ACTA ARITHMETICA
137.1 (2009)

On some new estimates for $h^{-}(\mathbb{Q}(\zeta_p))$

by

STANISLAV JAKUBEC (Bratislava)

1. Introduction. Let p be an odd prime number and $m = (p-1)/2$. Let h_p resp. h_p^+ denote the class numbers of the cyclotomic field $\mathbb{Q}(\zeta_p)$, resp. the maximal real subfield $\mathbb{Q}(\zeta_p)^+$ of this field. The Dirichlet class number formula for the class number $h_p = h(\mathbb{Q}(\zeta_p))$ is

$$h_p = \frac{p^{p/2}}{2^{m-1}\pi^m R} \prod_{\chi\neq 1} L(1,\chi),$$

where the product is taken over all nonprincipal characters of $\mathbb{Q}(\zeta_p)$. It is well known that $h_p^+ \mid h_p$ (see Theorem 4.10 in [4]). We have $h_p = h_p^+ h_p^-$, where

$$h_p^- = \frac{1}{2^{m-1}}\, p^{(p+3)/4}\, \frac{1}{\pi^m} \prod_{\chi\,\mathrm{odd}} L(1,\chi) = \frac{1}{(2p)^{m-1}} \prod_{\chi\,\mathrm{odd}} \sum_{k=1}^{p-1} k\overline{\chi}(k) \tag{1}$$

(see Theorems 4.17 and 4.9 in [4]).

We consider two types of sequences $(a_i)_{1\le i\le m}$ over $\mathbb{Z}$: $a_i = m+i$, $i = 1,\ldots,m$, or $a_i = r^i$, $i = 1,\ldots,m$, where $p \equiv 1 \pmod 4$ and r is a primitive root modulo p, or $p \equiv 3 \pmod 4$ and r generates the group of quadratic residues modulo p. For the sequences $\{a_i\}_{1\le i\le m}$, if $1 \le j \le m$ there exists $1 \le i \le m$ such that $a_i \equiv j \pmod p$ or $a_i \equiv -j \pmod p$.

In [2] and [3] it is proved that

$$h_p^- \le 2p\left(\frac{p}{24}\right)^{m/2}.$$

We prove the estimates

$$h_p^- < 3.492 \cdot p\left(\frac{p}{32}\right)^{m/2},$$

2000 *Mathematics Subject Classification*: Primary 11R18.

Key words and phrases: first factor class number.

DOI: 10.4064/aa137-1-2

provided $p \equiv 1 \pmod 4$ and $r = 2$ is a primitive root modulo p or $p \equiv 3 \pmod 4$ and $r = 2$ generates the group of quadratic residues modulo p. Analogously, if we replace $r = 2$ by $r = 3$ resp. $r = 5$ we obtain the estimates

$$h_p^- < 1.502 \cdot p\left(\frac{p}{27}\right)^{m/2} \quad \text{and} \quad h_p^- < 2p\left(\frac{p}{25}\right)^{m/2}.$$

In the proofs, we make use of two types of matrices $A = (A_{ij})_{1\le i,j\le m}$ or $B = (B_{ij})_{1\le i,j\le m}$ over $\mathbb{Z}$ associated to the sequences $(a_i)_{1\le i\le m}$:

$$A_{ij} = [a_i(m+j)/p],$$

for $a_i = m + i$ (here as usual $[x]$ denotes the integral part of x), and for $a_i = r^i$, $B_{1j} = 1$ and

$$B_{ij} = [a_i(m+j)/p] - r[a_{i-1}(m+j)/p] \quad \text{if } i \ge 2.$$

2. Some relations between the matrices A and h_p^-. Let χ be a generator of the group of characters of the field $\mathbb{Q}(\zeta_p)$. Then odd characters of this field are odd powers of χ. Moreover, it is well-known that for χ odd,

$$L(1,\chi) = \frac{\pi i \tau(\chi)}{p^2} \sum_{j=1}^{p-1} j\overline{\chi}(j), \tag{2}$$

where $\tau(\chi)$ as usual denotes the Gauss sum (see Theorem 4.9 in [4]). After some manipulation the formula can be rewritten as

$$L(1,\chi) = \frac{\pi i \tau(\chi)}{p(\overline{\chi}(2) - 2)} \sum_{j=1}^{m} \overline{\chi}(j). \tag{3}$$

