MATHEMATICS OF COMPUTATION, VOLUME 31, NUMBER 138
APRIL 1977, PAGES 599–607

Prime Factors of Cyclotomic Class Numbers

By D. H. Lehmer

Abstract. Let p be an odd prime. The "first factor" $h^*(p)$ of the class number of the field of pth roots of unity has been the subject of many investigations beginning with Kummer (1861). In the present paper it is shown how the theory of a function introduced by T. A. Pierce (1917) can be used to find the prime factors of $h^*(p)$.

1. Introduction. Let p be an odd prime with a primitive root g. Let $g^n \equiv g_n \pmod p$ $(0 < g_n < p)$ $(0 \leqslant n < p-1)$. Denote by $F = F_p$ the polynomial

$$F_p(x) = \sum_{n=0}^{p-2} g_n x^n. \tag{1}$$

Finally, let $\theta = \exp\{2\pi i/(p-1)\}$. Then $h^*(p)$, the so-called first factor of the number of classes of ideals in the field generated by $\exp\{2\pi i/p\}$, is given by Kummer's formula [3, p. 358, formula (5.6)]

$$(2p)^{(p-3)/2} h^*(p) = \left| \prod_{\nu=0}^{(p-3)/2} F_p(\theta^{2\nu+1}) \right|. \tag{2}$$

In Kummer's original paper [1] the formula appears without absolute value signs. If these are omitted, it is necessary to include a minus sign in (2) above, as will be shown below. It is our purpose to show in an elementary way how the theory of Pierce's function, as developed in [2], can be used to sort out the prime factors of $h^*(p)$ into arithmetic progressions so as to render feasible the factorization of $h^*(p)$ for quite large values of h^*.

2. Notation and Lemmas. Let $M = 2^\lambda \omega$, ω odd, be any positive integer and let $Q_k(x)$ be the cyclotomic polynomial whose roots are the primitive kth roots of unity. Let $\Omega_M(x)$ be the monic polynomial whose roots are the distinct odd powers of $\rho = \exp\{2\pi i/M\}$.

LEMMA 1. $\Omega_M(x) = \Pi_{\delta \mid \omega} Q_{M/\delta}(x)$.

Proof. In case M is odd, so that $M = \omega$, the lemma becomes the familiar identity

$$\prod_{d \mid M} Q_d(x) = x^M - 1.$$

In case M is even we have

Received August 30, 1976; revised September 20, 1976.
AMS (MOS) subject classifications (1970). Primary 12A35, 12A50, 12–04, 10A35.

$$\Omega_M(x) = \prod_{n=1;n\ \mathrm{odd}}^{M} (x - \rho^n) = \prod_{\delta \mid \omega} \prod_{(t,M/\delta)=1} (x - \rho^{t\delta}) = \prod_{\delta \mid \omega} Q_{M/\delta}(x).$$

We define Pierce's function $Q_k^*(P)$ of the polynomial P by

$$Q_k^*(P) = \prod_{i=1}^{r} Q_k(\beta_i), \tag{3}$$

where β_i are the roots of P. When P is monic with integer coefficients, it is clear that $Q_k^*(P)$ is an integer, being a symmetric function of the roots of P.

Before proceeding further, we give a variant of Kummer's formula (2) which has two advantages: (a) it is analytic, (b) it replaces F_p by a monic polynomial.

LEMMA 2. *Let $G_p(x)$ be the polynomial*

$$G_p(x) = \sum_{n=0}^{p-2} g_n x^{p-n-2}. \tag{4}$$

Then

$$(2p)^{(p-3)/2} h^*(p) = \prod_{\nu=0}^{(p-3)/2} G_p(\theta^{2\nu+1}). \tag{5}$$

Proof. Comparing (4) with (1), we see that

$$G_p(x) = x^{p-2} F_p(1/x)$$

and that

$$|G_p(\theta^{2\nu+1})| = |\theta^{(p-2)(2\nu+1)}||F_p(\theta^{p-2-2\nu})| = |F_p(\theta^{2\lambda+1})|,$$

where

$$\lambda = (p-3)/2 - \nu. \tag{6}$$

Hence the product in (5) does not differ in absolute value from that in (2). It remains to show that it is positive.

