Stanislav Jakubec

On divisibility of h^+ by the prime 5

Mathematica Slovaca, Vol. 44 (1994), No. 5, 651--661

Persistent URL: http://dml.cz/dmlcz/136635

Math. Slovaca, **44** (1994), No. 5, 651–661

Mathematica Slovaca
©1994
Mathematical Institute
Slovak Academy of Sciences

ON DIVISIBILITY OF h^+ BY THE PRIME 5

STANISLAV JAKUBEC

(Communicated by Milan Paštéka)

ABSTRACT. In this paper it is proved that under certain assumptions (see Theorem 1) 5 does not divide the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$.

Introduction

Let l, p be primes such that $p = 2l + 1$. Davis has proved in [1] that if 2 is a primitive root modulo l, then 2 does not divide the class number h of the cyclotomic field $\mathbf{Q}(\zeta_p)$. This result follows from the relation between the group of totally positive units and the group of squares of the field $L = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$.

In Estes [2], it is shown that provided the order of 2 modulo l is $\frac{l-1}{2}$, and $l \equiv 3 \pmod 4$, then 2 does not divide the class number h of the cyclotomic field $\mathbf{Q}(\zeta_p)$. This result was obtained using Hasse's theorem (Satz 45), i.e. h is odd if and only if h^- is odd.

Note that analogous assertions for divisibility of h by primes $q > 2$ do not hold. For example for $l = 29$, $p = 59$: 3 is a primitive root modulo 29 and 3 divides the class number of the cyclotomic field $\mathbf{Q}(\zeta_{59})$. For $l = 11$, $p = 23$: the order of 3 modulo 11 is 5 and 3 divides the class number of the cyclotomic field $\mathbf{Q}(\zeta_{23})$.

It seems that analogous assertions hold if we consider the divisibility of the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ instead of the divisibility of the class number h of the cyclotomic field $\mathbf{Q}(\zeta_p)$.

In [3], it is proved that if p, l are primes such that $p = 2l + 1$ and the prime q is a primitive root modulo l, then q does not divide the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.

In [4], it is proved that if the order of 3 modulo l is $\frac{l-1}{2}$, then 3 does not divide h^+.

AMS Subject Classification (1991): Primary 11R29.
Key words: Class number, Cyclotomic field, Divisibility.

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

THEOREM 1. *Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, and let the order of the prime 5 modulo l be $\frac{l-1}{2}$. Then 5 does not divide the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

This theorem is proved using the following theorem in [3].

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 L, $[K : \mathbf{Q}] = l$ and let h_K be the class number of the field K.*

If $q \mid h_K$, then $q \mid N_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\omega)$, where

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

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

In the following tables, the numbers a_i for $q = 3, 5, 7, 11, 13$ are given. These values were calculated on the basis of [3; p. 73, formula (4)].

Table 1: $q = 3$.

	a_1	a_2
$p \equiv 1 \pmod 3$	0	1
$p \equiv 2 \pmod 3$	1	0

Table 2: $q = 5$.

	a_1	a_2	a_3	a_4
$p \equiv 1 \pmod 5$	0	1	-1	1
$p \equiv 2 \pmod 5$	-1	0	1	1
$p \equiv 3 \pmod 5$	1	1	0	-1
$p \equiv 4 \pmod 5$	1	-1	1	0

Table 3: $q = 7$.

	a_1	a_2	a_3	a_4	a_5	a_6
$p \equiv 1 \pmod 7$	0	1	5	3	5	1
$p \equiv 2 \pmod 7$	5	0	6	4	4	6
$p \equiv 3 \pmod 7$	4	4	0	5	1	5
$p \equiv 4 \pmod 7$	2	6	2	0	3	3
$p \equiv 5 \pmod 7$	1	3	3	1	0	2
$p \equiv 6 \pmod 7$	6	2	4	2	6	0

Table 4: $q = 11$.

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
$p \equiv 1 \pmod{11}$	0	1	7	0	3	1	3	0	7	1
$p \equiv 2 \pmod{11}$	6	0	7	6	0	9	9	0	6	7
$p \equiv 3 \pmod{11}$	0	0	0	1	6	4	4	4	6	1
$p \equiv 4 \pmod{11}$	10	3	10	0	0	9	3	3	9	0
$p \equiv 5 \pmod{11}$	8	5	5	8	0	9	0	9	0	9
$p \equiv 6 \pmod{11}$	2	0	2	0	2	0	3	6	6	3
$p \equiv 7 \pmod{11}$	0	2	8	8	2	0	0	1	8	1
$p \equiv 8 \pmod{11}$	10	5	7	7	7	5	10	0	0	0
$p \equiv 9 \pmod{11}$	4	5	0	2	2	0	5	4	0	5
$p \equiv 10 \pmod{11}$	10	4	0	8	10	8	0	4	10	0

Table 5: $q = 13$.

