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 $2H_1(m)$ 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 $H_1(3^5)$ 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

$$F_n = F_n(b_1, b_2) = 2\pi (a_1 b_1 / \phi(p^h) + a_2 b_2 / \phi(q^k))$$

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])

(1)
$$H_1(m) = \frac{1}{2}H_1(p^h)H_1(q^k)M(p^hq^k)$$

with

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

where χ runs through certain odd primitive characters, namely through all the characters

Received May 15, 1968, revised November 7, 1968.

$$\chi(n) = 0$$
 if $(m, n) > 1$,
= exp $(iF_n(b_1, b_2))$ if $(m, n) = 1$

with $1 \leq b_1 \leq \phi(p^h) - 1$, $1 \leq b_2 \leq \phi(q^k) - 1$, $b_1 + b_2$ odd. We divide the product Π_{χ} , representing the "mixed factor" of $H_1(m)$, into two products Π_{10} and Π_{01} : let Π_{10} contain all those factors of Π_{χ} where, in χ , b_1 is odd and b_2 even, and Π_{01} the other factors. The values of Π_{10} and Π_{01} are rational integers [5, p. 14]. Denoting their absolute values by T_{10} and T_{01} , respectively, we obtain

(2)
$$M(p^{h}q^{k}) = T_{10}T_{01}$$

because of the positivity of $M(p^hq^k)$. Furthermore,

(3)
$$T_{\mu\nu} = \Pi_{\mu\nu} \left\{ \left(\left(\sum_{n=1}^{m} n \cos F_n \right) \middle/ 2m \right)^2 + \left(\left(\sum_{n=1}^{m} n \sin F_n \right) \middle/ 2m \right)^2 \right\}^{1/2} (\mu\nu = 10, 01) .$$

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

$$H_1(m) = \left(\frac{1}{2}\right)^2 H_1(p^h) H_1(q^k) H_1(r^t) M(p^h q^k) M(p^h r^t) M(q^k r^t) N(p^h q^k r^t) ,$$

where $N(p^hq^kr^t)$ 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 μ , ν , and λ , 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 $H_1(p^h)$, for each power of prime dividing m, were previously known. (For the other m's, not only some of the numbers $H_1(p^h)$ 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

$$T_{10} = 0.1091819068999960 \cdot 10^{10} ,$$

$$T_{01} = 0.5200472999999732 \cdot 10^{7}$$

so that

$$T_{10} = 1 \ 091 \ 819 \ 069 = 11 \cdot 67^2 \cdot 22111$$
,
 $T_{01} = 5 \ 200 \ 473 = 3 \cdot 67 \cdot 25873$.

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 $m \leq 100$. The whole running time on the IBM 7090 was about two hours.

