MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 142
APRIL 1978, PAGES 577–582

Table of the Cyclotomic Class Numbers $h^*(p)$ and Their Factors for $200 < p < 521$

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, $200 < p < 521$. 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 $p \leqslant 257$. In setting the range $200 < p < 521$ 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 $(p - 5)/2$

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

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,

Received March 14, 1977.
AMS (MOS) subject classifications (1970). Primary 12A35, 12A50, 12C20.

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 $[p/6] + 1$, $[p/4] + 1$, and $[p/3] + 1$, 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 $200 < p < 521$ the matrix 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 [8] 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

$$|\det B| < q_1 q_2 \cdots q_t. \tag{1}$$

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

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

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

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

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

These results can be improved by methods used in [6] but not enough to yield Kummer's conjecture. For the range $200 < p < 521$ the best known upper bound is

$$\log(h^*(p)/G(p)) \leqslant \log p + \log\log(p/3) + 3.52. \tag{3}$$

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

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

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

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

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 τth 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 $N_e(W_e(p))$ is the norm of $W_e(p)$ 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 μ is the Möbius function. Thus, the real expense of this method is that of the calculation of the norm

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

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 (mod p). We can then think of $W_e(p, 1)$ simply as a vector of dimen-

sion $(p-1)/2$

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

Since

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

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

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

where the a's are small integers. The corresponding vectors for the other factors $W_e(p, t)$ 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

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

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 δ be any divisor of e and let $e = e_1\delta$. If t_i $(i = 1(1)\phi(e_1))$ are the numbers $\leqslant e_1$ and relatively prime to e_1, then $\alpha^{\delta t_i}$ are the primitive e_1th 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 $h_e(p)$. The following table lists these cases.

p	$2a$	e	p	$2a$	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 $200 < p < 521$ the value of the first factor $h^*(p)$ 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^α, $\alpha > 1$, such that e divides $q^\alpha - 1$. For example, for $p = 313$, $e = 24$, the entry 1369# is 37^2 and $1368 = 24 \cdot 57$. 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

$$13^N \equiv 13 \pmod{N}. \tag{8}$$

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. A*1, 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.