ACTA ARITHMETICA
LXXI.1 (1995)

Connection between the Wieferich congruence and divisibility of h^+

by

Stanislav Jakubec (Bratislava)

As is well known, the Wieferich congruence is the congruence $2^{q-1} \equiv 1 \pmod{q^2}$. Wieferich proved in 1909 that if $2^{q-1} \not\equiv 1 \pmod{q^2}$ then for the exponent q the first case of Fermat's Last Theorem holds.

The aim of this paper is to prove Theorem 1, which gives a connection between the Wieferich congruence and divisibility of h^+ (the class number of the field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$) by the prime q.

Theorem 1. *Let q be an odd prime. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, $p \equiv -1 \pmod q$, $p \not\equiv -1 \pmod{q^3}$ and let the order of the prime q modulo l be $(l-1)/2$. Suppose that q divides h^+, the class number of the real cyclotomic field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Then $2^{q-1} \equiv 1 \pmod{q^2}$.*

To prove this theorem, the following assertion from [1] 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 $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $[K : \mathbb{Q}] = l$ and let h_K be the class number of the field K. If $q \mid h_K$, then $q \mid N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\omega)$, where*

$$\omega = a_1 \sum_{i \equiv 1 \pmod q} \chi(i) + a_2 \sum_{i \equiv 2 \pmod q} \chi(i) + \ldots + a_{q-1} \sum_{i \equiv q-1 \pmod q} \chi(i),$$

and $\chi(x)$ is the Dirichlet character modulo p, $\chi(x) = \zeta_l^{\operatorname{ind} x}$.

The values a_i were calculated on the basis of the formula (4), p. 73 in [1]. Note that the numbers $a_1, a_2, \ldots, a_{q-1}$ do not depend on the prime p, but depend on p modulo q. It is clear that instead of $a_1, \ldots, a_{q-1}$, we can consider the numbers $aa_1, \ldots, aa_{q-1}$ modulo q for any $a \not\equiv 0 \pmod q$.

Before we give a proof of Theorem 1 we show some connections of this paper with q-adic L-functions $L_q(1, \chi)$.

1991 *Mathematics Subject Classification*: Primary 11R29.

The number

$$\omega=\sum_{r=1}^{q-1}a_r\sum_{i\equiv r\ (\bmod\ q)}\chi(i)$$

plays a fundamental role in the proof.

Let $F'_\gamma=(\gamma^q-\gamma^{\sigma_q})/(q\gamma^{\sigma_q})\in\mathbb{Z}_K$ (where σ_q is the Frobenius automorphism at q in $K/\mathbb{Q}$), and let $\varphi:\mathbb{Z}_K\to\mathbb{Z}(\zeta_l)$ be defined by $\varphi(\alpha)=c_1+c_2\zeta_l+\ldots+c_l\zeta_l^{l-1}$, where $\alpha=c_1\alpha_1+c_2\alpha_2+\ldots+c_l\alpha_l$ and $\alpha_1,\ldots,\alpha_l$ are Gauss periods.

It is proved in [1] that ω is equal to $\varphi(F'_\gamma)$ up to a multiplicative constant $\beta\in\mathbb{Q}(\zeta_l)$ such that $N(\beta)\not\equiv 0 \pmod q$.

For the q-adic L-function $L_q(1,\chi^{-1})$ we have

$$\begin{aligned}L_q(1,\chi^{-1})&=-\left(1-\frac{\chi^{-1}(q)}{q}\right)\frac{\tau(\chi^{-1})}{p}\sum_{a=1}^{p}\chi(a)\log_q(1-\zeta_p^q)\\&=u_\chi\frac{1}{q}\sum_{\sigma\in G}\chi(\sigma)\log_q(\gamma^\sigma),\end{aligned}$$

where u_χ is a q-adic unit.

The connection between ω and $L_q(1,\chi^{-1})$ is stated in the following lemma.