1016 1					
m	T ₁₀	T _{OL}	m	T ₁₀	T ₀₁
1236	1	1	$143 = 11 \cdot 13$	5 ² •7•61•661	61.83701
39 = 3.13	2	1	$144 = 2^4 \cdot 3^2$	3•13	13
4048	1 5	1	145 = 5.29	27.281.421	24.757
51 = 3.17	5	1	$147 = 3 \cdot 7^2$	7.29.673	1
$52 = 2^2 \cdot 13$	3	1	$148 = 2^2 \cdot 37$	3 ² •7•19•109	1
55 = 5.11	5	1 2 2	$152 = 2^3 \cdot 19$	3 ² •19 ²	3 ³ •19
56 = 2 ³ •7	1		$153 = 3^2 \cdot 17$	2 ⁶ •5•11 ²	2 ² •15601
57 = 3.19	3 ²	1	155 = 5•31	2 ⁴ •3 ² •5 ² •129121	2 ⁵ •631
63 = 3 ² •7	1	7	159 = 3.53	5•53 ² •3251	1
65 = 5.13	24	22	160 = 2 ⁵ •5	17	3 ² •5•41
$68 = 2^2 \cdot 17$	23	1	$161 = 7 \cdot 23$	11•67 ² •22111	3•67•25873
69 = 3.23	23	1	$164 = 2^2 \cdot 41$	23.5.71.241	1_
$72 = 2^3 \cdot 3^2$	3	1	$171 = 3^2 \cdot 19$	36 • 19 • 109	2 ² •7•73•163
$75 = 3 \cdot 5^2$	11	1	$172 = 2^2 \cdot 43$	2 ² •43•21841	1
$76 = 2^2 \cdot 19$	19	1	$175 = 5^2 \cdot 7$	61•1861	2 ⁸ •271•601
77 = 7.11	24.5	24	176 = 24.11	5•521	5 ² •11•41
80 = 24.5	1	5	177 = 3.59	523•3789257	1
85 = 5.17	5•73	17	183 = 3.61	26.5 ² .31 ³ .211	1
87 = 3.29	2 ⁶ •3	1	$184 = 2^3 \cdot 23$	23•67 ²	2•2399
$88 = 2^3 \cdot 11$	5_	11	185 = 5•37	5•7 ² •37•53 ² •9433	5•13•23833
91 = 7.13	22.7.13	2 ² •37	187 = 11.17	17 ² •41•241•299681	4801•9447601
$92 = 2^2 \cdot 23$	67	1	$188 = 2^2 \cdot 47$	47 • 742717	1
93 = 3.31	5•151	1	$189 = 3^3 \cdot 7$	109•181	7•37•127•163
95 = 5.19	13•109	22.19	$192 = 2^6 \cdot 3$	1	3 ² •401
96 = 2 ⁵ •3	1	3 ²	$196 = 2^2 \cdot 7^2$	71.27091	1
$99 = 3^2 \cdot 11$	31	3•31	$200 = 2^3 \cdot 5^2$	5.112.41	601
$100 = 2^2 \cdot 5^2$	5.11	1	201 = 3.67	2 ² •11•23 ² •67•189817	1
$10^4 = 2^3 \cdot 13$	3 ³	13	$207 = 3^2 \cdot 23$	23•727•17491	3•67•326437
$108 = 2^2 \cdot 3^3$	19	1	$208 = 2^{4} \cdot 13$	3 ³ •5•13•37	5 ² •13 ² •109
111 = 3.37	2 ² •3 ² •19 ²	1	$212 = 2^2 \cdot 53$	3.13.1093.32579	1
$112 = 2^4 \cdot 7$	3 ²	2 ² •13	$216 = 2^3 \cdot 3^3$	3 ² •19•37	271
115 = 5.23	45013	331	224 = 25.7	3 ² •5 ² •7 ²	2 ³ •13•17•769
$116 = 2^2 \cdot 29$	2 ⁶ •3•7	1	$225 = 3^2 \cdot 5^2$	11.331.2791	61 • 24 481
$117 = 3^2 \cdot 13$	2.7.13	36	$232 = 2^3 \cdot 29$		2 ³ •13•1877
119 = 7.17	3 ⁴ •5 ³ •13	97 ²	$236 = 2^2 \cdot 59$	109337677693	1
123 = 3.41	212.17	1	$244 = 2^2 \cdot 61$	33 • 5 • 11 • 61 • 691 • 6481	1
$124 = 2^2 \cdot 31$	2 ² •31•41	1	$248 = 2^3 \cdot 31$	24.11.31.41.5281	24.11.31.211
129 = 3.43	7•29•883	1,0	$272 = 2^4 \cdot 17$		2 ³ •97•577•1601
133 = 7.19	2 ² •13•19•37•73	3 ¹⁰	$288 = 2^5 \cdot 3^2$	3•13•1753	34 • 13 • 457
$135 = 3^3 \cdot 5$	37	2053	$304 = 2^4 \cdot 19$	3 ² •19 ² •37 ² •73•109	33•5•19•37•525241
$136 = 2^3 \cdot 17$	2 ⁶ •3 ²	2•97	$\cdot 320 = 2^6 \cdot 5$	17 ² •337	32•5•17•41•97•7841
141 = 3.47	47 • 13 9• 277	1	$324 = 2^2 \cdot 3^4$	19.117132157	
l		1	×432 = 2 [≝] •3 ^{\$}	32•13•19•37•1358821	13•37•109•271•541

