A Table of the First Factor for Prime Cyclotomic Fields

By Morris Newman

Abstract. The first factor of the prime cyclotomic fields for all primes < 200 is computed by means of a determinantal formula, correcting some errors in tables of Kummer.

Let $p = 2m + 1$ be an odd prime. Let ζ be a primitive pth root of unity, and let R be the field of rationals. It is well known that if h is the class number of the cyclotomic field $R(\zeta)$, and h_0 the class number of the totally real subfield $R(\zeta + 1/\zeta)$, then h is divisible by h_0. The quotient h/h_0 is denoted by h^*, and is known as the *first factor* of h. A complete discussion of these matters is to be found in the beautiful book [1] by Borevič and Šafarevič, where a table (uncredited) of h^* is given for all odd primes $p < 100$. Presumably, this table is due to Kummer, who computed h^* for all odd primes $\leqq 163$ (see [2] and [3]). The numbers h^* are quite difficult to compute, and it is of some interest to verify and to extend the above-mentioned tables. The importance of h^* stems from the fact that the prime p is irregular if and only if p divides h^*.

It turns out that Kummer's tables are not error-free: the values of h^* corresponding to $p = 103$, 139, and 163 are incorrect. The fact that $p = 103$ is irregular, and was correctly identified to be so by Kummer, is explicable by his method of computation.

Let g be a primitive root modulo p. Define

$$g_n = g^n - p[g^n/p], \qquad n = 0, 1, 2, \cdots .$$

Let θ be a primitive $(p - 1)$st root of unity. Then the first factor h^* is given by the formula

$$h^* = \frac{1}{(2p)^{m-1}} F(\theta)F(\theta^3) \cdots F(\theta^{p-2}) ,$$

where

$$F(x) = \sum_{n=0}^{p-2} g_n x^n .$$

Kummer expresses h^* as the product of norms

$$h^* = \frac{1}{(2p)^{m-1}} \prod_{d\mid m;\, d \text{ odd}} N\{F(\theta^d)\} ,$$

and computes each rational integral factor $N\{F(\theta^d)\}$ separately. Thus an error in the computation of h^* can occur without violating the divisibility (or nondivisibility)

Received June 5, 1969, revised August 7, 1969.
AMS Subject Classifications. Primary 1002; Secondary 1066.
Key Words and Phrases. Cyclotomic fields, class numbers, tables, factorizations.

of h^* by p, if the error occurs in the proper place. Notice that the formula above indicates that if m has many odd divisors, then h^* can be expected to have many factors.

The number h^* can also be expressed as a determinant. The companion matrix of the $m \times m$ diagonal matrix diag $(\theta, \theta^3, \cdots, \theta^{p-2})$ is the generalized permutation matrix

$$Q = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 \\ -1 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

which of course is nonderogatory and satisfies $Q^m + I = 0$. Therefore, the determinant of the matrix $F(Q)$ is just $(2p)^{m-1}h^*$, and this leads (after some elementary rearrangements) to the formula

$$(2p)^{m-1}h^* = |\det(A)| ,$$
$$A = (g_{m+i+j} - g_{i+j}) , \qquad 0 \leqq i , \;\; j \leqq m - 1 ,$$

given as problem 5 on p. 367 of [1].

This formula is somewhat unsatisfactory however, because of the occurrence of the factor $(2p)^{m-1}$. This can be remedied very simply by taking into account the relationships

$$g_{i+j} \equiv g_i g_j \bmod p , \qquad g_{i+m} + g_i = p .$$

Subtract row 0 of A from every other row. A factor 2 now occurs throughout the last $m - 1$ rows. Remove this factor of 2^{m-1}, and then subtract g_j times column 0 from column j, $1 \leqq j \leqq m - 1$. A factor p now occurs throughout the last $m - 1$ columns. Remove this factor of p^{m-1}. The result is that

$$h^* = |\det(B)| , \qquad B = (b_{ij}) , \qquad 0 \leqq i , \;\; j \leqq m - 1 ,$$

where

$$\begin{aligned} b_{00} &= p - 2 , & & \\ b_{0j} &= 1 - g_j , & & 1 \leqq j \leqq m - 1 , \\ b_{i0} &= 1 - g_i , & & 1 \leqq i \leqq m - 1 , \\ b_{ij} &= (g_i g_j - g_{i+j})/p , & & 1 \leqq i, j \leqq m - 1 . \end{aligned}$$

The computation of det (B) for all odd primes < 200 was carried out as a test of a program of the author's which finds the exact solution of a system of linear equations with whole number coefficients, and which also produces the determinant of the system. Storage requirements limit the program to systems of 100 equations or less, which is sufficient to accommodate the above mentioned primes. The program incorporates a check by direct multiplication which guarantees the accuracy of the results obtained. In addition, it is known that the irregular primes under 200 are $p = 37, 59, 67, 101, 103, 131, 149, 157$; and in each of these instances h^* is divisible by p, furnishing an additional check on the computation. For $p = 157$, h^* is divisible by p^2, as was already noticed by Kummer [3]. This suggests the conjecture: There are infinitely many primes p such that h^* is divisible by p^2, or indeed