Lemma. *There is an automorphism σ^{**} of the field $\mathbb{Q}(\zeta_l)$ and a q-adic unit v_χ such that*

$$v_\chi\sigma^{**}(\omega)\equiv L_q(1,\chi^{-1}) \pmod q.$$

Proof. Let

$$\frac{1}{q}\log_q\gamma\equiv b_1\alpha_1+\ldots+b_l\alpha_l \pmod q.$$

Thus

$$(*)\qquad \frac{1}{q}\sum_{\sigma\in G}\chi(\sigma)\log_q(\gamma^\sigma)\equiv\sum_{\sigma\in G}\chi(\sigma)\sigma(b_1\alpha_1+\ldots+b_l\alpha_l) \pmod q,$$

$$\varphi(b_1\alpha_1+\ldots+b_l\alpha_l)=b_1+b_2\zeta_l+\ldots+b_l\zeta_l^{l-1}.$$

By reduction of the right side of $(*)$ we deduce that there is an automorphism σ^* of $\mathbb{Q}(\zeta_l)$ and a natural number n such that

$$\frac{1}{q}\sum_{\sigma\in G}\chi(\sigma)\log_q(\gamma^\sigma)\equiv\tau(\chi^n)\sigma^*(b_1+b_2\zeta_l+\ldots+b_l\zeta_l^{l-1}) \pmod q.$$

It can be proved that

$$F'_\gamma\equiv\frac{1}{q}\log_q(\gamma^{\sigma_q}) \pmod q.$$

Finally, we have

$$v_\chi \sigma^{**}(\omega) \equiv L_q(1, \chi^{-1}) \pmod{q},$$

for a suitable automorphism σ^{**} of $\mathbb{Q}(\zeta_l)$. That v_χ is a q-adic unit follows from the fact that u_χ and the Gauss sum $\tau(\chi^n)$ are both q-adic units. ∎

By considering the congruence

$$L_q(1, \chi^{-1}) \equiv B_1(\chi^{-1}\theta^{-1}) \pmod{q},$$

(where θ is the Teichmüller character at q and B_1 the generalized Bernoulli number) the result of this paper can be stated as follows:

$$q \mid NB_1(\chi^{-1}\theta^{-1}) \Rightarrow \text{Wieferich congruence for prime } q.$$

Proof of Theorem 1. We shall prove that if $p \not\equiv -1 \pmod{q^3}$ and $2^{q-1} \not\equiv 1 \pmod{q^2}$ then q does not divide h^+. Since the order of q modulo l is $(l-1)/2$ we have $\left(\frac{q}{l}\right) = 1$. From $p \equiv -1 \pmod{q}$ we have $l \equiv -1 \pmod{q}$. Let $q \equiv 1 \pmod{4}$. Then

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

If $q \equiv 3 \pmod{4}$, then

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

As we will prove later (see Lemma 3), for $p \equiv -1 \pmod{q}$ we have $a_{q-1} = 0$. It follows that $\omega = 2\tau$, where

$$\tau = a_1 \sum_{\substack{i \equiv 1 \pmod{q} \\ i < p/2}} \chi(i) + a_2 \sum_{\substack{i \equiv 2 \pmod{q} \\ i < p/2}} \chi(i) + \ldots + a_{q-1} \sum_{\substack{i \equiv q-1 \pmod{q} \\ i < p/2}} \chi(i).$$

Since the order of q modulo l is $(l-1)/2$, we see that q splits into two divisors in $\mathbb{Q}(\zeta_l)$. Because $l \equiv 3 \pmod{4}$, we have $\left(\frac{-1}{l}\right) = -1$, hence if $q \mid N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\omega)$ then q divides $\tau\overline{\tau}$.

The following formula holds:

$$\tau\overline{\tau} = \sum_{\substack{i,j \equiv 1,2,\ldots,q-1 \pmod{q} \\ i,j < p/2}} a_i a_j \chi(ij^{-1}) = b_0 + b_1\zeta_l + b_2\zeta_l^2 + \ldots + b_{l-1}\zeta_l^{l-1}.$$

Then $q \mid \tau\overline{\tau}$ if and only if $b_0 \equiv b_1 \equiv \ldots \equiv b_{l-1} \pmod{q}$. We shall compute the coefficient b_0.

Let $\chi(ij^{-1}) = 1$. Then $ij^{-1} \equiv 1 \pmod{p}$ or $ij^{-1} \equiv -1 \pmod{p}$, therefore either $i - j \equiv 0 \pmod{p}$ or $i + j \equiv 0 \pmod{p}$, $i, j < p/2$. Hence $i \equiv j \pmod{p}$, and therefore $i = j$.