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
$p \equiv 1 \pmod{13}$	0	1	8	4	1	9	7	9	1	4	8	1
$p \equiv 2 \pmod{13}$	10	0	11	7	7	4	2	2	4	7	7	11
$p \equiv 3 \pmod{13}$	9	9	0	10	3	9	7	11	7	9	3	10
$p \equiv 4 \pmod{13}$	1	5	1	0	2	12	10	10	10	10	12	2
$p \equiv 5 \pmod{13}$	7	12	12	7	0	8	6	8	4	8	6	8
$p \equiv 6 \pmod{13}$	10	11	12	11	10	0	11	5	8	8	5	11
$p \equiv 7 \pmod{13}$	2	8	5	5	8	2	0	3	2	1	2	3
$p \equiv 8 \pmod{13}$	5	7	5	9	5	7	5	0	6	1	1	6
$p \equiv 9 \pmod{13}$	11	1	3	3	3	3	1	11	0	12	8	12
$p \equiv 10 \pmod{13}$	3	10	4	6	2	6	4	10	3	0	4	4
$p \equiv 11 \pmod{13}$	2	6	6	9	11	11	9	6	6	2	0	3
$p \equiv 12 \pmod{13}$	12	5	9	12	4	6	4	12	9	5	12	0

Proof of Theorem 1. Since the order of 5 modulo l is $\frac{l-1}{2}$, we have $\left(\frac{5}{l}\right) = 1$.

$$1 = \left(\frac{5}{l}\right) = \left(\frac{l}{5}\right),$$

hence $l \equiv 1$ or $4 \pmod 5$. From this, we have $p \equiv 3$ or $4 \pmod 5$.

According to Proposition 1 and Table 2 it holds that if $5 \mid h^+$, then $5 \mid \mathrm{N}_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\omega)$, where

$$\omega = \sum_{i \equiv 1 \pmod 5} \chi(i) + \sum_{i \equiv 2 \pmod 5} \chi(i) - \sum_{i \equiv 4 \pmod 5} \chi(i), \qquad \text{for} \quad p \equiv 3 \pmod 5,$$

$$\omega = \sum_{i \equiv 1 \pmod 5} \chi(i) - \sum_{i \equiv 2 \pmod 5} \chi(i) + \sum_{i \equiv 3 \pmod 5} \chi(i), \qquad \text{for} \quad p \equiv 4 \pmod 5,$$

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

$$\tau = \sum_{\substack{i\equiv 1 \pmod 5\\ i<\frac{p}{2}}} \chi(i) + \sum_{\substack{i\equiv 2 \pmod 5\\ i<\frac{p}{2}}} \chi(i) - \sum_{\substack{i\equiv 4 \pmod 5\\ i<\frac{p}{2}}} \chi(i), \qquad \text{for} \quad p \equiv 3 \pmod 5,$$

$$\tau = \sum_{\substack{i\equiv 1 \pmod 5\\ i<\frac{p}{2}}} \chi(i) - \sum_{\substack{i\equiv 2 \pmod 5\\ i<\frac{p}{2}}} \chi(i) + \sum_{\substack{i\equiv 3 \pmod 5\\ i<\frac{p}{2}}} \chi(i), \qquad \text{for} \quad p \equiv 4 \pmod 5.$$

Since the order of 5 modulo l is $\frac{l-1}{2}$, we have that 5 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 $5 \mid \mathrm{N}_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\omega)$, then 5 divides $\tau\overline{\tau}$.

The proof will be in two steps: I. $p \equiv 4 \pmod 5$; II. $p \equiv 3 \pmod 5$.

I. case: $p \equiv 4 \pmod 5$.

The following formula holds:

$$\tau\overline{\tau} = \sum_{\substack{i,j\equiv 1:2:3 \pmod 5\\ i,j<\frac{p}{2}}} a_{ij}\chi(ij^{-1}) = b_0 + b_1\zeta_l + b_2\zeta_l^2 + \cdots + b_{l-1}\zeta^{l-1}, \tag{1}$$

where $a_{11} = 1$, $a_{12} = -1$, $a_{13} = 1$, $a_{21} = -1$, $a_{22} = 1$, $a_{23} = -1$, $a_{31} = 1$, $a_{32} = -1$, $a_{33} = 1$.

