## Table of the Cyclotomic Class Numbers $h^*(p)$ and Their Factors for 200

By D. H. Lehmer and J. M. Masley

Abstract. This table gives the values of the "first factor"  $h^*(p)$  and their factorizations for all primes p, 200 . This extends similar data by M. Newman [Math. Comp., v. 24, 1970, pp. 215-219], and Schrutka [Berlin Akad. Abn., 1964]. The two methods used to compute these data are described.

1. Introduction. The present table extends a similar one given by Newman [8], for p < 200, in 1970. At that time Newman was unaware of a larger table by Schrutka [10] containing  $h^*(p)$  and its factors for  $p \le 257$ . In setting the range 200 the authors decided to include the nine primes between 200 and 257 because Schrutka's table is incomplete as to some factorizations and also because his table is unavailable in most libraries. The present table appears in the microfiche section.

Two methods were used to obtain the results given herewith. The first method, an elaboration of Newman's, gives the value of  $h^*(p)$  by a determinant. The second method obtains  $h^*(p)$  as a product of its "algebraic" factors which in turn have their factors so strongly restricted that many quite large values of  $h^*(p)$  have been completely factored. This factorization theory has been set forth in two other papers (Lehmer [5] and Masley [6]) from different points of view. This second method is more expensive than the first and, for p > 300, was used only to get all but the largest factor of  $h^*(p)$ , the latter being obtained from the value of  $h^*(p)$  as given by the first method.

2. First Method. This method uses modular arithmetic to evaluate  $h^*(p)$  from the formula

$$h^*(p) = |\det M|,$$

where M is the 0-1 matrix of order (p-5)/2

$$M = \{m_{rc}\}$$
  $(r, c = 3(1)(p-1)/2)$ 

with

$$m_{rc} = \left[\frac{rc}{p}\right] - \left[\frac{(r-1)c}{p}\right].$$

This formula was first published by Carlitz and Olson [1] as a consequence of their work on Maillet's determinant. A direct derivation is given in [6].

Before resorting to congruential computation it is advantageous to reduce M by elementary row and column operations to a much smaller matrix B. This reduction is aided by the fact that M is relatively sparse, having almost 75% of its entries zero,

and the fact that the ones in M in column c are situated in rows

$$r = \left[\frac{(i-2)p}{c}\right] + 1 \qquad (i = 3(1)[(c-1)/2]).$$

Some of this reduction can be done for a general p. In fact, one may cross out columns 3, 4, 6 and rows  $\lfloor p/6 \rfloor + 1$ ,  $\lfloor p/4 \rfloor + 1$ , and  $\lfloor p/3 \rfloor + 1$ , thus reducing M to a 0-1 matrix of order (p-11)/2. Further reductions depending on the form of p can be automated. For the range 200 the matrix <math>M was reduced to a matrix B of order k with p/5 < k < p/3 without any element of B exceeding  $10^6$  in absolute value. This preliminary reduction can be compared with that used by Newman  $\lfloor 8 \rfloor$  whose B is of order (p-1)/2 with mostly nonzero entries less than p in absolute value. To compute det B use was made of modular arithmetic. Remainders  $r_i$  were found for which

$$\det B \equiv r_i \pmod{q_i} \qquad (i = 1(1)t)$$

and then combined by the Chinese remainder theorem to determine the actual value of det B. The  $q_i$  were chosen to be primes slightly greater than  $10^9$ , and the process is valid provided

$$|\det B| < q_1 q_2 \cdots q_t.$$

To make an efficient choice of t it is essential to know quantitative upper bounds for  $|\det B| = h^*(p)$ . Fortunately, these have recently become available. Kummer [2] asserted that  $h^*(p)$  is asymptotic to the function

(2) 
$$G(p) = 2p(p/4\pi^2)^{(p-1)/4}.$$

This has not yet been proved. The best result to date in this direction is due to Lepistö [3] who proves that for p > 200,

$$-\frac{1}{2} \log p - 4 \log \log p - 12.93 - 4.66 \log p$$

$$\leq \log(h^*(p)/G(p)) \leq 5 \log \log p + 15.49 + 4.66/\log p.$$

These results can be improved by methods used in [6] but not enough to yield Kummer's conjecture. For the range 200 the best known upper bound is

(3) 
$$\log(h^*(p)/G(p)) \le \log p + \log \log(p/3) + 3.52.$$

The number t of moduli was chosen using (2) and (3) so that at most one modulus was "wasted" in satisfying (1).

