ON THE FIRST FACTOR OF THE CLASS NUMBER OF A CYCLOMATIC FIELD

KEQIN FENG

Abstract. Let \( p \) be an odd prime. \( h_1(p) \) is the first factor of the class number of field \( \mathbb{Q} (\zeta_p) \). We proved that

\[
h_1(p) \leq \begin{cases} 
2p \left( \frac{p - 1}{8(2^{l/2} + 1)^{4/l}} \right)^{(p-1)/4}, & \text{if } l \text{ is even,} \\
2p \left( \frac{p - 1}{8(2^l - 1)^{2/l}} \right)^{(p-1)/4}, & \text{if } l \text{ is odd.}
\end{cases}
\]

From that we obtain \( h_1(p) \leq 2p((p - 1)/31.997158 \ldots)^{(p-1)/4} \) which is better than Carlitz's and Metsänkyla's results. For the fields \( \mathbb{Q}(\zeta_{2^n}) \) and \( \mathbb{Q}(\zeta_p) \) (\( n \geq 2 \)), we get the similar results.

Let \( p \) be an odd prime, \( \zeta_p = e^{(2\pi i)/p} \), \( h(p) \) and \( h_2(p) \) be the class number of the cyclotomic field \( \mathbb{Q}(\zeta_p) \) and its maximal real subfield \( \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \) respectively. In 1850 Kummer \([2]\) proved that \( h_1(p) = h(p)/h_2(p) \) is a rational integer which is called the first factor of the class number of \( \mathbb{Q}(\zeta_p) \). Kummer conjectured that

\[
h_1(p) \sim 2p \left( \frac{p}{4\pi^2} \right)^{(p-1)/4} = 2p \left( \frac{p}{39.4784 \ldots} \right)^{(p-1)/4} \text{ (when } p \to \infty).\]

In 1961 L. Carlitz \([1]\) proved that \( h_1(p) < (p - 1)((p - 1)/2)^{(p-1)/4} \). In 1974 T. Metsänkyla proved that \( h_1(p) < 2p((p - 1)(p - 2)/24p)^{(p-1)/4} \). In this short paper I will show that

\[
h_1(p) < 2p \left( \frac{p - 1}{31.997158 \ldots} \right)^{(p-1)/4} .
\]

Exactly speaking, I will show the following theorem.

THEOREM. Let \( l \) be the order of 2 (mod \( p \)). Then

\[
h_1(p) \leq \begin{cases} 
2p \left( \frac{p - 1}{8(2^{l/2} + 1)^{4/l}} \right)^{(p-1)/4}, & \text{if } l \text{ is even,} \\
2p \left( \frac{p - 1}{8(2^l - 1)^{2/l}} \right)^{(p-1)/4}, & \text{if } l \text{ is odd.}
\end{cases}
\]

Received by the editors August 1, 1980.
1980 Mathematics Subject Classification. Primary 12A35, 12A50.
Key words and phrases. Class number, cyclotomic field.

© 1982 American Mathematical Society
0002-9939/81/0000-1087/$02.00
From the theorem to (1). For even \( l \), from the theorem we know that
\[
h_1(p) \leq 2p \left( \frac{p - 1}{8(2^{(2/2)} + 1)^{(p-1)/4}} \right)^{(p-1)/4} \leq 2p \left( \frac{p - 1}{32} \right)^{(p-1)/4}.
\]
For odd \( l \), it is easy to see that if \( p > 127 \) then \( l \geq 11 \) and
\[
(2^l - 1)^{2/l} \geq (2^{11} - 1)^{2/11} = 3.9996448\ldots.
\]
Thus
\[
h_1(p) \leq 2p \left( \frac{p - 1}{8 \times 3.9996448\ldots} \right)^{(p-1)/4} = 2p \left( \frac{p - 1}{31.997158} \right)^{(p-1)/4}.
\]
For \( p \leq 127 \) we can verify (1) directly.
To prove the theorem we need

**Lemma.** Let \( \chi \) be an odd Dirichlet character with the conductor \( f \). If \( f \equiv 2 \pmod{4} \), then
\[
\sum_{1 \leq a < f} \chi(a) = \frac{f}{\bar{\chi}(2) - 2} \sum_{0 < a < f/2} \chi(a).
\]

**Proof.** Long [3] proved this lemma for quadratic character \( \chi \). His method is available for any character satisfying the conditions of the lemma. We restate it for sake of completeness.
When \( 2 \mid f \) then, on one hand,
\[
- \sum_{0 < a < f} \chi(a) = - \sum_{0 < a < f/2} \chi(a) + \chi(f-a)(f-a)
\]
\[
= - \sum_{0 < a < f/2} \chi(2a)2a + \sum_{0 < a < f/2} \chi(2a)(f-2a)
\]
\[
= \chi(2) \sum_{0 < a < f/2} (f-4a)\chi(a).
\]
Thus
\[
(2) \quad - \bar{\chi}(2) \sum_{0 < a < f} \chi(a) = \sum_{0 < a < f/2} (f-4a)\chi(a).
\]
On the other hand,
\[
- \sum_{0 < a < f} \chi(a) = - \sum_{0 < a < f/2} \chi(a) - \sum_{0 < a < f/2} \chi(f-a)(f-a)
\]
\[
= - \sum_{0 < a < f/2} \chi(a) + \sum_{0 < a < f/2} \chi(a)(f-a)
\]
\[
= \sum_{0 < a < f/2} (f-2a)\chi(a).
\]
From (2) and (3) we obtain
\[
\sum_{0 < a < f} \chi(a) = \frac{f}{\bar{\chi}(2) - 2} \sum_{0 < a < f/2} \chi(a).
\]
When $4 \mid f$ then $\chi(2) = 0$ and $\chi(x + f/2) = -\chi(x)$. Thus
\[
\sum_{0 < a < f/2} \chi(a) a = \sum_{0 < a < f/2} \chi(a) a + \sum_{0 < a < f/2} \chi\left(a + \frac{f}{2}\right)\left(a + \frac{f}{2}\right) = \frac{f}{2} \sum_{0 < a < f/2} \chi(a).
\]