The following equalities hold:

$$\#\{i \equiv 1 \pmod q : i < p/2\} = \frac{p+1}{2q},$$
$$\#\{i \equiv 2 \pmod q : i < p/2\} = \frac{p+1}{2q},$$
$$\vdots$$
$$\#\{i \equiv q-2 \pmod q : i < p/2\} = \frac{p+1}{2q}.$$

It follows that

$$b_0 = \frac{p+1}{2q} \sum_{i=1}^{q-1} a_i^2.$$

LEMMA 1. *Let* $p \equiv z \pmod q$. *For the coefficients* $a_1, \ldots, a_{q-1}$, *the following congruence holds*:

$$a_k \equiv \frac{z}{2q} \sum_{i=1}^{q-1} \frac{1}{i} \cdot \left(\overline{\frac{i-k}{z}} - \overline{\frac{i}{z}} - \overline{\frac{-k-i}{z}} + \overline{\frac{-i}{z}} \right) \pmod q,$$

where

$$\overline{\frac{i-k}{z}},\ \overline{\frac{i}{z}},\ \overline{\frac{-k-i}{z}},\ \overline{\frac{-i}{z}},$$

are residues modulo q *from the interval* $\langle 0, q-1\rangle$.

Proof. By the formula (4), p. 73 in [1] we have

$$\frac{(\zeta_p - 1)^q - (\zeta_p^q - 1)}{q} \sum_{i=1}^{p-1} i\zeta_p^{qi} = c_0 + c_1\zeta_p + c_2\zeta_p^2 + \ldots + c_{p-1}\zeta_p^{p-1}.$$

Let $\zeta_p^i \zeta_p^{qj} = 1$. Then $i + qj \equiv 0 \pmod p$, and therefore

$$j \equiv \frac{-i}{q} \pmod p, \qquad 0 \le j < p.$$

Hence

$$c_0 \equiv \frac{1}{q} \sum_{i=1}^{q-1} \overline{\frac{-i}{q}} \binom{q}{q-i} (-1)^{q-i} \pmod q,$$

where $\overline{\frac{-i}{q}}$ is a residue modulo p, with $0 \le \overline{\frac{-i}{q}} < p$. According to [1],

$$a_k = c_k - c_0 = \frac{1}{q} \sum_{i=1}^{q-1} \binom{q}{q-i} (-1)^{q-i} \left(\overline{\frac{k-i}{q}} - \overline{\frac{-i}{q}} \right).$$

Replacing i by $q-i$ and using $\binom{q}{i} = \binom{q}{q-i}$ we get

$$a_k \equiv \frac{1}{2}\frac{z}{q}\sum_{i=1}^{q-1}\binom{q}{i}(-1)^{i+1}\left(\frac{\overline{k-i}}{q} - \frac{\overline{-i}}{q} - \frac{\overline{k+i}}{q} + \frac{\overline{i}}{q}\right) \pmod q.$$

Let $p = aq + z$. Let x_1 be such that

$$x_1 p + k - i \equiv 0 \pmod q, \quad 0 \le x_1 < q.$$

The numbers x_2, x_3, x_4 will be defined analogously. Then

$$\begin{aligned}
\frac{\overline{k-i}}{q} &= \frac{x_1(aq+z)+k-i}{q} = ax_1 + \frac{x_1 z + k - i}{q},\\
\frac{\overline{-i}}{q} &= \frac{x_2(aq+z)-i}{q} = ax_2 + \frac{x_2 z - i}{q},\\
\frac{\overline{k+i}}{q} &= \frac{x_3(aq+z)+k+i}{q} = ax_3 + \frac{x_3 z + k + i}{q},\\
\frac{\overline{i}}{q} &= \frac{x_4(aq+z)+i}{q} = ax_4 + \frac{x_4 z + i}{q}.
\end{aligned}$$

Hence

$$\begin{aligned}
&\frac{\overline{k-i}}{q} - \frac{\overline{-i}}{q} - \frac{\overline{k+i}}{q} + \frac{\overline{i}}{q}\\
&\quad = a(x_1 - x_2 - x_3 + x_4) + \frac{x_1 z + k - i}{q} - \frac{x_2 z - i}{q} - \frac{x_3 z + k + i}{q} + \frac{x_4 z + i}{q}.
\end{aligned}$$

It is easy to see that

$$x_1 - x_2 - x_3 + x_4 \equiv 0 \pmod q.$$

The assertion of Lemma 1 now follows from the congruence

$$\frac{1}{q}\binom{q}{i}(-1)^{i+1} \equiv \frac{1}{i} \pmod q. \ \blacksquare$$

LEMMA 2. *Let $p \equiv z \pmod q$, $0 < z < q$. Then $a_k \equiv a_{z-k} \pmod q$.*

Proof. This follows from Lemma 1. ■

Let $r < l$. Then $g^r \equiv 2$ or $-2 \pmod p$. We shall compute the coefficient b_r.

