ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 24, Number 4, Fall 1994

ON THE DIVISIBILITY OF h^+ BY THE PRIME 3

STANISLAV JAKUBEC

Introduction. Let l and p be primes such that $p = 2l + 1$. In the paper [**1**] it is proved that if 2 is a primitive root modulo l then 2 does not divide class number of real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. In the paper [**3**] it is proved that the same result holds for arbitrary prime q which is primitive root modulo l. In [**2**] it is shown that, provided the order of 2 modulo l is $(l-1)/2$ and 2 is prime in the real subfield of $\mathbf{Q}(\zeta_l)$, then 2 does not divide the class number of real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.

The aim of this paper is to prove the same result for the prime 3.

The following theorem holds.

Theorem. *Let l and p be primes such that $l > 3$, $p = 2l + 1$, and the order of* 3 *modulo l is $(l-1)/2$. Then* 3 *does not divide the class number h^+ of real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

Proof. Clearly $l \equiv p \equiv 2 \pmod 3$. Since the order of 3 modulo l is $(l-1)/2$ we have $(3/l) = 1$. If $l \equiv 1 \pmod 4$, then

$$1 = (3/l) = (l/3) = (2/3) = -1.$$

Hence $l \equiv 3 \pmod 4$ and it follows that 3 is prime in the real subfield of $\mathbf{Q}(\zeta_l)$.

In [**3**] it is proved if $3|h^+$ then $3|N_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\omega)$, where

$$\omega = \sum_{i \equiv 1 \pmod 3} \chi(i),$$

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

Received by the editors on July 10, 1992, and in revised form on March 18, 1993.
AMS *Mathematics Subject Classification* (1991). Primary 11R29.

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

$$\tau = \sum_{\substack{i \equiv 1 \pmod 3 \\ i < p/2}} \chi(i).$$

Since the order of 3 modulo l is $(l-1)/2$ and 3 is prime in the real subfield of $\mathbf{Q}(\zeta_1)$, we have $3 | N_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\omega)$ if and only if $\tau\bar{\tau} \equiv 0 \pmod 3$. For a proof of the theorem it is sufficient to prove $\tau\bar{\tau} \not\equiv 0 \pmod 3$.

Let

$$\tau\bar{\tau} = a_0 + a_1\zeta_l + a_2\zeta_l^2 + \cdots + a_{l-1}\zeta^{l-1}. \tag{1}$$

Then $3|\tau\bar{\tau}$ if and only if

$$a_0 \equiv a_1 \equiv \cdots \equiv a_{l-1} \pmod 3.$$

The following formula holds

$$\tau\bar{\tau} = \sum_{\substack{i,j \equiv 1 \pmod 3 \\ i,j < p/2}} \chi(ij^{-1}).$$

Clearly

$$a_0 = \#\{i : i \equiv 1 \pmod 3,\ i < p/2\} = (p+1)/6.$$

Determine the coefficient a_k from equality (1). $\chi(xy^{-1}) = \zeta_l^k$, so $\operatorname{ind}(xy^{-1}) = k$ or $\operatorname{ind}(xy^{-1}) = k + l$.

From the above we have

$$xy^{-1} \equiv g^k \pmod p \quad \text{or} \quad xy^{-1} \equiv -g^k \pmod p.$$

Since $x \equiv 1 \pmod 3$ if and only if $p - x \equiv 1 \pmod 3$, it follows that

$$a_k = \#\left\{ y : y \equiv 1 \pmod 3,\ y < p/2,\ g^k y - p\left[\frac{g^k y}{p}\right] \equiv 1 \pmod 3 \right\}.$$

Let $g^k \equiv 2 \pmod p$, then

$$a_k = \#\{y : y \equiv 1 \pmod 3,\ y < p/2,\ 2y \equiv 1 \pmod 3\} = 0.$$

To complete the proof it is only necessary to exhibit an index j between 0 and $l-1$ such that $a_j \not\equiv 0 \pmod 3$. In the event $(p+1)/6$ is not divisible by 3,

$$a_0 = (p+1)/6 \not\equiv a_k = 0 \pmod 3,$$

hence we can assume for the remainder of the article that $p+1 \equiv 0 \pmod 9$.

Let I denote the set of all integral numbers x,

$$p/3 < x < p/2.$$

If the elements from the set I are multiplied by 3 and then reduced modulo p, we get the set

$$\{i : i \equiv 1 \pmod 3,\ i < p/2\}.$$

Let N be a positive integer. It is easy to see that the number of solutions to the following congruence

$$3Nx - p[3Nx/p] \equiv 1 \pmod 3; \qquad x \in I, \tag{2}$$

is equal to some a_j from (1).

The congruence

$$3Nx - p[3Nx/p] \equiv 1 \pmod 3; \qquad x \in I$$

holds if and only if

$$[3Nx/p] \equiv 1 \pmod 3; \qquad x \in I.$$

Hence

$$ap < 3Nx < (a+1)p, \quad \text{where } a \equiv 1 \pmod 3;$$

therefore

$$\frac{ap}{3N} < x < \frac{(a+1)p}{3N}.$$

The number of integers in this range is

$$\left[\frac{(a+1)p}{3N}\right] - \left[\frac{ap}{3N}\right].$$

Suppose now that $N \equiv 4 \pmod 6$.