If we compare $\theta^{2\nu+1}$ with $\theta^{2\lambda+1}$, where λ is defined by (6), we see that they are complex conjugates and so the corresponding factors of (5), $G_p(\theta^{2\nu+1})$ and $G_p(\theta^{2\lambda+1})$, have a positive product to contribute to (5) as long as ν and λ are distinct. If they are equal, their value is $(p-3)/4$, which can happen only when $p \equiv -1 \pmod 4$. It remains to consider this case in which $\theta^{2\nu+1} = -1$. To prove the lemma it suffices, then, to show that $G_p(-1)$ is positive. In fact, more is true, namely if $p \equiv 3 \pmod 4$

$$G_p(-1) = ph, \tag{7}$$

where h denotes the class number of the imaginary quadratic field $K(\sqrt{-p})$. We have only to note that

$$G_p(-1) = \sum_{n=0}^{p-2} g_n(-1)^{p-n-2} = -\sum_{\nu=1}^{p-1} \nu\left(\frac{\nu}{p}\right),$$

since the g's with even subscripts are the quadratic residues of p. But it is well known that (see, for example, [3, p. 344, formula (4.3)])

$$\sum_{\nu=1}^{p-1} \nu\left(\frac{\nu}{p}\right) = -ph$$

so (7) follows and the lemma is proved. This also gives a simple proof of the following well-known [6]

COROLLARY. *If $p \equiv 3 \pmod 4$, then $h^*(p)$ is divisible by h.*

3. First Factorization Theorem.

THEOREM 1. *Let p be an odd prime and let $p - 1 = 2^\lambda \omega$ where ω is odd. Then the right-hand member of*

$$(2p)^{(p-3)/2} h^*(p) = (-1)^{(p-1)/2} \prod_{d \mid \omega} Q^*_{2^\lambda d}(G_p) \tag{8}$$

is a factorization into rational integers.

Proof. The degree of $\Omega_{p-1}(x)$ is seen to be $(p-1)/2$ while that of $G_p(x)$ is $p - 2$. The right-hand side of (5) is the product of $G_p(x)$ taken over the roots of $\Omega_{p-1}(x)$ and is thus the resultant

$$\begin{aligned} R(G_p, \Omega_{p-1}) &= (-1)^{(p-2)(p-1)/2} R(\Omega_{p-1}, G_p) \\ &= (-1)^{(p-1)/2} \prod_{i=1}^{p-2} \Omega_{p-1}(\alpha_i) \quad (G_p(\alpha_i) = 0) \\ &= (-1)^{(p-1)/2} \prod_{d \mid \omega} Q^*_{2^\lambda d}(G_p) \end{aligned}$$

by Lemma 1. Since G_p is monic with integer coefficients the Q^*'s are integers.

This theorem allows us to "divide and conquer" the problem of factoring $h^*(p)$ by considering separately the prime factors of the Q^*'s.

4. Second Factorization Theorem. Of course, the product on the right of (8) must contain at least $(p-3)/2$ factors 2 and p, and we show in Section 5 how these can be removed automatically in obtaining a more efficient variant of (8). Other prime factors of $Q^*_{2^\lambda d}(G_p)$ may divide d and are called *intrinsic* factors and are discussed in Sections 8 and 9. They are easily discovered and removed. The remaining prime factors of $Q^*_{2^\lambda d}$ are called *characteristic*. To facilitate their discovery we use the following lemma.

LEMMA 3. *Let π^k be the highest power of a characteristic prime π dividing $Q^*_n(p)$. Let μ be the least positive exponent for which $\pi^\mu \equiv 1 \pmod n$. Then $\mu \mid k$.*

Proof. A proof of this fundamental result from the theory of Pierce functions is found in [1].

THEOREM 2. *Let $P_d = q_1 q_2 \cdots q_t$ be the product of all the characteristic factors of $Q^*_{2^\lambda d}(G_p)$ into distinct powers of odd primes. Then*

$$q_i \equiv 1 \pmod{2^\lambda d} \qquad (i = 1(1)t).$$

Proof. Using Lemma 3 with $\pi^k = q_i$, $n = 2^\lambda d$, $P = G_p$ and writing $k = \mu j$, we have at once

$$q_i = \pi^k = (\pi^\mu)^j \equiv 1^j = 1 \pmod{2^\lambda d}.$$

To search for the prime factors of P_d, we therefore try as divisors of P_d only the numbers in the arithmetic progression $2^\lambda dx + 1$ ($x = 1, 2, 3, \ldots$). The first such divisor is either a prime or a power of a prime. After removing all such factors below some limit, an attempt can be made to represent the cofactor as $a^2 - b^2$. In this case a is restricted to one case modulo $2^{2\lambda-1}d^2$.

5. Simplification of Character Sums. We now develop a practical method of computing an isolated value of $Q^*_{2^\lambda d}(G_p)$. This involves four lemmas and the following notation.

p is an odd prime.
g is a primitive root of p.
$p - 1 = ef$ where f is odd.
$\tau = e/(e, \operatorname{ind}_g 2)$.
$\alpha = \exp\{2\pi i/e\}$.
$\chi(k) = \chi_e(k) = \alpha^{\operatorname{ind}_g k}$ $(\chi_e(0) = 0)$.
$M_e(p) = \sum_{k=1}^{p-1} k\chi_e(k)$.
$m_e(p) = \sum_{k=1}^{(p-1)/2} \chi_e(k)$.