Therefore formula (1) can be rewritten as

$$h_p^- = \left| \frac{p}{2^{m-1}} \prod_{j=1}^{m} \frac{1}{\overline{\chi}^{2j-1}(2) - 2} \sum_{k=1}^{m} \chi^{2j-1}(k) \right|. \tag{4}$$

Let $[x]^* = [x] - 1/2$ if $x \in \mathbb{Z}$ and $[x]^* = [x]$ otherwise. It is well-known that

$$[x]^* = x - \frac{1}{2} + \sum_{j=1}^{\infty} \frac{\sin(2jx\pi)}{\pi j}.$$

LEMMA 1. *Let χ be an odd Dirichlet character modulo p, and a be a natural number. Then*

$$\sum_{j=1}^{m} \left[\frac{aj}{p}\right] \chi(j) = \frac{1}{2}\left(\frac{a - \overline{\chi}(a)}{\overline{\chi}(2) - 2} + a - 1\right) \sum_{j=1}^{m} \chi(j),$$

$$\sum_{j=m+1}^{p-1} \left[\frac{aj}{p}\right] \chi(j) = \frac{1}{2}\left(\frac{a - \overline{\chi}(a)}{\overline{\chi}(2) - 2} - a + 1\right) \sum_{j=1}^{m} \chi(j).$$

Proof. From the formulas before the lemma, (2), (3) and well-known properties of the Gauss sum we obtain

$$\begin{aligned}\sum_{k=1}^{p-1}\left[\frac{ak}{p}\right]\chi(k) &= \sum_{k=1}^{p-1}\left[\frac{ak}{p}\right]^*\chi(k) = \sum_{k=1}^{p-1}\chi(k)\biggl(\frac{ak}{p}-\frac{1}{2}+\frac{1}{\pi}\sum_{j=1}^{\infty}\frac{1}{j}\sin\frac{2\pi akj}{p}\biggr)\\
&= \sum_{k=1}^{p-1}\chi(k)\biggl(\frac{ak}{p}-\frac{1}{2}+\frac{1}{2\pi i}\sum_{j=1}^{\infty}\frac{1}{j}\,(\zeta_p^{akj}-\zeta_p^{-akj})\biggr)\\
&= \frac{a}{p}\sum_{k=1}^{p-1}k\chi(k)+\frac{\tau(\chi)\overline{\chi}(a)}{\pi i}\sum_{j=1}^{\infty}\frac{\overline{\chi}(j)}{j}\\
&= \frac{p(a-\overline{\chi}(a))}{\pi i\tau(\overline{\chi})}\,L(1,\overline{\chi}) = \frac{a-\overline{\chi}(a)}{\overline{\chi}(2)-2}\sum_{k=1}^{m}\chi(k).\end{aligned}$$

Lemma 1 now follows from

$$\left[\frac{ai}{p}\right]+\left[\frac{a(p-i)}{p}\right] = a-1. \ \blacksquare$$

Let s be a rational p-integer number and let χ be a Dirichlet character modulo p. Define $\chi(s)=\chi(n)$ where $n\in\mathbb{Z}$ and $s\equiv n \pmod p$. For χ odd we have

$$\sum_{j=1}^{m}\chi^{2j-1}(s) = \begin{cases}0 & \text{if } s\not\equiv\pm1 \pmod p,\\ \pm m & \text{if } s\equiv\pm1 \pmod p.\end{cases} \tag{5}$$

THEOREM 1. *Let p be an odd prime and $m=(p-1)/2$. For the matrix A defined in the Introduction we have*

$$|\det(A)| = h_p^-.$$

Proof. Let χ be a generator of the group of characters of the field $\mathbb{Q}(\zeta_p)$. Set $K=(K_{ij})_{1\le i,j\le m}$, where $K_{ij}=\chi^{2j-1}(a_i)$. Let as usual K^T denote the transpose of K. Write $M=KK^T=(M_{ij})_{1\le i,j\le m}$. Then by (5) we obtain

$$M_{ij} = \sum_{k=1}^{m}\chi^{2k-1}(a_ia_j) = \begin{cases}0 & \text{if } a_ia_j\not\equiv\pm1 \pmod p,\\ \pm m & \text{if } a_ia_j\equiv\pm1 \pmod p,\end{cases}$$

and consequently

$$\det(M) = \pm m^m. \tag{6}$$

On the other hand, applying Lemma 1 and (4) gives

$$AK = \frac{1}{2}\,h_p^-p^{m-1}C,$$

where $C = \{C_{ij}\}$ with

$$C_{ij} = 3m + 3i - 2 - \chi^{2j-1}\left(\frac{1}{m+i}\right) + (-m-i+1)\chi^{2j-1}\left(\frac{1}{2}\right).$$

