ACTA ARITHMETICA
145.4 (2010)

On the class number of some real abelian number fields of prime conductors

by

Stanislav Jakubec (Bratislava)

1. Introduction. The aim of this paper is to prove two theorems on the class number h_K.

Theorem 1. *Let $p = 4l + 1$ and l be odd primes. Let $K \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $[K : \mathbb{Q}] = l$ and let h_K be the class number of the field K. Let q be an odd prime with $3 < q < \sqrt{p}$. If q is a primitive root modulo l then q does not divide h_K.*

Theorem 2. *Let $p = 6l + 1$ and l be odd primes. Let $K \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $[K : \mathbb{Q}] = l$ and let h_K be the class number of the field K. Let q be an odd prime with $3 < q < \sqrt{p}/2$. If q is a primitive root modulo l then q does not divide h_K.*

Using Schinzel's conjecture for linear polynomials (see [5] and [4, p. 56]) we prove that for each prime q there exist infinitely many prime numbers p satisfying the assumptions of Theorems 1 and 2.

Proposition. *Assume that Schinzel's conjecture for linear polynomials holds true. Then, for any given prime $q > 3$, there are infinitely many pairs of primes (l, p) of the form $p = 4l + 1$ (respectively, of the form $p = 6l + 1$), for which q is a primitive root modulo l.*

Proof. Let $l = 2r + 1$ where r is an odd prime. Then q is a primitive root modulo l if and only if $q \not\equiv 0, \pm 1 \pmod{l}$ and the Legendre symbol $\left(\frac{q}{l}\right)$ equals -1.

Because $l \equiv 3 \pmod 4$, by the quadratic reciprocity law we have

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

2010 *Mathematics Subject Classification*: Primary 11R29.
Key words and phrases: class number.

DOI: 10.4064/aa145-4-1

Let the residues modulo q be represented by odd numbers $\{1,3,\ldots,2q-1\}$. Let $z\in\{1,3,\ldots,2q-1\}$, $z\neq q$, $z\neq 1$, $z\neq (q-1)/4$. Put

$$r=f_1(X)=qX+\frac{z-1}{2},\ l=f_2(X)=2qX+z,\ p=f_3(X)=8qX+4z+1,$$

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

If $z\neq 1$, $z\neq q$, $z\neq (q-1)/4$ then the linear polynomials $f_1(X)$, $f_2(X)$, $f_3(X)$ satisfy the assumptions of Schinzel's conjecture and consequently the prime numbers q,l,p satisfy the assumptions of Theorem 1. In the case of Theorem 2 we consider the polynomials

$$r=f_1(X)=qX+\frac{z-1}{2},\ l=f_2(X)=2qX+z,\ p=f_3(X)=12qX+6z+1. \blacksquare$$

Our approach is based on the results [1] and [2] (see also [3]). Let q be an odd prime. Let $j\mapsto A(j)$ be the q-periodic function defined by

$$A(0)=0,\qquad A(j)=\sum_{i=1}^{j}\frac{1}{i}\qquad\text{for } j=1,\ldots,q-1.$$

Let s be a rational q-integer. Put $A(s)=A(j)$ where j is an integer, $0\leq j<q$, and $s\equiv j \pmod q$.

For $i=1,\ldots,q-1$ we have the congruence $A(i-1)\equiv A(q-i) \pmod q$. This implies that

$$A\left(\frac{-i}{p}\right)\equiv A\left(\frac{-(p-i)}{p}\right) \pmod q\qquad\text{for } i=1,\ldots,p-1.$$

From [1]–[3], we have

Proposition 1. *Let l, p, q be primes, $p\equiv 1 \pmod l$, $q\neq 2$, $q\neq l$, $q<p$. Suppose that q is a primitive root modulo l. If q divides h_K, and $[K:\mathbb{Q}]=l$, then*

$$\sum_{j\in X}A\left(\frac{-j}{p}\right)\equiv\sum_{j\in Y}A\left(\frac{-j}{p}\right) \pmod q$$

for any cosets $X,Y\subset\{1,\ldots,p-1\}$ of the subgroup H of index l in $(\mathbb{Z}/p\mathbb{Z})^*$.

Proof of Theorem 1. Let $H=\{1,-1,a/b,-a/b\}$ be the subgroup of order four of $(\mathbb{Z}/p\mathbb{Z})^*$ where $p=a^2+b^2$, $a,b>0$. Then $bH=\{a,p-a,b,p-b\}$ and $xbH=\{ax,p-ax,b,p-bx\}$. By Proposition 1 and since $A(-i/p)\equiv A(-(p-i)/p) \pmod q$, the following congruence holds if $q\mid h_K$, for $x=1,\ldots,[\sqrt{p}]$:

$$A\left(\frac{-a}{p}\right)+A\left(\frac{-b}{p}\right)\equiv A\left(\frac{-ax}{p}\right)+A\left(\frac{-bx}{p}\right) \pmod q.$$

Further let B_n and $B_n(X)$ denote the Bernoulli numbers and Bernoulli polynomials (see [4]).