Every value of  $h^*(p)$  obtained by this method was later compared with the table of approximations to  $h^*(p)$  given in Pajunen [9]. These values were also subjected to stringent divisibility conditions imposed by the second method. Newman's results for p < 200 were recomputed in 90 seconds, as opposed to 30 minutes by Newman's method, and no discrepancy was found.

3. Second Method. This method is based on a norming procedure as applied to the fundamental factorization formula

(4) 
$$h^*(p) = \prod_{ef=p-1; f \text{ odd}} h_e(p).$$

The positive integer  $h_e(p)$ , called the relative class number of degree e, is given by

(5) 
$$h_e(p) = p^{[e/(p-1)]} N_e(W_e(p)) / Q_{\tau}(2)^{\gamma}.$$

Here

$$\tau = \tau(e) = \frac{e}{(e, \operatorname{ind}_{g} 2)},$$

where g is any primitive root of p.  $Q_{\tau}(x)$  is the monic polynomial of degree  $\phi(\tau)$  whose roots are the primitive  $\tau$ th roots of unity and

$$\gamma = \gamma(e) = \phi(e)/\phi(\tau).$$

Finally,

$$W_e(p) = \sum_{n=1}^{(p-1)/2} (\epsilon_n - \epsilon_{n-1}) \alpha^n,$$

where  $\alpha = \exp\{2\pi i/e\}$ ,

$$\epsilon_n = \begin{cases} 1 & \text{if } g^n - p[g^n/p] < p/2, \\ 0 & \text{otherwise;} \end{cases}$$

and  $N_{\rho}(W_{\rho}(p))$  is the norm of  $W_{\rho}(p)$  in the cyclotomic field of eth roots of unity.

This elaborate and relatively expensive formula is effective in factoring  $h^*(p)$ . Furthermore, it is shown in [5] and [6] that if

$$h_e(p) = q_1 q_2 \cdots q_t$$

is the canonical factorization of  $h_e(p)$  into a product of distinct prime powers  $q_i$  (i = 1(1)t) then each  $q_i$  prime to e is of the form ex + 1, a valuable condition for several methods of factorization.

In (5) the function  $Q_{\tau}(2)$  is readily evaluated by

$$Q_{\tau}(2) = \prod_{\delta \mid \tau} (2^{\delta} - 1)^{\mu(\tau/\delta)},$$

where  $\mu$  is the Möbius function. Thus, the real expense of this method is that of the calculation of the norm

(6) 
$$N_e(W_e(p)) = \prod_{(t,e)=1; t < e} \left\{ \sum_{n=1}^{p-1} (\epsilon_n - \epsilon_{n-1}) \alpha^{nt} \right\} = \prod_{(t,e)=1} W_e(p, t).$$

Metsankyla [7] has suggested a straightforward approach via multiprecise approximation of each factor of (6) using floating-point arithmetic followed by the recognition of the huge integer  $N_e$ . Instead, it was decided to follow a suggestion of Spira [11] and use a vector manipulation method with exact fixed point multiprecision arithmetic.

We begin the norming program by determining the coefficients

$$A_n = \epsilon_n - \epsilon_{n-1} = \pm 1, 0$$

of  $W_e(p, 1)$  in a prelude to the main routine which generates a table of powers of a primitive root  $g \pmod{p}$ . We can then think of  $W_e(p, 1)$  simply as a vector of dimen-

sion (p-1)/2

$$W_e(p, 1) \sim [A_1, A_2, \dots, A_{(p-1)/2}].$$

Since

$$\alpha^{n+e} = \alpha^n, \quad \alpha^{r+e/2} = -\alpha^r,$$

this vector can be compressed to one of dimension e' = e/2

(7) 
$$W_e(p, 1) \sim [a_1, a_2, \dots, a_{e'}],$$

where the a's are small integers. The corresponding vectors for the other factors  $W_{\rho}(p, t)$  have the same set of components but in a different order.

