1 (1995) 55-64. MR **96e:**11138

[8] S. Jakubec, Connection between congruences $n^{q-1} \equiv 1 \pmod{q^2}$ and divisibility of h^+, Abh. Math. Sem. Univ. Hamburg 66 (1996) 151-158. CMP 97:03

[9] P.L. Montgomery, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. 61 (1993), 361-363. MR **94d:**11003

[10] L.C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1982. MR **85g:**11001

[11] Zhi-Mong Sun and Zhi-Wei Sun, Fibonacci numbers and Fermat's Last theorem, Acta Arith. 60 (1992), 371-388. MR **93e:**11025

Mathematical Institute of the Slovak Academy of Sciences, Štefánikova 49, 814 73 Bratislava, Slovakia

E-mail address: jakubec@mau.savba.sk