Let $-a/p \equiv k \pmod{q}$ for an integer k, $0 \le k < q$, hence $A(-a/p) \equiv A(k) \pmod{q}$, so

$$A\left(\frac{-a}{p}\right) \equiv \sum_{i=1}^{k} i^{q-2} \equiv \frac{1}{q-1}\left(B_{q-1}\left(k+1\right) - B_{q-1}\right) \pmod{q}.$$

Since $B_n(1-x) = (-1)^n B_n(x)$ we have

$$\begin{aligned} A\left(\frac{-a}{p}\right) &\equiv \frac{1}{q-1}\left(B_{q-1}\left(\frac{-a}{p}+1\right) - B_{q-1}\right) \\ &\equiv \frac{1}{q-1}\left(B_{q-1}\left(\frac{a}{p}\right) - B_{q-1}\right) \pmod{q}. \end{aligned}$$

Let $F(x)$ be the polynomial

$$F(x) = B_{q-1}\left(\frac{ax}{p}\right) + B_{q-1}\left(\frac{bx}{p}\right) - B_{q-1}\left(\frac{a}{p}\right) - B_{q-1}\left(\frac{b}{p}\right).$$

The numbers $x = 1, \ldots, [\sqrt{p}]$ are roots of $F(x)$ modulo q. As $\deg F(x) < q$ we see that $F(x)$ has more roots modulo q than its degree. However, we will prove that $F(x)$ is not identically zero modulo q. The coefficient of x^{q-3} in $F(x)$ is equal to

$$c_{q-3} = \binom{q-1}{2} B_2 \frac{1}{p^{q-3}}(a^{q-3} + b^{q-3}).$$

We will prove that $c_{q-3} \not\equiv 0 \pmod{q}$. This is so if $ab \equiv 0 \pmod{q}$, since $a^2 + b^2 = p \not\equiv 0 \pmod{q}$. If $ab \not\equiv 0 \pmod{q}$, then

$$a^2 b^2 (a^{q-3} + b^{q-3}) \equiv a^2 + b^2 \equiv p \not\equiv 0 \pmod{q},$$

hence $c_{q-3} \not\equiv 0 \pmod{q}$. ∎

Proof of Theorem 2. Let H be the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of order six, $4p = a^2 + 3b^2$, $a, b > 0$, hence $a^2/b^2 \equiv -3 \pmod{p}$. It follows that

$$\frac{1}{2}\left(-1 + \frac{a}{b}\right), \frac{1}{2}\left(-1 - \frac{a}{b}\right) \in H.$$

This implies that

$$\left\{b, \frac{-b+a}{2}, \frac{a+b}{2}\right\} \subset bH \quad \text{and} \quad \left\{b, \frac{b-a}{2}, \frac{a+b}{2}\right\} \subset bH.$$

Let us consider the case when all three numbers are positive, for example in the first triple. Since $a^2 + 3b^2 = 4p$, we have $a < 2\sqrt{p}$, $b < 2\sqrt{p}$, $(-b+a)/2 < 2\sqrt{p}$, $(b+a)/2 < 2\sqrt{p}$. Just as in the proof of Theorem 1, if $q \mid h_K$, then the polynomial

$$F(x) = B_{q-1}\left(\frac{bx}{p}\right) + B_{q-1}\left(\frac{\frac{-b+a}{2}x}{p}\right) + B_{q-1}\left(\frac{\frac{b+a}{2}x}{p}\right) - B_{q-1}\left(\frac{b}{p}\right) - B_{q-1}\left(\frac{\frac{-b+a}{2}}{p}\right) - B_{q-1}\left(\frac{\frac{b+a}{2}}{p}\right)$$

has modulo q the roots $x = 1, \dots, [\sqrt{p}/2]$. However, we will prove that $F(x)$ is not identically zero modulo q.

The coefficient of x^{q-3} in $F(x)$ is equal to

$$c_{q-3} = \binom{q-1}{2} B_2 \frac{1}{p^{q-3}} \left(b^{q-3} + \left(\frac{a-b}{2}\right)^{q-3} + \left(\frac{a+b}{2}\right)^{q-3}\right).$$

We will prove that $c_{q-3} \not\equiv 0 \pmod{q}$. This is so if $b\frac{a-b}{2}\frac{a+b}{2} \equiv 0 \pmod{q}$, since $a^2 + 3b^2 = 4p \not\equiv 0 \pmod{q}$. If $b\frac{a-b}{2}\frac{a+b}{2} \not\equiv 0 \pmod{q}$, then

$$b^2(a-b)^2(a+b)^2\left(b^{q-3} + \left(\frac{a-b}{2}\right)^{q-3} + \left(\frac{a+b}{2}\right)^{q-3}\right)$$
$$\equiv (a-b)^2(a+b)^2 + 4b^2(a-b)^2 + 4b^2(a+b)^2 \equiv (a^2+3b^2)^2 \equiv 16p^2 \not\equiv 0 \pmod{q},$$

hence $c_{q-3} \not\equiv 0 \pmod{q}$. ∎

Acknowledgments. The author thanks the referees for their remarks that improved the readability of the paper.

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.

[2] —, *On divisibility of the class number h^+ of the real cyclotomic fields of prime degree l*, Math. Comp. 67 (1998), 369–398.

[3] T. Metsänkylä, *An application of the p-adic class number formula*, Manuscripta Math. 93 (1997), 481–498.

[4] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979.

[5] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), 185–208; Corrigendum, ibid. 5 (1960), 259.

Stanislav Jakubec
Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
814 73 Bratislava, Slovakia
E-mail: jakubec@mat.savba.sk

Received on 10.3.2008
and in revised form on 17.5.2010 (5658)