Then $5 \mid \tau\overline{\tau}$ if and only if

$$b_0 \equiv b_1 \equiv \cdots \equiv b_{l-1} \pmod 5.$$

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 $i + j \equiv 0 \pmod p$ $i,j < \frac{p}{2}$. Hence $i \equiv j \pmod p$.

The following equalities hold

$$\#\left\{i \equiv 1 \pmod 5,\ i < \frac{p}{2}\right\} = \frac{p+1}{10},$$

$$\#\left\{i \equiv 2 \pmod 5,\ i < \frac{p}{2}\right\} = \frac{p+1}{10},$$

$$\#\left\{i \equiv 3 \pmod 5,\ i < \frac{p}{2}\right\} = \frac{p+1}{10}.$$

Since $a_{11} = a_{22} = a_{33} = 1$, we get

$$b_0 = 3\frac{p+1}{10}.$$

Let $k < l$; $g^k \equiv 2$ or $-2 \pmod p$. We shall prove that the coefficient $b_k = 0$. Let $\chi(ij^{-1}) = \zeta_l^k$, then either $\mathrm{ind}(ij^{-1}) = k$ or $\mathrm{ind}(ij^{-1}) = k+l$, and therefore either

$$ij^{-1} \equiv 2 \pmod p \qquad \text{or} \qquad ij^{-1} \equiv -2 \pmod p\,,$$

$$i, j < \frac{p}{2}\,; \quad i, j \equiv 1; 2; 3 \pmod 5\,.$$

Since $a_{13} = a_{33} = 1$, $a_{21} = -1$, and $p \equiv 4 \pmod 5$, we obtain

$$b_k = \#\Big\{j \equiv 3 \pmod 5\,;\ j < \frac{p}{2}\Big\} - \#\Big\{j \equiv 1 \pmod 5\,;\ j < \frac{p}{2}\Big\} = 0\,.$$

Hence, if $5 \mid \tau\overline{\tau}$, then

$$b_0 \equiv b_k \equiv 0 \pmod 5\,, \qquad \text{hence} \quad p + 1 \equiv 0 \pmod{25}\,.$$

To prove the theorem, it is sufficient to show that there is a coefficient $b_t \not\equiv 0 \pmod 5$ in (1).

Let I_1, I_2 denote the sets of all integral numbers x

$$I_1 : \ \frac{p}{5} < x < \frac{2p}{5}\,; \qquad I_2 : \ \frac{2p}{5} < x < \frac{p}{2}\,.$$

Multiply the integers in the set I_1 by 5 and reduce by modulo p. In such a way we get numbers $x_1, x_2, \dots, x_r$. We take the numbers $y_1, y_2, \dots, y_r$ in the following way: if $x_i < \frac{p}{2}$, then $y_i = x_i$, and if $x_i > \frac{p}{2}$, then $y_i = p - x_i$. It is easy to see that

$$\{y_1, y_2, \dots, y_r\} = \Big\{i \equiv 1\,;\ 3 \pmod 5\,,\ i < \frac{p}{2}\Big\}\,.$$

Analogously, the 5th multiplier of interval I_2 (reduced modulo p) is equal to the set $\Big\{i \equiv 2 \pmod 5\,,\ i < \frac{p}{2}\Big\}$.

Let N be a positive integer $N \equiv 0 \pmod 2$. Consider the numbers:

$$s_1 = \#\Big\{x\,,\ \Big[\frac{5Nx}{p}\Big] \equiv 1 \pmod 5\,;\ x \in I_1\Big\}\,,$$

$$s_2 = \#\Big\{x\,,\ \Big[\frac{5Nx}{p}\Big] \equiv 1 \pmod 5\,;\ x \in I_2\Big\}\,,$$

$$t_1 = \#\Big\{x\,,\ \Big[\frac{5Nx}{p}\Big] \equiv 3 \pmod 5\,;\ x \in I_1\Big\}\,,$$

$$t_2 = \#\Big\{x\,,\ \Big[\frac{5Nx}{p}\Big] \equiv 3 \pmod 5\,;\ x \in I_2\Big\}\,,$$

$$r_1 = \#\Big\{x\,,\ \Big[\frac{5Nx}{p}\Big] \equiv 2 \pmod 5\,;\ x \in I_1\Big\}\,,$$

$$r_2 = \#\Big\{x\,,\ \Big[\frac{5Nx}{p}\Big] \equiv 2 \pmod 5\,;\ x \in I_2\Big\}\,.$$

It is easy to see that

$$S = s_1 - s_2 + t_1 - t_2 - r_1 + r_2$$

is equal to some coefficient from (1).

