# Calculation of the First Factor of the Class Number of the Cyclotomic Field 

By Tauno Metsänkylä


#### Abstract

The values of the first factor $H_{1}(m)$ of the class number of the $m$ th cyclotomic field are tabulated for 120 composite $m$ 's larger than 100 . A conjecture concerning a divisibility property of $H_{1}(m)$ is stated.


1. Introduction. Denote by $H_{1}(m)$ the so-called first factor of the class number of the $m$ th cyclotomic field $R(\exp (2 \pi i / m))$. One can assume that $m$ is either odd or divisible by 4 , since for any other $m$ the $m$ th and ( $m / 2$ ) th cyclotomic fields coincide.

Kummer [2], [3] calculated the values of $H_{1}(m)$ for all $m$ up to 100 and for prime $m$ up to 163. (See also Hasse [1, pp. 148-194]. It should be noted that the so-called relative class number introduced by Hasse equals $H_{1}(m)$ if $m$ is a power of a prime, and $2 H_{1}(m)$ otherwise.) In addition to that, the value of $H_{1}(m)$ is known for $m=2^{7}$, $2^{8}, 3^{5}$, and $5^{3}$ [1, pp. 105-114]. For large $m$, the value of $H_{1}(m)$ seems to be quite enormous if $m$ is a power of a prime, but much smaller otherwise-e.g., $H_{1}(163)$ and $H_{1}\left(3^{5}\right)$ are of order $10^{25}$ but $H_{1}(100)=55 / 2$.

The explicit expression of $H_{1}(m)$ is rather complicated, when $m$ contains distinct prime factors. We show in the following, however, that it is not difficult to calculate $H_{1}(m)$, for such $m$, on an electronic computer without any special arrangements, provided that $H_{1}(m)$ is not too large. With the double-precision of the IBM 7090 ( 16 digits) our method gave the value of $H_{1}(m)$ for 120 new $m$ 's. By some refinements of this method it would be possible to extend the collection of these results.

In Section 4 we mention an experimentally observed divisibility property of of $H_{1}(m)$, that we are not, however, able to formulate exactly, much less to prove.
2. Decomposition of the First Factor. Assume that $m=p^{h} q^{k}$, where $p$ and $q$ are distinct odd primes. For $(m, n)=1$, put

$$
F_{n}=F_{n}\left(b_{1}, b_{2}\right)=2 \pi\left(a_{1} b_{1} / \phi\left(p^{h}\right)+a_{2} b_{2} / \phi\left(q^{k}\right)\right),
$$

where $b_{1}$ and $b_{2}$ are integral parameters and $a_{1}$ and $a_{2}$ denote indices of $n$ to fixed primitive roots of $p^{h}$ and $q^{k}$, respectively. Then (see e.g. [5, pp. 10-12])

$$
\begin{equation*}
H_{1}(m)=\frac{1}{2} H_{1}\left(p^{h}\right) H_{1}\left(q^{k}\right) M\left(p^{h} q^{k}\right) \tag{1}
\end{equation*}
$$

with

$$
M\left(p^{h} q^{k}\right)=\prod_{\chi}(2 m)^{-1} \sum_{n=1}^{m}(-\chi(n) n),
$$

where $\chi$ runs through certain odd primitive characters, namely through all the characters

$$
\begin{aligned}
\chi(n) & =0 \quad \text { if }(m, n)>1 \\
& =\exp \left(i F_{n}\left(b_{1}, b_{2}\right)\right) \quad \text { if }(m, n)=1
\end{aligned}
$$

with $1 \leqq b_{1} \leqq \phi\left(p^{h}\right)-1,1 \leqq b_{2} \leqq \phi\left(q^{k}\right)-1, b_{1}+b_{2}$ odd. We divide the product $\Pi_{\chi}$, representing the "mixed factor" of $H_{1}(m)$, into two products $\Pi_{10}$ and $\Pi_{01}$ : let $\Pi_{10}$ contain all those factors of $\Pi_{\chi}$ where, in $\chi, b_{1}$ is odd and $b_{2}$ even, and $\Pi_{01}$ the other factors. The values of $\Pi_{10}$ and $\Pi_{01}$ are rational integers [5, p. 14]. Denoting their absolute values by $T_{10}$ and $T_{01}$, respectively, we obtain