Then the number of solutions for convergence (2) is

$$S = \sum_{i=0}^{[N/6]} \left(\left[\frac{(N+1+3i)p}{3N} \right] - \left[\frac{(N+3i)p}{3N} \right] \right).$$

Let $p = 3Nt + z$, hence

$$S = t\left(\left[\frac{N}{6} \right] + 1 \right) + \sum_{i=0}^{[N/6]} \left(\left[\frac{(N+1+3i)z}{3N} \right] - \left[\frac{(N+3i)z}{3N} \right] \right).$$

For the number t the following congruence holds

$$t = \frac{p-z}{3N} \equiv \frac{p+1-(z+1)}{3N} \equiv -\frac{z+1}{3} \pmod 3.$$

Hence

$$\begin{aligned} S \equiv & -\frac{z+1}{3}\left(\left[\frac{N}{6} \right] + 1 \right) \\ & + \sum_{i=0}^{[N/6]} \left(\left[\frac{(N+1+3i)z}{3N} \right] - \left[\frac{(N+3i)z}{3N} \right] \right) \pmod 3. \end{aligned}$$

For $N \equiv 2 \pmod 6$, we similarly obtain

$$\begin{aligned} S \equiv & \frac{z+1}{3}\left(\left[\frac{N-4}{6} \right] + 1 \right) \\ & + \sum_{i=0}^{[(N-4)/6]} \left(\left[\frac{N+3+3i)z}{3N} \right] - \left[\frac{(N+2+3i)z}{3N} \right] \right) \pmod 3. \end{aligned}$$

The prime p is congruent to one of

$$z = 5 + 6j; \qquad j = 0, 1, \dots, ((N/2) - 1),$$

modulo $3N$.

Define the numbers $S_N(z)$ by the following way:

$$S_N(z) = -\frac{z+1}{3}\left(\left[\frac{N}{6}\right]+1\right) + \sum_{i=0}^{[N/6]}\left(\left[\frac{(N+1+3i)z}{3N}\right] - \left[\frac{(N+3i)z}{3N}\right]\right),$$

for $N \equiv 1 \pmod 3$; $N \equiv 0 \pmod 2$, $z = 5+6j$; $j = 0, 1, \dots, ((N/2)-1)$ and

$$S_N(z) = \frac{z+1}{3}\left(\left[\frac{N-4}{6}\right]+1\right) + \sum_{i=0}^{[(N-4)/6]}\left(\left[\frac{(N+3+3i)z}{3N}\right] - \left[\frac{(N+2+3i)z}{3N}\right]\right),$$

for $N \equiv 2 \pmod 3$; $N \equiv 0 \pmod 2$, $z = 5+6j$; $j = 0, 1, \dots, ((N/2)-1)$.

Lemma 1. *Let $N = 2^n$, $n > 2$. Then*

$$S_{2^n}(3.2^{n-1}-1) \not\equiv 0 \pmod 3.$$

Proof. Suppose that $2^n \equiv 1 \pmod 3$

$$S_{2^n}(3.2^{n-1}-1) = -2^{n-1}([2^n/6]+1) + \sum_{i=0}^{[2^n/6]}\left(\left[\frac{(2^n+1+3i)(3.2^{n-1}-1)}{3.2^n}\right] - \left[\frac{(2^n+3i)(3.2^{n-1}-1)}{3.2^n}\right]\right).$$

It is easy to see that:

$$\left[\frac{(2^n+1+3i)(3.2^{n-1}-1)}{3.2^n}\right] = 2^{n-1} + \left[\frac{3i}{2}\right],$$

$$\left[\frac{(2^n+3i)(3.2^{n-1}-1)}{3.2^n}\right] = \begin{cases} 2^{n-1} + [3i/2], & \text{for } i \equiv 1 \pmod 2, \\ 2^{n-1} + [3i/2] - 1, & \text{for } i \equiv 0 \pmod 2, \end{cases}$$

and we get

$$S_{2^n}(3.2^{n-1}-1) = f - 2^{n-1}([2^n/6]+1),$$

where f is the number of even numbers (also zero) from zero to $[2^n/6]$.

$$\left[\frac{2^n}{6}\right] = \left[\frac{2^{n-1}}{3}\right] = \frac{2^{n-1}-2}{3},$$

so $f = (2^{n-1}-2)/6+1$, and we have $S_{2^n}(3.2^{n-1}-1) \not\equiv 0 \pmod 3$. The proof is similar in the remaining case ($2^n \equiv 2 \pmod 3$). □

Lemma 2. *There exists* $N = 2^n$ *such that* 3 *does not divide the number of solutions for congruence* (2).

Proof. Take s such that $p+1 \not\equiv 0 \pmod{3.2^s}$. Let $p \equiv z \pmod{3.2^s}$, so $z \neq 3.2^s - 1$.

Generate the sequence z_i, $i = 1, 2, \dots, s-3$ by the following way

$$z_i \equiv z \pmod{3.2^{s-i}}, \qquad 0 < z_i < 3.2^{s-i}.$$

Clearly, $p \equiv z_i \pmod{3.2^{s-i}}$.

If $S_{2^{s-i}}(z_i) \not\equiv 0 \pmod 3$ for some i, then we take $N = 2^{s-i}$ and Lemma 2 is proved. □

So let

$$S_{2^s}(z) \equiv S_{2^{s-1}}(z_1) \equiv \cdots \equiv S_{2^3}(z_{s-3}) \equiv 0 \pmod 3.$$

By supposition $z \neq 3.2^s - 1$ and, according to Lemma 1, $z \neq 3.2^{s-1}-1$. Then $z_1 \neq 3.2^{s-1}-1$ and, according to Lemma 2, $z_1 \neq 3.2^{s-2}-1$. By the induction we get $z_{s-3} \neq 3.8-1$. Then by computation it is easy to see $S_8(z_{s-3}) \not\equiv 0 \pmod 3$. Lemma 2 is proved. According to Lemma 2 there exists such a j that coefficient $a_j \not\equiv 0 \pmod 3$. Hence $\tau\bar{\tau} \not\equiv 0 \pmod 3$. The theorem is proved. □

REFERENCES

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

2. D.R. Estes, *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. 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, Czechoslovakia