**Proof of the Theorem.** Starting from the analytic formula of $h_1(p)$,
\[
h_1(p) = 2p \prod_{x(-1) = 1} \sum_{a=1}^{p-1} \left(-\frac{1}{2p}\right) \chi(a) a = \left(2p\right)^{(p-1)/2+1} \prod_{x(-1) = 1} \left| \sum_{a=1}^{p-1} \chi(a) a \right|,
\]
where $\chi$ is taken to be the $(p - 1)/2$ odd characters of mod $p$. Let $g$ be a primitive root of mod $p$ and $\chi_0(a) = \exp((2\pi i)/(p - 1) \cdot \ind_g a) (1 \leq a \leq p - 1)$. Then
\[
h_1(p) = \left(2p\right)^{(p-1)/2+1} \prod_{\lambda=1}^{(p-1)/2} \left| \chi_0^{2\lambda-1}(a) \right|.
\]

From the above lemma we also have
\[
(4) \quad h_1(p) = \left(2p\right) \cdot 2^{-{(p-1)/2}} \left( \prod_{\lambda=1}^{(p-1)/2} \left| 2 - \chi_0^{2\lambda-1}(2) \right|^{-1} \right) \prod_{\lambda=1}^{(p-1)/2} \left| \sum_{a=1}^{(p-1)/2} \chi_0^{2\lambda-1}(a) \right|.
\]

Using the orthogonal relations of odd characters of mod $p$,
\[
\sum_{\lambda=1}^{(p-1)/2} \chi_0^{2\lambda-1}(a) \overline{\chi}_0^{2\lambda-1}(b) = \sum_{\lambda=1}^{(p-1)/2} \exp\left(\frac{2\pi i \cdot \ind_g(a/b)}{p - 1} \cdot (2\lambda - 1)\right) = \begin{cases} (p-1)/2, & \text{if } a \equiv b \pmod{p}, \\ -(p-1)/2, & \text{if } a \equiv -b \pmod{p}, \\ 0, & \text{otherwise.} \end{cases}
\]

For $1 \leq a, b \leq p - 1$, we have
\[
\prod_{\lambda=1}^{(p-1)/2} \left| \sum_{a=1}^{(p-1)/2} \chi_0^{2\lambda-1}(a) \right|^{4/(p-1)} = \prod_{\lambda=1}^{(p-1)/2} \left( \sum_{a, b=1}^{(p-1)/2} \chi_0^{2\lambda-1}(a) \overline{\chi}_0^{2\lambda-1}(b) \right)^{2/(p-1)} \leq \frac{2}{p-1} \sum_{\lambda=1}^{(p-1)/2} \sum_{a, b=1}^{(p-1)/2} \chi_0^{2\lambda-1}(a) \overline{\chi}_0^{2\lambda-1}(b) = \frac{2}{p-1} \sum_{a, b=1}^{(p-1)/2} \sum_{\lambda=1}^{(p-1)/2} \chi_0^{2\lambda-1}(a) \overline{\chi}_0^{2\lambda-1}(b) = \frac{2}{p-1} \cdot \frac{p-1}{2} \cdot \frac{p-1}{2} = \frac{p-1}{2}.
\]
Thus
\[
\prod_{\lambda=1}^{(p-1)/2} \left| \sum_{a=1}^{(p-1)/2} \chi^{2\lambda-1}(a) \right| \leq \left( \frac{p-1}{2} \right)^{(p-1)/4}.
\]

On the other hand, we can assume \( \text{ind}_g 2 = (p - 1)/l \) without loss of generality. So
\[
\prod_{\lambda=1}^{(p-1)/2} \left( 2 - \chi^{2\lambda-1}(2) \right) = \prod_{\lambda=1}^{(p-1)/2} \left( 2 - \exp \left( \frac{2\pi i \cdot \text{ind}_g 2}{p-1} (2\lambda - 1) \right) \right)
\]
\[
= \prod_{\lambda=1}^{(p-1)/2} \left( 2 - \exp \left( \frac{2\pi i (2\lambda - 1)}{l} \right) \right).
\]

Combining (4), (5), and (6) we obtain the theorem.

**Remark.** Let \( h_1(p^n) \) be the first factor of class number of field \( \mathbb{Q}(\zeta_{p^n}) \). Using the similar argument and the same lemma we can get that
(i) \( h_1(2^n) \leq 2^{n+(\alpha-6)2^{-n-1}} (n \geq 2) \),
(ii) For odd prime \( p \)
\[
h_1(p^n) \leq \begin{cases} 
2p^n \left( \frac{\varphi(p^n)}{8(2^{l/2} + 1)^{4/l}} \right)^{\psi(p^n)/4}, & \text{if } l \text{ is even,} \\
2p^n \left( \frac{\varphi(p^n)}{8(2^l - 1)^{2/l}} \right)^{\psi(p^n)/4}, & \text{if } l \text{ is odd,}
\end{cases}
\]

where \( l \) is the order of 2 (mod \( p^n \)).

**References**


**Department of Mathematics, University of Maryland, College Park, Maryland 20742**

**Current address:** Department of Mathematics, Chinese University of Science and Technology, Hofei, Anhui, The People’s Republic of China