Moreover, by (5) we have

$$CK^T = \begin{pmatrix} -m & * & \ldots & * & * \\ 0 & -m & \ldots & * & * \\ \multicolumn{5}{c}{\dotfill} \\ 0 & 0 & \ldots & -m(3-2m) & -m(6m-5) \\ 0 & 0 & \ldots & -m(1-2m) & -m(-1+6m) \end{pmatrix}.$$

Hence

$$\det(CK^T) = \pm 2pm^m. \ \blacksquare$$

THEOREM 2. *Let p be an odd prime and let $m = (p-1)/2$. Let $1 \le n < m$ and $\varepsilon_0 = \pm 1$ be the unique integers satisfying $r^n \equiv 2\varepsilon_0 \pmod p$. Write $\varepsilon = \varepsilon_0(r/p)$. For the matrix B defined in the Introduction we have*

$$|\det(B)| = \frac{2r^{m-1} - \varepsilon r^{n-1}}{p}\, h_p^-.$$

Proof. Let K be the matrix defined in the proof of Theorem 1. Applying Lemma 1 and (4) gives

$$BK = \frac{1}{2}\, h_p^- p^{m-1} D,$$

where $D = (D_{ij})_{1\le i,j\le m}$ with $D_{1j} = 4 - 2\overline{\chi}^{2j-1}(2)$ and

$$\begin{aligned} D_{ij} &= a_i - \overline{\chi}^{2j-1}(a_i) - (a_i - 1)(\overline{\chi}^{2j-1}(2) - 2) \\ &\quad - r(a_{i-1} - \overline{\chi}^{2j-1}(a_{i-1}) - (a_{i-1} - 1)(\overline{\chi}^{2j-1}(2) - 2)) \\ &= -(2-2r) + (1-r)\chi^{2j-1}\left(\frac{1}{2}\right) - \chi^{2j-1}\left(\frac{1}{a_i}\right) + r\chi^{2j-1}\left(\frac{1}{a_{i-1}}\right), \end{aligned}$$

if $i \ge 2$. Write $R = DK^T = (R_{ij})_{1\le i,j\le m}$. Then we have

$$R_{1k} = 4\sum_{j=1}^{m} \chi^{2j-1}(a_k) - 2\sum_{j=1}^{m} \chi^{2j-1}\left(\frac{a_k}{2}\right) \quad \text{for } k = 1, \ldots, m,$$

and

$$\begin{aligned} R_{ik} = &-(2-2r)\sum_{j=1}^{m} \chi^{2j-1}(a_k) + (1-r)\sum_{j=1}^{m} \chi^{2j-1}\left(\frac{a_k}{2}\right) \\ &- \sum_{j=1}^{m} \chi^{2j-1}\left(\frac{a_k}{a_i}\right) + r\sum_{j=1}^{m} \chi^{2j-1}\left(\frac{a_k}{a_{i-1}}\right), \end{aligned}$$

where $i \geq 2$. Define $F = (F_{ik})_{1\leq i,k\leq m}$, where $F_{1k} = R_{1k}$ and for $i \geq 2$,

$$F_{ik} = R_{ik} + \frac{1-r}{2} R_{1k} = -\sum_{j=1}^{m} \chi^{2j-1}\left(\frac{a_k}{a_i}\right) + r\sum_{j=1}^{m} \chi^{2j-1}\left(\frac{a_k}{a_{i-1}}\right).$$