$$
\begin{equation*}
M\left(p^{h} q^{k}\right)=T_{10} T_{01} \tag{2}
\end{equation*}
$$

because of the positivity of $M\left(p^{h} q^{k}\right)$. Furthermore,

$$
\begin{equation*}
T_{\mu \nu}=\Pi_{\mu \nu}\left\{\left(\left(\sum_{n=1}^{m} n \cos F_{n}\right) / 2 m\right)^{2}+\left(\left(\sum_{n=1}^{m} n \sin F_{n}\right) / 2 m\right)^{2}\right\}^{1 / 2} \tag{3}
\end{equation*}
$$

$$
(\mu \nu=10,01) .
$$

If $m=p^{h} q^{k} r^{t}$ with an additional odd prime $r$, then one gets, correspondingly, the decomposition

$$
H_{1}(m)=\left(\frac{1}{2}\right)^{2} H_{1}\left(p^{h}\right) H_{1}\left(q^{k}\right) H_{1}\left(r^{t}\right) M\left(p^{h} q^{k}\right) M\left(p^{h} r^{t}\right) M\left(q^{k} r^{t}\right) N\left(p^{h} q^{k} r^{t}\right),
$$

where $N\left(p^{h} q^{k} r^{t}\right)$ is further to be divided into four factors $T_{100}, T_{010}, T_{001}$, and $T_{111}$. Here, the three parameters defining the characters in question take, in each $T_{\mu \nu \lambda}$, again the values of the same parity as $\mu, \nu$, and $\lambda$, respectively, and the factors $T_{\mu \nu \lambda}$ have expressions similar to Eq. (3). In an analogous way one can treat those $m$ 's that contain more prime factors.

If $m$ is even, the above considerations need slight modifications (see [5]).
3. Calculation Process. In calculating $H_{1}(m)$, there arises first the question of picking out those values of $m$, for which $H_{1}(m)$ is not too large. Here, we made use of a certain number $G(m)$, defined by Lepistö [4], that is conjectured to be asymptotically equal to $H_{1}(m)$, when $m$ tends to infinity. The calculation of $G(m)$ (or rather its logarithm if $m$ is large) on a computer can be easily accomplished. It should be mentioned that in all cases calculated by us $G(m)$ was fairly close to $H_{1}(m)$.

Our method restricted us to such values of $m$, for which the factors $H_{1}\left(p^{h}\right)$, for each power of prime dividing $m$, were previously known. (For the other $m$ 's, not only some of the numbers $H_{1}\left(p^{h}\right)$ but also some of the $T$-factors were always too large.) Thus, by Eqs. (1) and (2) and their analogues, we had to compute only the $T$-factors. The approximate values of these factors were calculated using Eq. (3) (and its analogues) and the corresponding exact values then derived from these. We mention as a typical example that for $m=161=7 \cdot 23$ the computer gave the result

$$
\begin{aligned}
& T_{10}=0.1091819068999960 \cdot 10^{10} \\
& T_{01}=0.5200472999999732 \cdot 10^{7}
\end{aligned}
$$

so that

$$
\begin{aligned}
& T_{10}=1091819069=11 \cdot 67^{2} \cdot 22111 \\
& T_{01}=5200473=3 \cdot 67 \cdot 25873
\end{aligned}
$$

As a test of our computer program and for the sake of completeness we calculated (partly on the IBM 1130) the $T$-factors also for all possible $m \leqq 100$. The whole running time on the IBM 7090 was about two hours.