Let $\chi(ij^{-1}) = \zeta_l^r$. Then either $\operatorname{ind}(ij^{-1}) = r$ or $\operatorname{ind}(ij^{-1}) = r + l$ and therefore either $ij^{-1} \equiv 2 \pmod p$ or $ij^{-1} \equiv -2 \pmod p$, $i, j < p/2$. Hence by Lemma 2 we have

$$b_r \equiv \frac{p+1}{2q}\sum_{i=1}^{q-1} a_i a_{2i} \pmod q.$$

Therefore if $q \mid \tau\overline{\tau}$, then

$$\frac{p+1}{2q}\Big(\sum_{i=1}^{q-1} a_i a_{2i} - \sum_{i=1}^{q-1} a_i^2\Big) \equiv 0 \pmod{q}.$$

If

$$\sum_{i=1}^{q-1} a_i a_{2i} - \sum_{i=1}^{q-1} a_i^2 \not\equiv 0 \pmod{q},$$

then

$$\frac{p+1}{2q} \equiv 0 \pmod{q},$$

and hence $p \equiv -1 \pmod{q^2}$.

We shall prove that

$$\sum_{i=1}^{q-1} a_i a_{2i} - \sum_{i=1}^{q-1} a_i^2 \equiv -\frac{2^{q-1}-1}{q} \pmod{q}.$$

LEMMA 3. *Let* $p \equiv -1 \pmod{q}$. *Then*

$$a_k \equiv \sum_{i=1}^{k} \frac{1}{i} \pmod{q} \qquad \textit{for } k = 1, 2, \ldots, q-1.$$

P r o o f. It is easy to see that

$$\overline{\frac{i-k}{q-1}} = i - k + \delta_{i,k}, \qquad \text{where } \delta_{i,k} = \begin{cases} 0, & k \le i, \\ q, & i < k, \end{cases}$$
$$\overline{\frac{i}{q-1}} = q - i,$$
$$\overline{\frac{-i-k}{q-1}} = i + k - \beta_{i,k}, \qquad \text{where } \beta_{i,k} = \begin{cases} 0, & i + k < q, \\ q, & q \le k + i, \end{cases}$$
$$\overline{\frac{-i}{q-1}} = i.$$

It follows that

$$a_k \equiv \frac{1}{q} \sum_{i=1}^{q-1} \frac{1}{i}(\delta_{i,k} + \beta_{i,k} - q) \pmod{q}.$$

Analysing all cases we get the congruence of Lemma 3. ∎

LEMMA 4. *The following congruence holds*:

$$\sum_{i=1}^{q-1} a_i^2 \equiv -2 \pmod{q}.$$

P r o o f. It is easy to see that

$$\begin{aligned}
&\sum_{i=1}^{q-1} a_i^2 \\
&\quad\equiv (q-1)1^2 + (q-2)\frac{1}{2^2} + (q-3)\frac{1}{3^2} + \ldots + 1\cdot\frac{1}{(q-1)^2} \\
&\qquad + 2\biggl(1\cdot(-1)(q-2) + \frac{1}{2}(-1)(q-3) + \ldots + \frac{1}{q-2}(-1)(q-(q-1))\biggr) \\
&\quad\equiv -\biggl(1+\frac{1}{2}+\ldots+\frac{1}{q-1}\biggr) + 2\biggl(\frac{2}{1}+\frac{3}{2}+\ldots+\frac{q-1}{q-2}\biggr) \\
&\quad\equiv -2 \pmod q. \quad\blacksquare
\end{aligned}$$

Lemma 5. *Let $m = (q-1)/2$. The following congruence holds*:

$$\sum_{i=1}^{q-1} a_i a_{2i} \equiv \biggl(-1+\frac{1}{2}-\frac{1}{3}+\ldots+(-1)^m\frac{1}{m}\biggr) - 2 \pmod q.$$