Now we express the numbers s_1, s_2, t_1, t_2, r_1, r_2 by sums of integral parts.

Let $N \equiv 1 \pmod 5$. Then it holds:

$$s_1 = \sum_{i=0}^{\left[\frac{N-1}{5}\right]} \left(\left[\frac{(N+1+5i)p}{5N}\right] - \left[\frac{(N+5i)p}{5N}\right] \right),$$

$$s_2 = \sum_{i=\left[\frac{N-1}{5}\right]+1}^{\left[\frac{3N-2}{10}\right]} \left(\left[\frac{(N+1+5i)p}{5N}\right] - \left[\frac{(N+5i)p}{5N}\right] \right),$$

$$t_1 = \sum_{i=0}^{\left[\frac{N-3}{5}\right]} \left(\left[\frac{(N+3+5i)p}{5N}\right] - \left[\frac{(N+2+5i)p}{5N}\right] \right),$$

$$t_2 = \sum_{i=\left[\frac{N-3}{5}\right]+1}^{\left[\frac{3N-6}{10}\right]} \left(\left[\frac{(N+3+5i)p}{5N}\right] - \left[\frac{(N+2+5i)p}{5N}\right] \right),$$

$$r_1 = \sum_{i=0}^{\left[\frac{N-2}{5}\right]} \left(\left[\frac{(N+2+5i)p}{5N}\right] - \left[\frac{(N+1+5i)p}{5N}\right] \right),$$

$$r_2 = \sum_{i=\left[\frac{N-2}{5}\right]+1}^{\left[\frac{3N-4}{10}\right]} \left(\left[\frac{(N+2+5i)p}{5N}\right] - \left[\frac{(N+1+5i)p}{5N}\right] \right).$$

Let $0 < z < 5N$. Define the numbers S_1, S_2, T_1, T_2, R_1, R_2 dependent on z in the following way

$$S_1 = \sum_{i=0}^{\left[\frac{N-1}{5}\right]} \left(\left[\frac{(N+1+5i)z}{5N}\right] - \left[\frac{(N+5i)z}{5N}\right] \right),$$

$$S_2 = \sum_{i=\left[\frac{N-1}{5}\right]+1}^{\left[\frac{3N-2}{10}\right]} \left(\left[\frac{(N+1+5i)z}{5N}\right] - \left[\frac{(N+5i)z}{5N}\right] \right),$$

$$T_1 = \sum_{i=0}^{\left[\frac{N-3}{5}\right]} \left(\left[\frac{(N+3+5i)z}{5N} \right] - \left[\frac{(N+2+5i)z}{5N} \right] \right),$$

$$T_2 = \sum_{i=\left[\frac{N-3}{5}\right]+1}^{\left[\frac{3N-6}{10}\right]} \left(\left[\frac{(N+3+5i)z}{5N} \right] - \left[\frac{(N+2+5i)z}{5N} \right] \right),$$

$$R_1 = \sum_{i=0}^{\left[\frac{N-2}{5}\right]} \left(\left[\frac{(N+2+5i)z}{5N} \right] - \left[\frac{(N+1+5i)z}{5N} \right] \right),$$

$$R_2 = \sum_{i=\left[\frac{N-2}{5}\right]+1}^{\left[\frac{3N-4}{10}\right]} \left(\left[\frac{(N+2+5i)z}{5N} \right] - \left[\frac{(N+1+5i)z}{5N} \right] \right).$$

Let $p = 5Nk + z$; then

$$\begin{aligned} S =& k\left(\left[\frac{N-1}{5}\right]+1\right) - k\left(\left[\frac{3N-2}{10}\right] - \left[\frac{N-1}{5}\right]\right) + k\left(\left[\frac{N-3}{5}\right]+1\right) \\ & - k\left(\left[\frac{3N-6}{10}\right] - \left[\frac{N-3}{5}\right]\right) - k\left(\left[\frac{N-2}{5}\right]+1\right) + k\left(\left[\frac{3N-4}{10}\right] - \left[\frac{N-2}{5}\right]\right) \\ & + S_1 - S_2 + T_1 - T_2 - R_1 + R_2 . \end{aligned}$$