| m | $T_{100}$ | $\begin{aligned} & \text { Table } \\ & T_{010} \\ & \hline \end{aligned}$ | $\mathrm{T}_{001}$ | T111 |
| :---: | :---: | :---: | :---: | :---: |
| $60=2^{2} \cdot 3 \cdot 5$ | 1 | 1 | 1 | 2 |
| $84=2^{2} \cdot 3 \cdot 7$ | 1 | 1 | 1 | 2 |
| $105=3 \cdot 5 \cdot 7$ | 1 | 1 | 1 | 2.13 |
| $120=23 \cdot 3 \cdot 5$ | 1 | 2 | 1 | $2^{2}$ |
| $132=2^{2 \cdot 3 \cdot 11}$ | 1 | 1 | 1 | $2 \cdot 11$ |
| $140=2{ }^{2} \cdot 5 \cdot 7$ | 3 | 1 | 1 | $2 \cdot 13$ |
| $156=2^{2} \cdot 3 \cdot 13$ | 1 | 1 | 1 | $2^{2} \cdot 13$ |
| $165=3 \cdot 5 \cdot 11$ | 11 | 1 | 1 | $2{ }^{2} \cdot 421$ |
| $168=2 \cdot 3 \cdot 3 \cdot 7$ | 1 | 3 | 1 | $2^{2} \cdot 7$ |
| $180=2^{2} \cdot 3^{2} \cdot 5$ | 3 | 1 | 1 | $2 \cdot 5^{2}$ |
| $195=3 \cdot 5 \cdot 13$ | $2^{5}$ | 1 | 1 | $2^{6} \cdot 13^{2}$ |
| $204=2^{2} \cdot 3 \cdot 17$ | 1 | 1 | 1 | $2^{2} \cdot 193$ |
| $220=2^{2} \cdot 5 \cdot 11$ | 31 | 1 | 1 | $2^{2} \cdot 1381$ |
| $228=2^{2} \cdot 3 \cdot 19$ | 1 | 1 | 1 | 2-7-199 |
| $231=3 \cdot 7 \cdot 11$ | $2^{4} \cdot 61$ | 1 | 1 | $25 \cdot 3^{2} \cdot 11 \cdot 151$ |
| $240=24 \cdot 3 \cdot 5$ | 1 | $2^{2} \cdot 5$ | 1 |  |
| $252=2^{2} \cdot 3^{2} \cdot 7$ | $2^{2} \cdot 7$ | 1 | 1 | $2^{3} \cdot 7 \cdot 13$ |
| $255=3 \cdot 5 \cdot 17$ | $2^{3} \cdot 3 \cdot 17$ | 1 | 1 | $2^{2} \cdot 353 \cdot 1889$ |
| $260=2{ }^{2} \cdot 5 \cdot 13$ | $2^{6}$ | 1 | 1 | $29.13^{2}$ |
| $264=2^{3} \cdot 3 \cdot 11$ |  | $5^{2}$ | 1 | $2^{3} \cdot 11 \cdot 31$ |
| $273=3 \cdot 7 \cdot 13$ | $2^{6} \cdot 3^{2} \cdot 19$ | 1 | 1 | $2^{10 \cdot 13 \cdot 37 \cdot 73}$ |
| $276=2^{2} \cdot 3 \cdot 23$ | 1 | 1 | 1 | $2^{2} \cdot 23 \cdot 617$ |
| $280=23 \cdot 5 \cdot 7$ | $3^{3}$ | 73 | $2 \cdot 7$ | $2^{2} \cdot 5 \cdot 13 \cdot 37$ |
| $285=3 \cdot 5 \cdot 19$ | $3^{2} \cdot 181$ | 1 | 1 | $\mathbf{2}^{2} \cdot 37^{2} \cdot 73 \cdot 109$ |
| $300=2{ }^{2} \cdot 3 \cdot 5^{2}$ | 1 | 1 | 1 | $2 \cdot 2161$ |
| $308=2{ }^{2} \cdot 7 \cdot 11$ | $2^{4} \cdot 181$ | 1 | 1 | $2^{10 \cdot 7 \cdot 312}$ |
| $312=23 \cdot 3 \cdot 13$ | 1 | 2.7-13 | 1 | $25 \cdot 13 \cdot 61$ |
| $315=3^{2} \cdot 5 \cdot 7$ | $2^{2} \cdot 37$ | $2^{2} \cdot 7^{2} \cdot 37$ | $2^{2} \cdot 3^{4}$ | $2^{3} \cdot 5^{2} \cdot 13^{2} \cdot 97$ |