Applying (5) gives

$$F = \begin{pmatrix} * & * & \ldots & * & 4m(r/p) \\ rm & -m & \ldots & 0 & 0 \\ 0 & rm & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & rm & -m \end{pmatrix},$$

where $F_{1n} = -2\varepsilon_2 m$, $F_{1m} = 4m(r/p)$, and all remaining entries vanish. It follows that

$$\det(F) = \pm 2pm^m \frac{2r^{m-1} - \varepsilon r^{n-1}}{p} \quad \text{where} \quad 2r^{m-1} - \varepsilon r^{n-1} \equiv 0 \pmod{p},$$

which completes the proof. ∎

3. Applications. Let $X = (X_{ij})_{1\leq i,j\leq m}$ be a real matrix and let $\|\cdot\|$ denote the Euclidean matrix norm defined as

$$\|X\| = \Big(\sum_{i,j} X_{ij}^2\Big)^{1/2}.$$

By Hadamard's inequality and the inequality between geometric and arithmetic means we have

$$|\det(X)| \leq \left(\frac{\|X\|}{n}\right)^{n/2}. \tag{7}$$

THEOREM 3 (Schur 1909, see [1, Theorem 7.3.1, p. 202]). *Let X be an $n \times n$ matrix with eigenvalues $\lambda_1, \ldots, \lambda_n$. Then*

$$\sum_{i=1}^{n} |\lambda_i|^2 \leq \|X\|^2.$$

COROLLARY TO THEOREM 2. *Let p be a prime number and r be a natural number such that either $p \equiv 1 \pmod 4$ and r is a primitive root modulo p, or $p \equiv 3 \pmod 4$ and r generates the group of quadratic residues modulo p. We have*

1. *If $r = 2$ and $p > 23$,*

$$h_p^- < 3.492 \cdot p\left(\frac{p}{32}\right)^{m/2}.$$

2. *If* $r = 3$ *and* $p > 100$,

$$h_p^- \le 1.502 \cdot p\left(\frac{p}{27}\right)^{m/2}.$$

3. *If* $r = 5$,

$$h_p^- \le 2p\left(\frac{p}{25}\right)^{m/2}.$$

Proof. Denote by $\mathbf{x}_i$ $(1 \le i \le m)$ the ith row of the matrix B. Let as usual $(\mathbf{x}, \mathbf{y})$ denote the scalar product. Then Theorem 3 implies the inequality

$$|\det(B)| \le \left(\frac{\overline{Q}}{m}\right)^{m/2}, \quad \text{where} \quad \overline{Q} = \sum_{i=1}^{m}(\mathbf{x}_i, \mathbf{x}_i). \tag{8}$$

1. If $r = 2$ the matrix B is a (0-1) matrix. Applying the Gram–Schmidt orthogonalization process we pass from the vectors $(\mathbf{x}_i)_{1\le i\le m}$ to an orthogonal system of vectors $(\mathbf{y}_i)_{1\le i\le m}$:

$$\mathbf{y}_1 = \mathbf{x}_1 \quad \text{and} \quad \mathbf{y}_i = \mathbf{x}_i - \sum_{j=1}^{i-1}\frac{(\mathbf{x}_i, \mathbf{y}_j)}{(\mathbf{y}_j, \mathbf{y}_j)}\,\mathbf{y}_j \quad \text{if } i \ge 2.$$

We have

$$(\mathbf{y}_1, \mathbf{y}_1) = (\mathbf{x}_1, \mathbf{x}_1) \quad \text{and} \quad (\mathbf{y}_i, \mathbf{y}_i) = (\mathbf{x}_i, \mathbf{x}_i) - \sum_{j=1}^{i-1}\frac{(\mathbf{x}_i, \mathbf{y}_j)^2}{(\mathbf{y}_j, \mathbf{y}_j)} \quad \text{if } i \ge 2.$$

Moreover, Theorem 2 for $r = 2$ together with (8) implies the inequality

$$\frac{2^m - \left(\frac{2}{p}\right)}{p}\,h_p^- = |\det(B)| \le \left(\frac{Q}{m}\right)^{m/2}, \quad \text{where} \quad Q = \sum_{i=1}^{m}(\mathbf{y}_i, \mathbf{y}_i). \tag{9}$$