Clearly,

$$k = \frac{p-z}{5N} = \frac{p+1-(z+1)}{5N} \equiv -\frac{z+1}{5} \pmod 5 .$$

Finally,

$$S = S_N(z) \equiv -\frac{z+1}{5}\frac{N+14}{10} + S_1 - S_2 + T_1 - T_2 - R_1 + R_2 \pmod 5 .$$

Lemma 1. *If $N = 6^n$, then*

$$S_N\left(5 \cdot \frac{N}{6} - 1\right) \not\equiv 0 \pmod 5 .$$

Proof. If we substitute $z = 5 \cdot \dfrac{N}{6} - 1$ to the sums S_1, S_2, T_1, T_2, R_1, R_2, we get:

$$S_1 = \#\Big\{ i \equiv 4 \pmod 6\,, \quad i \in \Big\langle \Big[\frac{2N}{15}\Big] + 1,\ \Big[\frac{N-1}{5}\Big] \Big\rangle\,,$$
$$i \equiv 5 \pmod 6\,, \quad i \in \Big\langle 0,\ \Big[\frac{2N-13}{15}\Big] \Big\rangle \Big\}\,,$$
$$S_2 = \#\Big\{ i \equiv 4 \pmod 6\,, \quad i \in \Big\langle \Big[\frac{N-1}{5}\Big] + 1, \Big[\frac{3N-2}{10}\Big] \Big\rangle \Big\}\,.$$

It follows that

$$S_1 = \frac{\frac{N}{6} - 6}{5}\,; \qquad S_2 = \frac{\frac{N}{6} + 4}{10}\,,$$

$$T_1 = \#\Big\{ i \equiv 0 \pmod 6\,, \quad i \in \Big\langle \Big[\frac{2N-6}{15}\Big] + 1, \Big[\frac{N-3}{5}\Big] \Big\rangle\,,$$
$$i \equiv 1 \pmod 6\,, \quad i \in \Big\langle 0, \Big[\frac{2N-9}{15}\Big] \Big\rangle \Big\}\,,$$
$$T_2 = \#\Big\{ i \equiv 0 \pmod 6\,, \quad i \in \Big\langle \Big[\frac{N-3}{5}\Big] + 1, \Big[\frac{3N-6}{10}\Big] \Big\rangle \Big\}\,.$$

Hence

$$T_1 = \frac{\frac{N}{6} + 4}{5}\,; \qquad T_2 = \frac{\frac{N}{6} - 6}{10}\,,$$

$$R_1 = \#\Big\{ i \equiv 5 \pmod 6\,, \quad i \in \Big\langle \Big[\frac{2N-3}{15}\Big] + 1, \Big[\frac{N-2}{5}\Big] \Big\rangle\,,$$
$$i \equiv 0 \pmod 6\,, \quad i \in \Big\langle 0, \Big[\frac{2N-6}{15}\Big] \Big\rangle \Big\}\,,$$
$$R_2 = \#\Big\{ i \equiv 5 \pmod 6\,, \quad i \in \Big\langle \Big[\frac{N-2}{5}\Big] + 1, \Big[\frac{3N-4}{10}\Big] \Big\rangle \Big\}\,.$$

Therefore

$$R_1 = \frac{\frac{N}{6} + 4}{5}\,; \qquad R_2 = \frac{\frac{N}{6} - 6}{10}\,.$$

Furthermore,

$$\frac{z+1}{5} = \frac{5 \cdot \dfrac{N}{6} - 1 + 1}{5} \equiv 1 \pmod 5 .$$

Now we have

$$S_N\Big(5 \cdot \frac{N}{6} - 1\Big) \equiv -1 \not\equiv 0 \pmod 5 .$$

Lemma 1 is proved.

Now we shall show that there exists a coefficient $b_t \not\equiv 0 \pmod 5$ in (1).