| Table II (continued) |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: |
| m | $T_{100}$ | $\mathrm{T}_{010}$ | $\mathrm{T}_{001}$ | $\mathrm{T}_{111}$ |
| $336=2^{4} \cdot 3 \cdot 7$ | 1 | $3 \cdot 97$ | 1 | $2^{5 \cdot 7 \cdot 61}$ |
| $340=2{ }^{2} \cdot 5 \cdot 17$ | $2^{6} \cdot 5^{2}$ | 1 | 1 | $2^{4} \cdot 593 \cdot 3217$ |
| $345=3 \cdot 5 \cdot 23$ | 11.4159 | 1 | 1 | 2-5•2152502881 |
| $348=2{ }^{2} \cdot 3 \cdot 29$ | 1 | 1 | 1 | $2^{4 \cdot 5 \cdot 71317}$ |
| $357=3 \cdot 7 \cdot 17$ | $7^{2} \cdot 13 \cdot 37 \cdot 97$ | 1 | 1 | $2 \cdot 7^{2} \cdot 1873 \cdot 1157953$ |
| $360=2^{3} \cdot 3^{2} \cdot 5$ | $3 \cdot 7$ | $2 \cdot 7$ | 109 | $22^{2} \cdot 5^{2} \cdot 109$ |
| $364=2^{2} \cdot 7 \cdot 13$ | $2^{6} \cdot 3^{6}$ | 1 | 1 | $2^{5} \cdot 5^{4} \cdot 13^{4}$ |
| $372=2{ }^{2} \cdot 3 \cdot 31$ | 1 | 1 | 1 | $2^{5} \cdot 41 \cdot 13591$ |
| $380=22 \cdot 5 \cdot 19$ | 7-613 | 1 | 1 | $2^{3} \cdot 53^{2} \cdot 73 \cdot 433$ |
| $396=2^{2} \cdot 3^{2} \cdot 11$ | 19231 | 1 | 1 | 2-11-13-31-181 |
| $408=2^{3 \cdot 3 \cdot 17}$ | 1 | $2^{6} \cdot 41$ | 1 | $2^{4} \cdot 193 \cdot 2081$ |
| $440=2^{3} \cdot 5 \cdot 11$ | $5 \cdot 31^{2}$ | 61.181 | 2•3•61 | $2^{5} \cdot 1381 \cdot 15641$ |
| $444=2^{2} \cdot 3 \cdot 37$ | 1 | 1 | 1 | $2^{3} \cdot 37 \cdot 109 \cdot 54721$ |
| $456=2^{3} \cdot 3 \cdot 19$ | 1 | 19.487 | 1 | $2^{3} \cdot 7^{2} \cdot 199 \cdot 3259$ |
| $460=2^{2} \cdot 5 \cdot 23$ | $11 \cdot 17029$ | 1 | 1 | 2.5-617-114259861 |
| $468=2^{2} \cdot 3^{2} \cdot 13$ | $2^{6} \cdot 3^{3} \cdot 13^{2}$ |  | 1 | $2^{4} \cdot 5^{2} \cdot 11^{2} \cdot 13 \cdot 181$ |
| $480=25 \cdot 3 \cdot 5$ | 1 | $2^{3} \cdot 5 \cdot 7^{2}$ | 1 | $2^{9} \cdot 7^{2} \cdot 89$ |
| $492=2{ }^{2} \cdot 3 \cdot 41$ |  |  |  | $2^{6 \cdot 41} \cdot 1321 \cdot 33161$ |
| $504=2^{3} \cdot 3^{2} \cdot 7$ | $2^{4} \cdot 3^{3} \cdot 7$ | $2^{2} \cdot 3^{5}$ | $2^{2} \cdot 3^{4} \cdot 7$ | $2^{8} \cdot 7^{3} \cdot 13^{2}$ |
| $516=2^{2} \cdot 3 \cdot 43$ |  |  |  | $2^{3} \cdot 3^{2} \cdot 43 \cdot 71 \cdot 2490307$ |
| $520=2^{3} \cdot 5 \cdot 13$ | $2^{11} \cdot 3 \cdot 7$ | $2^{5} \cdot 5 \cdot 7^{2} \cdot 37$ | $2^{3} \cdot 5^{2} \cdot 17$ | $2^{18} \cdot 5 \cdot 13^{2} \cdot 37 \cdot 73$ |
| $528=2^{4} \cdot 3 \cdot 11$ |  | $5^{2} \cdot 65521$ | 1 | $2^{4} \cdot 5^{2} \cdot 11 \cdot 31 \cdot 61 \cdot 101$ |
| $540=2^{2} \cdot 3^{3} \cdot 5$ | $3^{2} \cdot 19 \cdot 73$ |  | 1 | $2 \cdot 5^{2} \cdot 109 \cdot 38557$ |
| $552=2^{3} \cdot 3 \cdot 23$ | 1 | 23-10781 | 1 | $2^{4} \cdot 23^{2} \cdot 617 \cdot 34673$ |
| $588=2{ }^{2} \cdot 3 \cdot 7^{2}$ |  | 1 | 1 | 2.2017•3571-5923 |
| $612=2^{2} \cdot 3^{2} \cdot 17$ | $2^{6} \cdot 3 \cdot 61 \cdot 73 \cdot 241$ | 1 | 1 | $2^{4} \cdot 97 \cdot 193 \cdot 7712737$ |