TABLE 1

p	h^*
3	1
5	1
7	1
11	1
13	1
17	1
19	1
23	3
29	8
31	9
37	37
41	121
43	211
47	695
53	4889
59	41241
61	76301
67	8 53513
71	38 82809
73	119 57417
79	1001 46415
83	8382 16959
89	1 33793 63737
97	41 13228 24001
101	354 74043 78125
103	906 90946 43165
107	6343 49335 42623
109	16178 48001 22409
113	1 61207 20013 62952
127	2604 52918 62639 92195
131	28496 37972 92721 36525
137	6 46901 57017 52009 68153
139	17 53848 91648 49256 81747
149	6878 87859 68717 47201 23201
151	23335 46653 54774 25844 39257
157	5 62343 27700 40183 27670 69245
163	270 85347 44692 07705 18751 31636
167	2812 11898 30322 93317 83153 82891
173	1 70254 62666 54155 84751 67800 34265
179	77 28157 72120 30298 59275 69747 21745
181	211 42175 77499 87541 69722 55015 39625
191	1 65008 36548 72236 56458 98761 13269 29859
193	5 46617 10591 35681 65545 65075 26307 67041
197	55 32802 21871 36007 06095 99371 32906 31720
199	188 44055 28660 25308 02019 84701 27215 55487

TABLE 2
Factorization of h^*

p	
3	–
5	–
7	–
11	–
13	–
17	–
19	–
23	3
29	2·2·2
31	3·3
37	37
41	11·11
43	211
47	5·139
53	4889
59	3·59·233
61	41·1861
67	67·12739
71	7·7·79241
73	89·134353
79	5·53·377911
83	3·279405653
89	113·118401449
97	577·3457·206209
101	5·5·5·5·5·101·601·18701
103	5·103·1021·17247691
107	3·743·9859·2886593
109	17·1009·9431866153
113	2·2·2·17·11853470598257
127	5·13·43·547·883·3079·626599
131	3·3·3·5·5·53·131·1301·4673706701
137	17·17·47737·46890540621121
139	3·3·47·47·277·277·967·1188961909
149	3·3·149·512966338320040805461
151	7·11·11·281·25951·1207501·312885301
157	5·13·13·157·157·1093·1873·418861·3148601
163	2·2·181·23167·365473·441845817162679
167	11·499·5123189985484229035947419
173	5·20297·231169·725717293628518706 21
179	5·1069·1445866739233494828676463 5121
181	5·5·5·37·41·61·1321·2521·5488435782589277701
191	11·13·51263·612771091·3673395066973 3713761
193	6529·15361·29761·91969·10369729·192026280449
197	2·2·2·5·1877·7841·9398302684870866656225611549
199	3·3·3·3·19·727·25645093·207293548177·3168190412839

by any given power of p. The conjecture is true for the first power, since it is known that there are infinitely many irregular primes. Vandiver has proved that h^* is divisible by p^2 if and only if there are integers a, b such that $1 \leqq a < b \leqq m - 1$, and the numerators of the Bernoulli numbers B_{2a}, B_{2b}, are each divisible by p.

Table 1 gives the values of p and h^*. Table 2 gives the factorization of h^*, and was computed by D. H. Lehmer. The author had determined all prime factors $< 10^5$ of h^*, but was unable to produce all factors, because of lack of machine time. Professor Lehmer kindly remedied this situation.

There are some interesting points in the tables. Thus for p under 200, h^* is even only for $p = 29, 113, 163$, and 197; and in all of these cases h^* is divisible by 4. There is thus a distinct possibility that h^* is never singly even. Also h^* is composite for all primes p such that $59 \leqq p \leqq 199$, prompting the somewhat dubious conjecture that h^* is always composite except for finitely many p. Also h^* is square-free in 29 of the 45 cases given; and $29/45 = .64444 \cdots$ does not compare too badly with $6/\pi^2 = .60792 \cdots$.

The computation of Table 1 was carried out on the computer of the National Bureau of Standards, and required approximately 30 minutes of machine time.

National Bureau of Standards
Washington, D. C. 20234

1. Z. I. Borevič & I. R. Šafarevič, *Number Theory*, "Nauka", Moscow, 1964; English transl., Academic Press, New York, 1966. MR **30** #1080; MR **33** #4001.

2. E. Kummer, "Über die Klassenanzahl der aus $n$ten Einheitswurzeln gebildeten complexen Zahlen," *Monatsh. Preuss. Akad. Wiss. Berlin*, 1861, pp. 1051–1053.

3. E. Kummer, "Über diejenigen Primzahlen λ, für welche die Klassenzahl der aus λ ten Einheitswurzeln gebildeten complexen Zahlen durch λ theilbar ist," *Monatsh. Preuss. Akad. Wiss. Berlin*, 1874, pp. 239–248.