Let n be such that $p \not\equiv -1 \pmod{5 \cdot 6^n}$. Let $p \equiv z \pmod{5 \cdot 6^n}$. Generate the sequence $z_1, z_2, \dots, z_{n-2}$ in the following way

$$z_i \equiv z \pmod{5 \cdot 6^{n-i}}, \qquad z_i < 5 \cdot 6^{n-i} .$$

If $S_{6^{n-i}}(z_i) \not\equiv 0 \pmod 5$ for some i, then we take $N = 6^{n-i}$ and the theorem is proved. Otherwise, let

$$S_{6^{n-1}}(z_1) \equiv S_{6^{n-2}}(z_2) \equiv \cdots \equiv S_{6^2}(z_{n-2}) \equiv 0 \pmod 5 .$$

Supposing that $p \not\equiv -1 \pmod{5 \cdot 6^n}$, by Lemma 1 we have

$$z_i \neq 5 \cdot 6^{n-i} - 1 ; \qquad z_i \neq 5 \cdot 6^{n-i-1} - 1 . \tag{2}$$

Possible values for a prime number p modulo 180 are 59 or 119 or 179 (it follows from $p \equiv -1 \pmod 5$, $p \equiv -1 \pmod 3$, $p \equiv -1 \pmod 4$.)

By (2) and the induction we get $z_{n-2} = 59$ or 119. By computation we shall verify that $S_{36}(59) \not\equiv 0 \pmod 5$ and $S_{36}(119) \not\equiv 0 \pmod 5$. This contradicts the fast that $S_{36}(z_{n-2}) \equiv 0 \pmod 5$. The theorem is proved for $p \equiv 4 \pmod 5$.

II. case: $p \equiv 3 \pmod 5$.

In this situation we have

$$\tau\overline{\tau} = \sum_{\substack{i,j \equiv 1;2;4 \pmod 5 \\ i,j < \frac{p}{2}}} a_{ij}\chi(ij^{-1}) = b_0 + b_1\zeta_l + b_2\zeta_l^2 + \cdots + b_{l-1}\zeta^{l-1} , \tag{3}$$

where $a_{11} = 1$, $a_{12} = 1$, $a_{14} = -1$, $a_{21} = 1$, $a_{22} = 1$, $a_{24} = -1$, $a_{41} = -1$, $a_{42} = -1$, $a_{44} = 1$.

Analogously as in case I, we obtain $b_0 \equiv 1 \pmod 5$ in (3). Let $N \equiv 0 \pmod 2$. Define S_1, S_2, T_1, T_2, R_1, R_2 analogously as in case I.

Similarly as in case I, we prove that $p \equiv 3 \pmod{25}$. In the same way as in case I, we shall define the numbers $S_N(z)$.

$$S_N(z) = \frac{3-z}{5N} \cdot \frac{N+14}{10} + S_1 - S_2 + T_1 - T_2 - R_1 + R_2\,, \quad \text{for } N \equiv 1 \pmod 5\,,$$
$$S_N(z) = \frac{3-z}{5N} \cdot \frac{N-2}{10} + S_1 - S_2 + T_1 - T_2 - R_1 + R_2\,, \quad \text{for } N \equiv 2 \pmod 5\,,$$
$$S_N(z) = \frac{3-z}{5N} \cdot \frac{N+2}{10} + S_1 - S_2 + T_1 - T_2 - R_1 + R_2\,, \quad \text{for } N \equiv 3 \pmod 5\,,$$
$$S_N(z) = \frac{3-z}{5N} \cdot \frac{N-14}{10} + S_1 - S_2 + T_1 - T_2 - R_1 + R_2\,, \quad \text{for } N \equiv 4 \pmod 5\,.$$

LEMMA 2. *Let $N = 2^n$, then*

$$S_N\Big(5 \cdot \frac{N}{2} + 3\Big) \not\equiv 1 \pmod 5\,.$$

P r o o f. This is analogous to Lemma 1. Here we consider the cases $N \equiv 1, 2, 3, 4 \pmod 5$.

The proof of the theorem is similar as in case I. Now we take n such that $p \not\equiv 3 \pmod{5.2^n}$.

REFERENCES

[1] DAVIS, D.: *Computing the number of totally positive circular units which are squares*, J. Number Theory **10** (1978), 1–9.

[2] ESTES, D. R.: *On the parity of the class number of the field of q-th roots of unity*, Rocky Mountain J. Math. **19** (1989), 675–681.

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

[4] JAKUBEC, S.: *On divisibility of h^+ by the prime* 3, Rocky Mountain J. Math. (1992) (To appear).

Received July 22, 1993

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK-814 73 Bratislava
Slovakia