Table III

| m | T1110 | T1101 | Other T-factors that are > 1 |
| :---: | :---: | :---: | :---: |
| $420=2^{2 \cdot 3 \cdot 5 \cdot 7}$ | 97 | $2^{2} \cdot 13$ | - |
| $660=2^{2} \cdot 3 \cdot 5 \cdot 11$ | $5^{2} \cdot 3181$ | $2^{2} \cdot 181$ | - |
| $780=2^{2} \cdot 3 \cdot 5 \cdot 13$ | $2^{6} \cdot 5 \cdot 61 \cdot 157$ | $2^{6} \cdot 109$ | - |
| $840=2^{3 \cdot 3 \cdot 5 \cdot 7}$ | $13 \cdot 37 \cdot 97$ | $2^{4} \cdot 5^{2} \cdot 13$ | $T_{0100}=19, T_{0111}=2 \cdot 5 \cdot 397$ |
| $924=2^{2} \cdot 3 \cdot 7 \cdot 11$ | $2^{4} \cdot 5 \cdot 31 \cdot 101 \cdot 691$ | $2^{4} \cdot 3^{3} \cdot 31 \cdot 751$ | $-$ |
| $1020=2^{2} \cdot 3 \cdot 5 \cdot 17$ | $2^{20} \cdot 3^{2} \cdot 5^{2} \cdot 17$ | $2^{3} \cdot 69857$ | - |
| $1092=2^{2} \cdot 3 \cdot 7 \cdot 13$ | $2^{12} \cdot 7^{4} \cdot 13 \cdot 19 \cdot 31$ | $2^{10} \cdot 13 \cdot 157 \cdot 229$ | - |
| $1140=2^{2} \cdot 3 \cdot 5 \cdot 19$ | $3^{4} \cdot 97 \cdot 46714069$ | $2^{3} \cdot 7^{2} \cdot 19^{2} \cdot 37$ | - |
| $1260=2^{2} \cdot 3^{2} \cdot 5 \cdot 7$ | $2^{4} \cdot 97 \cdot 193 \cdot 373$ | $2^{6} \cdot 7^{2} \cdot 13 \cdot 31$ | $T_{1000}=2^{4} \cdot 3^{4}, T_{1011}=2^{4} \cdot 193 \cdot 373 \cdot 1153$ |
| $1320=2^{3} \cdot 3 \cdot 5 \cdot 11$ | $5^{2} \cdot 101 \cdot 3181 \cdot 20261$ | $2^{4} \cdot 181 \cdot 1481$ | $\mathrm{T}_{0100}=5 \cdot 331, \mathrm{~T}_{0111}=2^{5} \cdot 1127281$ |