If t_i denotes the number of 1's in the ith row, then

$$\begin{aligned} Q = \sum_{i=1}^{m}(\mathbf{y}_i, \mathbf{y}_i) &< \sum_{i=1}^{m}(\mathbf{x}_i, \mathbf{x}_i) - \frac{1}{m}\sum_{i=2}^{m}(\mathbf{x}_i, \mathbf{x}_1)^2 = \sum_{i=1}^{m} t_i - \frac{1}{m}\sum_{i=2}^{m} t_i^2 \\ &\le m + (m-1)\,\frac{m}{2} - \frac{1}{m}\,(m-1)\left(\frac{m}{2}\right)^2 = m + m\,\frac{m-1}{4}, \end{aligned}$$

therefore

$$\frac{Q}{m} < 1 + \frac{m-1}{4} = \frac{m+3}{4} = \frac{p+5}{8}.$$

Hence and by (9) for $m \ge 14$ we obtain

$$\frac{2^m \cdot 2^{-0.0001}}{p}\,h_p^- < \frac{2^m - \left(\frac{2}{p}\right)}{p}\,h_p^- \le \left(\frac{p+5}{8}\right)^{m/2} < e^{5/4}\left(\frac{p}{8}\right)^{m/2},$$

because

$$\lim_{n\to\infty}\left(1+\frac{5}{4n}\right)^n = e^{5/4}.$$

This gives the corollary for $r = 2$ at once.

2. For $i \geq 2$ subtract the first row of B from its ith row for $i = 2, \dots, m$ and denote the resulting matrix by E. The number of entries in the ith row of E for $i = 2, \dots, m$ that are equal to ± 1 is $[p/3]$. Therefore

$$\|E\| = m + (m-1)\left[\frac{p}{3}\right] \leq m + (m-1)\frac{2m}{3}$$

and so

$$\frac{\|E\|}{m} \leq 1 + \frac{2(m-1)}{3} = \frac{p}{3}.$$

Consequently, by (7) and Theorem 2 for $r = 3$ we obtain

$$\text{(10)} \qquad \frac{2\cdot 3^{m-1} - 3^{m-7}}{p}\, h_p^- < \frac{2\cdot 3^{m-1} - \varepsilon 3^{n-1}}{p}\, h_p^- = |\det(B)| = |\det(E)| \leq \left(\frac{\|E\|}{m}\right)^{m/2} \leq \left(\frac{p}{3}\right)^{m/2},$$

because for $p > 100$ we have

$$2\cdot 3^{m-1} - \varepsilon 3^{n-1} > 2\cdot 3^{m-1} - 3^{m-7}.$$

The above inequality is obvious if $\varepsilon = -1$ or $\varepsilon = 1$ and $m - n > 6$. If $n = m - k$, $k \leq 6$ and $p > 100$, we have

$$0 \equiv 2\cdot 3^{m-1} - \varepsilon 3^{n-1} \equiv 3^{m-k-1}(2\cdot 3^k - 1) \not\equiv 0 \pmod{p},$$

because

$$\prod_{k=1}^{6}(2\cdot 3^k - 1) = 5^2\cdot 7\cdot 17\cdot 23\cdot 31\cdot 47\cdot 53\cdot 97 \not\equiv 0 \pmod{p},$$

if $p > 100$; a contradiction.

Now from (10) we have

$$3^{c-7}h^- < p\left(\frac{p}{27}\right)^{m/2},$$

where $c = \log_3(2\cdot 3^6 - 1)$. Hence the corollary follows in the case when $r = 3$.

3. For $r = 5$ analysis analogous to that in the proof of Corollary in the case $r = 3$ gives the Metsänkyla–Lepistö type inequality

$$h_p^- \leq 2p\left(\frac{p}{25}\right)^{m/2}. \ \blacksquare$$

Acknowledgements. The author would like to thank the referee for his comments which improved the paper generally. Moreover, his comments to some of the proofs helped to correct the formulation of the main result concerning the estimates of h_p^-.

References

[1] P. Lancaster, *Theory of Matrices*, Academic Press, New York, 1969.
[2] T. Lepistö, *On the growth of the first factor of the class number of the prime cyclotomic field*, Ann. Acad. Sci. Fenn. Ser. A I No. 577 (1974).
[3] T. Metsänkyla, *On the growth of the first factor of the cyclotomic class number*, Ann. Univ. Turku. Ser. A No. 155 (1972).
[4] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.

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

Received on 1.8.2007
and in revised form on 8.12.2008 (5486)