Table II				
m	^T 100	T ₀₁₀	T ₀₀₁	T111
$\begin{array}{r} 60 = 2^2 \cdot 3 \cdot 5 \\ 84 = 2^2 \cdot 3 \cdot 7 \\ 105 = 3 \cdot 5 \cdot 7 \\ 120 = 2^2 \cdot 3 \cdot 5 \\ 132 = 2^2 \cdot 3 \cdot 5 \\ 132 = 2^2 \cdot 3 \cdot 1 \\ 140 = 2^2 \cdot 5 \cdot 7 \\ 156 = 2^2 \cdot 3 \cdot 1 \\ 168 = 2^3 \cdot 3 \cdot 7 \\ 180 = 2^2 \cdot 3^2 \cdot 5 \\ 195 = 3 \cdot 5 \cdot 1 \\ 204 = 2^2 \cdot 3 \cdot 1 \\ 220 = 2^2 \cdot 3 \cdot 1 \\ 220 = 2^2 \cdot 3 \cdot 1 \\ 220 = 2^2 \cdot 5 \cdot 1 \\ 220$	$ \begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 3 \\ 2^{4} \cdot 61 \\ 1 \\ 2^{2} \cdot 7 \\ 2^{3} \cdot 3 \cdot 17 \\ 2^{6} \cdot 3^{2} \cdot 19 \\ 1 \\ 3^{3} \\ 2^{2} \cdot 181 \\ 1 \\ 2^{4} \cdot 181 \\ 1 \\ \end{array} $	1 1 1 1 1 1 1 1 1 1 1 2 ² ·5 1 1 5 ² 1 7 ³ 1 1 2 ² ·7·13	1 1 1 1 1 1 1 1 1 1 1 1 1 1	T_{111} 2 2 2 2 13 2 2 13 2 2 11 2 13 2 2 2 2 13 2 2 2 13 2 2 2 2
			1 1 2 ² •3 ⁴	2 ¹ 0•7•31 ² 2 ⁵ •13•61 2 ³ •5 ² •13 ² •97

Table I

m	T100	T ₀₁₀	TOOL	^T 111
$336 = 2^4 \cdot 3 \cdot 7$ $340 = 2^2 \cdot 5 \cdot 17$	1 2 ⁶ •5 ²	3•97 1	1	2 ⁵ •7•61 2 ⁴ •593•3217
345 = 3.5.23	11.4159	ī	1	2•5•2152502881
$348 = 2^2 \cdot 3 \cdot 29$ $357 = 3 \cdot 7 \cdot 17$	1 7 ² •13•37•97	1	1 1	2 ⁴ •5•71317 2•7 ² •1873•1157953
360 = 2 ³ •3 ² •5	3•7	2.7	109	2 ² •5 ² •109 2 ⁵ •5 ⁴ •13 ⁴
$364 = 2^2 \cdot 7 \cdot 13$ $372 = 2^2 \cdot 3 \cdot 31$	2 ⁶ •3 ⁶ 1	1	1	25.41.13591
$380 = 2^2 \cdot 5 \cdot 19$ $396 = 2^2 \cdot 3^2 \cdot 11$	7.613	1	1	2 ³ •53 ² •73•433 2•11•13•31•181
$408 = 2^3 \cdot 3 \cdot 17$	19231 1	26.41	1	24•193•2081
$440 = 2^3 \cdot 5 \cdot 11$ $444 = 2^2 \cdot 3 \cdot 37$	5•31 ²	61•181	2•3•61 1	2 ⁵ •1381•15641 2 ³ •37•109•54721
$456 = 2^3 \cdot 3 \cdot 19$	i	19•487	ī	2 ³ •7 ² •199•3259
$460 = 2^2 \cdot 5 \cdot 23$ $468 = 2^2 \cdot 3^2 \cdot 13$	$11 \cdot 17029$ $2^{6} \cdot 3^{3} \cdot 13^{2}$	1	1	2•5•617•114259861 2 ⁴ •5 ² •11 ² •13•181
$480 = 2^5 \cdot 3 \cdot 5$ $492 = 2^2 \cdot 3 \cdot 41$	1	2 ³ •5•7 ²	1	2 ⁹ •7 ² •89
$504 = 2^3 \cdot 3^2 \cdot 7$	2 ⁴ •3 ³ •7	2 ² •3 ⁵	2 ² •3 ⁴ •7	2 ⁶ •41•1321•33161 2 ⁸ •7 ³ •13 ²
$516 = 2^2 \cdot 3 \cdot 43$ $520 = 2^3 \cdot 5 \cdot 13$	1 2 ¹¹ •3•7	1 2 ⁵ •5•7 ² •37	1 2 ³ •5 ² •17	2 ³ •3 ² •43•71•2490307 2 ¹⁸ •5•13 ² •37•73
528 = 2 ⁴ •3•11	1	5 ² •65521	1	2 ⁴ •5 ² •11•31•61•101
$540 = 2^2 \cdot 3^3 \cdot 5$ $552 = 2^3 \cdot 3 \cdot 23$	3 ² •19•73	1 23•10781	1	2•5 ² •109•38557 2 ⁴ • 2 3 ² •617•34673
$588 = 2^2 \cdot 3 \cdot 7^2$		1	1	2•2017•3571•5923
$612 = 2^2 \cdot 3^2 \cdot 17$	26•3•61•73•241	lT .	1	24•97•193•7712737