To compute  $N_e(W_e(p))$  we multiply the several vectors together in the Cauchy sense. Thus, in multiplying (7) by any other vector

$$[b_1, b_2, \ldots, b_{e'}]$$

we first obtain a vector

$$[c_1, c_2, \ldots, c_e]$$

of dimension e with

$$c_n = \sum_{i+j=n} a_i b_j$$
  $(n = 1(1)e).$ 

This is then compressed into a vector of dimension e' by replacing  $c_n$  by  $c_n - c_{n+e'}$  for n=1(1)e'. (In case e=p-1 this whole procedure involves only addition and subtraction since  $a_i=A_i=\pm 1, 0$ .) Accumulating factors in this way, we obtain a vector representing the product of the first  $\phi(e)/2$  factors in (6). Since the factors for t and e-t are complex conjugates, the vector for the second half-product has the same components as those of the first but in reverse order. Multiplying these two vectors together, we obtain a vector for  $N_e(W_e(p))$ 

$$[C_1, C_2, \ldots, C_e]$$

with large integer components. To find the integer thus represented we change notation slightly, replacing  $C_i$  by f(i-1), and write

$$N_e(W_e(p)) = f(0) + f(1)\alpha + \cdots + f(e-1)\alpha^{e-1}$$
.

Let  $\delta$  be any divisor of e and let  $e=e_1\delta$ . If  $t_i$   $(i=1(1)\phi(e_1))$  are the numbers  $\leq e_1$  and relatively prime to  $e_1$ , then  $\alpha^{\delta t_i}$  are the primitive  $e_1$  th roots of unity and their sum is  $\mu(e_1)$ . Since they are algebraically indistinguishable, their corresponding coefficients  $f(\delta t_i)$  must be equal and equal to  $f(\delta)$ . Hence, we have

$$N_e(W_e(p)) = f(0) + \sum_{\delta \mid e} \mu(e_1) f(\delta) = f(0) + \sum_{\delta \mid e} \mu(\delta) f(e/\delta),$$

a formula that is easily programmed.

5. Irregular Primes. Kummer called a prime p irregular in case p divides a Bernoulli number  $B_{2a}$  with 2a < p. Of the 51 primes in the range of our table 20 are irregular. As a result of a recent paper by Ribet [12], it follows that  $p \mid h_e(p)$  where

e = (p-1)/(p-1, 2a-1). This affords a welcome check on the computed value of  $h_{\rho}(p)$ . The following table lists these cases.

p	2 <i>a</i>	e	p	2 <i>a</i>	e
233	84	232	389	200	388
257	164	256	401	382	400
263	100	262	409	126	408
271	84	270	421	240	420
283	20	282	433	366	432
293	156	292	461	196	92
307	88	102	463	130	154
311	292	310	467	94	466
347	280	346	467	194	466
353	186	352	491	292	490
353	300	352	491	336	98
379	100	42	491	338	490
379	174	378			

The evidence in the main table supports the conjecture that the product  $B_2B_4 \ldots B_{p-1}$  and  $h^*(p)$  contain p to the same highest power.

6. Description of the Tables. Table 1 gives for each of the 51 indented entries p with  $200 the value of the first factor <math>h^*(p)$  of the cyclotomic class number of  $Q(\exp{2\pi i/p})$ . This table and the next appear in the microfiche section of this issue.

Table 2 gives the factorizations of the entries in Table 1 as given by (4); one line is devoted to each  $h_e(p)$ . The first entry in each line is e itself. Each unmarked factor is a prime. If a factor is followed by \* it is intrinsic, i.e. all of its prime factors divide e. If a factor is followed by # the factor is a power of a prime,  $q^{\alpha}$ ,  $\alpha > 1$ , such that e divides  $q^{\alpha} - 1$ . For example, for p = 313, e = 24, the entry 1369 # is  $37^2$  and 1368 = 24.57. Oversize entries are put in two Appendices in order of size. The first of these is for primes designated by P followed by the number of its digits; a number greater than 37. The second Appendix is for composite numbers designated by C. For each of these numbers a space is left in the main Table 2 for writing in whatever factors may be discovered in the future. All such prime power factors are known to exceed  $10^{11}$ .