P r o o f. Let $m \equiv 0 \pmod 2$. It is easy to see that

$$\begin{aligned}
\sum_{i=1}^{q-1} a_i a_{2i} \equiv 1\cdot\biggl(1+\frac{1}{2}\biggr) &+ \biggl(1+\frac{1}{2}\biggr)\biggl(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}\biggr) \\
&+ \ldots + \biggl(1+\frac{1}{2}+\ldots+\frac{1}{m}\biggr)\biggl(1+\frac{1}{2}+\ldots+\frac{1}{2m}\biggr) \\
&+ \biggl(1+\frac{1}{2}+\ldots+\frac{1}{m-1}\biggr)\biggl(1+\frac{1}{2}+\ldots+\frac{1}{2m-1}\biggr) \\
&+ \biggl(1+\frac{1}{2}+\ldots+\frac{1}{m-2}\biggr)\biggl(1+\frac{1}{2}+\ldots+\frac{1}{2m-3}\biggr) \\
&+ \ldots + 1\cdot\biggl(1+\frac{1}{2}+\frac{1}{3}\biggr).
\end{aligned}$$

Multiplying out from the left by the numbers $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{m}$, one after another, we have

$$\begin{aligned}
&\sum_{i=1}^{q-1} a_i a_{2i} \\
&\equiv 1\cdot\biggl((q-2) + (q-2)\frac{1}{2} + (q-3)\frac{1}{3} + \ldots + 1\cdot\frac{1}{q-1}\biggr) \\
&\quad + \frac{1}{2}\biggl((q-4)\biggl(1+\frac{1}{2}+\frac{1}{3}\biggr) + (q-4)\frac{1}{4} + (q-5)\frac{1}{5} + \ldots + 1\cdot\frac{1}{q-1}\biggr)
\end{aligned}$$

$$+\frac{1}{3}\biggl((q-6)\Bigl(1+\frac{1}{2}+\ldots+\frac{1}{5}\Bigr)+(q-6)\frac{1}{6}+(q-7)\frac{1}{7}+\ldots+1\cdot\frac{1}{q-1}\biggr)$$
$$+\ldots+\frac{1}{i}\biggl((q-2i)\Bigl(1+\frac{1}{2}+\ldots+\frac{1}{2i-1}\Bigr)$$
$$+(q-2i)\frac{1}{2i}+\ldots+1\cdot\frac{1}{q-1}\biggr)$$
$$+\ldots+\frac{1}{m}\biggl((q-2m)\Bigl(1+\frac{1}{2}+\ldots+\frac{1}{2m-1}\Bigr)+\frac{1}{q-1}\biggr) \pmod q.$$

It follows that

$$\sum_{i=1}^{q-1} a_i a_{2i} \equiv -2-2\Bigl(1+\frac{1}{2}+\frac{1}{3}\Bigr)-2\Bigl(1+\frac{1}{2}+\ldots+\frac{1}{5}\Bigr)$$
$$-\ldots-2\Bigl(1+\frac{1}{2}+\ldots+\frac{1}{2m-1}\Bigr)+q-1 \pmod q.$$

Hence

$$\sum_{i=1}^{q-1} a_i a_{2i} \equiv -2m-2(m-1)\Bigl(\frac{1}{2}+\frac{1}{3}\Bigr)-2(m-2)\Bigl(\frac{1}{4}+\frac{1}{5}\Bigr)$$
$$-\ldots-2\Bigl(\frac{1}{2m-2}+\frac{1}{2m-1}\Bigr)-1 \pmod q.$$

From this we obtain

$$\sum_{i=1}^{q-1} a_i a_{2i} \equiv -2\biggl(m\Bigl(1+\frac{1}{2}+\ldots+\frac{1}{m-1}\Bigr)$$
$$-\biggl(m-\Bigl(\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{m+1}\Bigr)\biggr)\biggr)-1 \pmod q.$$

Therefore, we have

$$\sum_{i=1}^{q-1} a_i a_{2i} \equiv \Bigl(-1+\frac{1}{2}-\frac{1}{3}+\ldots+(-1)^m\frac{1}{m}\Bigr)-2 \pmod q.$$

In the case $m \equiv 1 \pmod 2$, we proceed analogously. ∎

The following congruence is known:

$$1-\frac{1}{2}+\frac{1}{3}+\ldots+(-1)^{m+1}\frac{1}{m} \equiv \frac{2^{q-1}-1}{q} \pmod q.$$

This easily implies that if $q \mid h^+$ and $2^{q-1} \not\equiv 1 \pmod{q^2}$ then

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

LEMMA 6. *If* $q \mid h^+$ *and* $p \equiv -1 \pmod{q^2}$, *then* $p \equiv -1 \pmod{q^3}$.