The results are presented in Tables I-III. We note that we have announced some of these results in [5].
4. A Divisibility Property. In checking the results, the few known facts about the factors of $H_{1}(m)$ are of some use (see e.g. [5, pp. 25, 31-32, 38]). More useful, however, is the following statement:

Let a prime $P$ divide a $T$-factor, for a given $m=p^{h} m_{1}$ where $p$ is a prime not dividing $m_{1}\left(p^{h} \geqq 3, m_{1}>1\right)$. Assume that $P$ does not divide the same $T$-factor (if this exists) for $m=p^{h-1} m_{1}$. Then, on some conditions which seem to be satisfied very often, one of the numbers $\phi(P)$ and $\phi\left(p^{h}\right)$ is a multiple of the other. (Note that this is a generalization of the relation $p=P$, discussed e.g. by us in [5].)

This relation holds especially for large values of $P$; checking in our tables all such pairs ( $p^{h}, P$ ), 132 in all, where $P>1000$ and the relation is not trivial (i.e., $p^{h} \geqq 5$ ), we found only 8 exceptions to it (e.g., for $m=2^{3} .23$ the pair ( $2^{3}, 2399$ )
where 2398 is not divisible by 4). All these exceptions can be removed by replacing the divisor $\phi\left(p^{h}\right)$ by $\frac{1}{2} \phi\left(p^{h}\right)$. This is not always the case, however (take, e.g., for $m=2^{2} \cdot 31$ the pair (31, 41)).

The prime factors of $H_{1}\left(p^{h}\right)$ seem often to have the corresponding property. To mention here only a few examples, $H_{1}(41)=11^{2}, H_{1}(43)=211$, and $H_{1}\left(7^{2}\right)=43$.
5. Acknowledgements. The computer mainly used in the present work was the IBM 7090 at the Northern Europe University Computing Center (NEUCC). Some parts of the calculations (e.g., the prime factorization of the values of $H_{1}(m)$ ) were carried out on the IBM 1130 at the University of Turku. The author is indebted to his colleagues at the Department of Applied Mathematics for their advice and assistance.

Department of Mathematics
University of Turku
Turku, Finland

1. H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952, MR 14, 141.
2. E. Kummer, "Über die Klassenanzahl der aus $n$ ten Einheitswurzeln gebildeten komplexen Zahlen," Monatsh. Preuss. Akad. Wiss. Berlin, 1861, pp. 1051-1053.
3. E. Kummer, "Über diejenigen Primzahlen $\lambda$, für welche die Klassenzahl der aus $\lambda$ ten Einheitswurzeln gebildeten komplexen Zahlen durch $\lambda$ theilbar ist," Monatsh. Preuss. Akad. Wiss. Berlin, 1874, pp. 239-248.
4. T. Lepistö, "On the first factor of the class number of the cyclotomic field and Dirichlet's L-functions," Ann. Acad. Sci. Fenn. Ser. A I, no. 387, 1966. MR 33 \#4041.
5. T. Metsänkylä, "Über den ersten Faktor der Klassenzahl des Kreiskörpers," Ann. Acad. Sci. Fenn. Ser. A I, no. 416, 1967.