The following procedures were followed in preparing Table 2. As soon as  $h^*(p)$  was computed by the first method it was searched for factors less than  $10^5$  to discover all its intrinsic factors and the factors that are powers of small primes. The residual factor N was next tested for pseudo-primality by seeing whether

$$13^N \equiv 13 \pmod{N}.$$

If (8) fails to hold, N is composite and all its extrinsic prime power factors are of the form ex + 1. In this case a search for small factors of N was made using the Illiac IV which makes 64 trial divisions simultaneously, up to the limit  $10^{11}$ . After removing such factors, if any, from N and applying (8) to the residual factor, a more serious

attempt at factorization was made. For numbers up to 30 digits the Delay Line Sieve was used and for numbers up to 38 digits the Pollard Rho method and, if necessary, the Brillhart-Morrison method were applied by M. Wunderlich of the Northern Illinois University. As a result, we can say of the 26 composite numbers in the appendix that none has a prime factor  $< 10^5$  and if any prime factor exists between  $10^5$  and  $10^{11}$  its square must also be a factor. Any pseudoprimes discovered were sent to H. S. Williams at the University of Manitoba, who carried out the final tests for primality in all cases.

Acknowledgements. The authors greatfully acknowledge the contributions of Professors Williams and Wunderlich noted above and the services of the Computer Centers of their Universities and those of the University of Illinois at Chicago Circle and the Institute for Advanced Computing. Professors A. O. L. Atkin and John Selfridge made several helpful suggestions and contributions.

Department of Mathematics University of California, Berkeley Berkeley, California 94720

Department of Mathematics University of Illinois at Chicago Circle Chicago, Illinois 60680

- 1. L. CARLITZ & F. R. OLSON, "Maillet's determinant," Proc. Amer. Math. Soc., v. 6, 1955, pp. 265-269.
- 2. E. E. KUMMER, "Memoire sur la theorie des nombres complexes composes de racine de l'unite et de nombre entiers," *J. Math. Pures Appl.*, v. 16, 1851, pp. 377-498, p. 473. *Collected Works*, v. 1, Springer-Verlag, Berlin and New York, 1975, p. 459.
- 3. T. LEPISTÖ, "On the growth of the first factor of the class number of the prime cyclotomic field," Ann. Acad. Sci. Fenn. A1, No. 577, 1974, p. 21.
- 4. D. H. LEHMER, "Factorization of certain cyclotomic functions," *Ann. of Math.*, v. 34, 1933, pp. 461-479.
- 5. D. H. LEHMER, "Prime factors of cyclotomic class numbers," Math. Comp., v. 31, 1977, pp. 599-607.
- 6. J. M. MASLEY, "On the first factor of the class number of prime cyclotomic fields," (To appear.)
- 7. T. METSANKYLA, "On prime factors of the relative class numbers of the cyclotomic fields," Ann. Univ. Turku. Ser. A I, no. 149, 1971, 8 pp.
- 8. M. NEWMAN, "A table of the first factor for prime cyclotomic fields," *Math. Comp.*, v. 24, 1970, pp. 215-219.
- 9. S. PAJUNEN, "Computation of the growth of the first factor for prime cyclotomic fields," BIT, v. 16, 1976, pp. 85-87.
- 10. G. SCHRUTKA V. RECHTENSTAMM, "Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, deren, Funktiones Wurzelexponenten (grad) nich grosser als 256 ist," Abh. Deutsch. Akad. Wiss. Berlin Kl. Math. Phys. Tech., v. 2, 1964, pp. 1-64.
- 11. R. SPIRA, "Calculation of the first factor of the cyclotomic class number," *Computers in Number Theory*, Proceedings Atlas Symposium 1969, Academic Press, New York, 1971, pp. 149-151.
- 12. K. A. RIBET, "A modular construction of unramified p-extensions of  $Q(\mu_p)$ ," Invent. Math., v. 34, 1976, pp. 151-162.

L. H. Kirm., and J. 24. Masky, Table of the gentleme transcriments of the party of the gentleme transcriments of the party of the gentlement of the gentlement

```
14 1
42 211
47
2 5
46 139
52
4 1
52 4889
59
2 1
56 59.233
61
4 1
12 1
60 1861
67
2 1
60 1861
67
7 1
10 1
14 7*
70 79241
73 889
24 1
72 134353
79
2 5 6 1
26 53
77 1
26 53
78 377011
83
2 3
8 118401449
97
32 3457
96 577.206209
```