Table II (continued)

Table	III

m	Tillo	Tilol	Other T-factors that are > 1
$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$	97	2 ² •13	-
660 = 2 ² •3•5•11	5 ² •3181	2 ² •181	-
780 = 2 ² •3•5•13	26.5.61.157	2 ⁶ •109	-
$840 = 2^3 \cdot 3 \cdot 5 \cdot 7$	13•37•97	2 ⁴ •5 ² •13	$T_{0100} = 19, T_{0111} = 2^2 \cdot 5 \cdot 397$
924 = 2 ² •3•7•11	24.5.31.101.691	24•3 ³ •31•751	
$1020 = 2^2 \cdot 3 \cdot 5 \cdot 17$	2 ²⁰ •3 ² •5 ² •17	2 ³ •69857	-
$1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$	212.74.13.19.31	210.13.157.229	-
$1140 = 2^2 \cdot 3 \cdot 5 \cdot 19$	34•97•46714069	2 ³ •7 ² •19 ² •37	-
$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$	24•97•193•373	2 ⁶ •7 ² •13•31	$T_{1000} = 2^4 \cdot 3^4$, $T_{1011} = 2^4 \cdot 193 \cdot 373 \cdot 1153$
1320 = 2 ³ •3•5•11	5 ² •101•3181•20261	24.181.1481	$T_{0100} = 5.331, T_{0111} = 2^{5}.1127281$

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} $(p^{h} \geq 3, m_{1} > 1)$. 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 $\phi(p^{h})$ 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., $p^{h} \geq 5$), we found only 8 exceptions to it (e.g., for $m = 2^{3} \cdot 23$ the pair $(2^{3}, 2399)$

where 2398 is not divisible by 4). All these exceptions can be removed by replacing the divisor $\phi(p^h)$ by $\frac{1}{2}\phi(p^h)$. This is not always the case, however (take, e.g., for $m = 2^2 \cdot 31$ the pair (31, 41)).

The prime factors of $H_1(p^h)$ seem often to have the corresponding property. To mention here only a few examples, $H_1(41) = 11^2$, $H_1(43) = 211$, and $H_1(7^2) = 43$.

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 nten Einheitswurzeln gebildeten komplexen

2. D. Monarsh. Preuss. Akad. Wiss. Berlin, 1861, pp. 1051–1053.
3. E. KUMMER, "Über diejenigen Primzahlen λ, für welche die Klassenzahl der aus λten Einheitswurzeln gebildeten komplexen Zahlen durch λ 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.