Proof. Let $s < l$. Then $g^s \equiv 2q$ or $-2q \pmod{p}$. We shall compute the coefficient b_s.

Let $\chi(ij^{-1}) = \zeta_l^s$. Then either $\operatorname{ind}(ij^{-1}) = s$ or $\operatorname{ind}(ij^{-1}) = s + l$ and therefore either $ij^{-1} \equiv 2q \pmod{p}$ or $ij^{-1} \equiv -2q \pmod{p}$ $i, j < p/2$.

Consider the intervals

$$\left(0, \frac{p}{2q}\right), \ \left(\frac{p}{2q}, \frac{2p}{2q}\right), \ \left(\frac{2p}{2q}, \frac{3p}{2q}\right), \ \ldots, \ \left(\frac{(q-1)p}{2q}, \frac{qp}{2q}\right).$$

If

$$x \in \left(\frac{ip}{2q}, \frac{(i+1)p}{2q}\right),$$

then $ip < 2qx < (i+1)p$. Reducing modulo p we get

$$2qx - ip \equiv -i(q-1) \equiv i \pmod{q}.$$

Let $p = aq^2 - 1$. Then

$$\#\left\{x \in \left(\frac{ip}{2q}, \frac{(i+1)p}{2q}\right), \ x \equiv k \pmod{q}\right\} = \frac{a}{2}$$

for $k = 1, 2, \ldots, q-1$, $i = 1, 2, \ldots, q-1$. By Lemma 2, it follows that

$$\begin{aligned} b_s \equiv {} & \frac{a}{2} a_1 (a_1 + a_2 + \ldots + a_{q-1}) + \frac{a}{2} a_2 (a_1 + a_2 + \ldots + a_{q-1}) \\ & + \ldots + \frac{a}{2} a_{q-1} (a_1 + a_2 + \ldots + a_{q-1}). \end{aligned}$$

Since

$$a_1 + a_2 + \ldots + a_{q-1} \equiv 1 \pmod{q},$$

we have $b_s \equiv \frac{a}{2} \pmod{q}$. If $q \mid h^+$ then $b_s \equiv b_0 \equiv 0 \pmod{q}$ and hence $a \equiv 0 \pmod{q}$. It follows that

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

Theorem 1 is proved.

Remark. For $q < 6 \cdot 10^9$ there are exactly two primes satisfying the congruence $2^{q-1} \equiv 1 \pmod{q^2}$, namely $q = 1093$ and $q = 3511$. Hence Theorem 1 does not give any information on divisibility of h^+ for these two primes.

This default can be removed in the following way. Consider the coefficient b_t corresponding to the congruences

$$ij^{-1} \equiv 3 \pmod{p} \quad \text{or} \quad ij^{-1} \equiv -3 \pmod{p}, \quad i, j < p/2.$$

Then

$$b_t \equiv \frac{p+1}{3q} \sum_{i=1}^{q-1} a_i a_{3i} + \frac{p+1}{6q} \sum_{i=1}^{q-1} a_i a_{3i+1} \pmod{q}.$$

Hence it is enough to prove that

$$(**)\qquad \frac{p+1}{3q}\sum_{i=1}^{q-1} a_i a_{3i} + \frac{p+1}{6q}\sum_{i=1}^{q-1} a_i a_{3i+1} - \frac{p+1}{2q}\sum_{i=1}^{q-1} a_i^2 \not\equiv 0 \pmod q.$$

By a numerical calculation for $q = 1093$ and $q = 3511$ we find that $(**)$ holds. Therefore if $p \not\equiv -1 \pmod{q^3}$ for $q = 1093$ and $q = 3511$, then under the assumptions of Theorem 1, neither 1093 nor 3511 divides h^+.

Acknowledgements. I am grateful to the referee for his suggestions concerning q-adic L-functions.

References

[1] S. Jakubec, *On divisibility of class number of real Abelian fields of prime conductor*, Abh. Math. Sem. Univ. Hamburg 63 (1993), 67–86.

MATEMATICKÝ ÚSTAV SAV
ŠTEFÁNIKOVA 49
814 73 BRATISLAVA, SLOVAKIA

Received on 24.2.1994
and in revised form on 21.9.1994 (2566)