3.

```
4.
```

241 16 2209# 48 2359873 60 18601.126767281 240 13921.518123008737871423891201

257 256 257.20738946049.P43

251 2 7 10 11 50 348270001 250 9631365977251.369631114567755437243663626501 5. -

C43

6.

```
7,

8 233
24 13609
104 65366361,30356065621633
312 158268017,82941207961,986685963782009603919680953
317
4 13
316
331
2 3
6 98
10 819
22 23,67
30 819,61
66 1740685061
110 476506973241786667381
330 270271,221478181712309125848473872740271
337
16 17,17,499,353
48 238321
112 49-634460358265098929
336 649,3246769.

347
2 5
346 347,P62
349
4 5
12 164-13
353
32 6113,9473
352 133,383,281249,1380c11233,3001891853,P50
369
2 19
366
367
2 3,3
2 613,9473
373
4 5
12 61
124 932,268738674461290742168853881
366 39163,P57
373
4 5
12 61
124 328-1117,6218651821,1699148567515153
372 1489,191953,P64
```

```
2 3
6 39-13
14 14-90
18 38-90
19 38-70
19 38-70
19 38-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
19 39-70
```

467 2 7

6 7
18 37-37
54 919-2647-10909
162 105792780991-1355141213769532941
486 58321-105290443.

491
2 3-3
10 11-11-11
14 644-29
70 1262296191031
96 491-101566319-2311247713517
490 491-491-6490251-17641391-74466731-P66
499
499
499
499
409
409
503
2 3-7
502 15061.

C137

DPI MES AND PSEUDOPRIMES

P 40 283 282
588646640749005679915789619426099076673

P 41 349 348
16068629796320170064136004281782850431947

P 43 257 256
1022907744563911961561298698183419037149697

P 45 263 262
418789100985678667328189444629948074260186283

P 50 353 352
39436838605418321373197463887181225470103134619777

P 54 311 310
656682084088129583850988747281311805392434897275868681

P 54 373 372
124204598699794021789479401683826456140588477617076789

P 57 367 366

P 68 491 490

*,,*.

```
P 75 457 456
2866261368100953583914839795438110146835356019940364553577391673663478x
73193
p 78 431 430
1122259884949922466392436728594502180831294900126573138239685965731922X
0712251
P 82 347 346
1984086942665238828259012186195350500935086726556560834433397220152315×
402574339617
P 92 461 460
3702458172193117785898149655903648058852928086226081699845637442037167X
471983906827999352581
P 93 443 442
3098602910769433690373034133232851589853135263981528310088719135950503X
72355089612436688273929
                                    COMPOSITE COFACTORS
```

C 41 337 336 90155255092450385897373749804875115776993

18022473215169065702224279183302091210994749548801576948376558921841

```
C 43 233 232 1042818810684723912819200922459107271266041
C 45 379 378 6679 16 371 334851141 4818462346350 90523847 £11057
C 46 269 268 7157703949875286788563837229656316512687317037
C 48 433 432 622088324646050444728308803354390803092611083297
C 59 397 396 985 985 985 985 985 985 985 124 1187 390 895 86 98 987 177 85 982 71 388 337 66 16 30 657 550 50 570 897
C 63 463 462
293093136731703607202057612534209505683184518607741865606347983
C 64 401 400
1225711629382980898939491451166603962805470574636880278524656401
C 64 409 408
A489027467098599562453763162012349492601639687360064733349887033
C 74 317 316
1164475330310779415596791998268165702139727841573981667433720227984197X
```

- C 79 499 498 1379859664125541127232716076628501109433371868500136710045903488661634×
  481872621
- ( 79 487 486 2653061774127486590992495990266403206868559033116723924341103789395399X 596493377
- C 83 389 388 1318810393670663433086629375321892487617273161081487576512160176357043X 9154394867861
- C 88 359 358 280027260039638618946752046409325116666477500724385046611055955572436X 780048605056309140
- C 88 383 382 22846016628829978160948556092709581696125257695406186411922697858X 7813781614378563037
- C 94 419 418 45008104751181594456024969850109A7794756412620409584452243425473174592× #715489506774710185811321
- C102 449 448 1752372714389140930875017461193597782783832015622478409931964789351065X 359324101382291222235820186930881
- C116 479 478 1871097411261585948545764453621534630583466428637695083286315528796115X 2884061744270377505550446401715621946096288691
- C122 467 466 54641661023761393420074367301496346099317:5531144153297812367300285471x 186018289270785601543223084063C523038537374078314923
- C 137 503 502 176758239285847574623471594487660729989329703033335548759180661969866602 1129435172945169259928866803424917161318916495662053049743744960683

C144 509 508 1133569133933777271278271038172373516365520615787844993430500930505415x 22303661144488619260756827331990221782091564990199335291686703341360133x 249