LEMMA 4. *Let r be any integer and let $(r, e) = \delta$ so that $e = \delta e_1$. Then*

$$\prod_{t \leqslant e;(t,e)=1} \{x - \exp(2\pi irt/e)\} = \{Q_{e_1}(x)\}^{\phi(e)/\phi(e_1)}, \tag{9}$$

where $\phi(n)$ is Euler's totient function.

Proof. The left member of (9) is a polynomial $\psi(x)$ of degree $\phi(e)$ which is monic and has for roots all the primitive e_1th roots of unity each with the same multiplicity ν, say. That is, $\psi(x) = \{Q_{e_1}(x)\}^\nu$. Taking the degrees of both sides of this identity, we have $\phi(e) = \nu\phi(e_1)$, which proves the lemma.

LEMMA 5. *The norm of $2 - \chi(2)$ in the cyclotomic field of the eth roots of unity is*

$$N_e(2 - \chi_e(2)) = \{Q_\tau(2)\}^{\phi(e)/\phi(\tau)}.$$

Proof. Set $r = \operatorname{ind}_g 2$ and $x = 2$ in Lemma 4.

LEMMA 6. $\{2 - \chi_e(2)\}M_e(p) = -pm_e(p)$.

Proof. First we note that $\chi_e(-1) = -1$. In fact

$$\chi_e(-1) = \chi_e(p-1) = \alpha^{\operatorname{ind}(p-1)} = \alpha^{(p-1)/2} = \exp\{\pi i(p-1)/e\} = (-1)^f = -1.$$

Now let M' denote the half sum

$$M' = M'_e(p) = \sum_{k<p/2} k\chi_e(k).$$

Then

$$M_e(p) - M' = \sum_{r<p/2} (p-r)\chi_e(p-r)$$

$$= p\chi_e(-1)m_e(p) - \chi_e(-1)M'.$$

Hence

$$M_e(p) = -pm_e(p) + 2M'. \tag{10}$$

On the other hand,

$$M_e(p) = \sum_{k<p/2} \{2k\chi_e(2k) + (2k+1)\chi_e(2k+1)\}$$

$$= 2\chi_e(2)M' + \sum_{k<p/2} (p-2k)\chi_e(p-2k)$$

or

$$\chi_e(2)M_e(p) = 4M' - pm_e(p). \tag{11}$$

Multiplying (10) by 2 and subtracting from (11) gives the lemma.

THEOREM 3.

$$Q_e^*(G_p) = (-1)^{\phi(e)} p^{\phi(e)} N_e(m_e(p))/\{Q_\tau(2)\}^{\phi(e)/\phi(\tau)}. \tag{12}$$

Proof. By definition (3), we have

$$Q_e^* = Q_e^*(G_p) = (-1)^{\phi(e)} R(G_p, Q_e) = (-1)^{\phi(e)} \prod_{t\leqslant e;(t,e)=1} G_p(\alpha^t)$$

$$= (-1)^{\phi(e)} \prod_{t\leqslant e;(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{t(p-n-2)}$$

$$= (-1)^{\phi(e)} \prod_{t\leqslant e;(t,e)=1} \alpha^{t(p-2)} \prod_{t\leqslant e;(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{-tn}$$

$$= \prod_{t\leqslant e;(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{tn} = \prod_{t\leqslant e;(t,e)=1} \sum_{k=1}^{p-1} k\chi_e(k).$$

That is, $Q_e^*(G_p) = N_e(M_e(p))$. By Lemmas 5 and 6 we have the theorem.

We now define a new exponential sum $W_e(p)$ by

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

$$\text{where } \epsilon_n = \begin{cases} 1 & \text{if } g_n < p/2, \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

Thus the coefficients of W_e are ± 1 or 0.

LEMMA 7. $(1-\alpha)m_e(p) = 2W_e(p, 1)$.

Proof. For typographic simplicity, we write p' for $(p-1)/2$. Since

$$\alpha^{p'} = (\alpha^{e/2})^f = (-1)^f = -1$$

and we have $g_{n+p'} \equiv g^{p'} g_n \equiv -g_n \pmod p$, then $g_{n+p'} = p - g_n$ so that $\epsilon_{p'+n} = 1 - \epsilon_n$. In what follows the summation index ν ranges over $0 \leqslant \nu \leqslant (p-3)/2$. From the above we can write

$$m_e(p) = \sum_{k=1}^{p'} \alpha^{\operatorname{ind} g^k} = \sum_{r=0}^{p-2} \epsilon_r \alpha^r = \sum \{\epsilon_\nu \alpha^\nu + \epsilon_{p'+\nu} \alpha^{p'+\nu}\}$$

$$= \sum \epsilon_\nu \alpha^\nu - \sum (1-\epsilon_\nu)\alpha^\nu = 2\sum \epsilon_\nu \alpha^\nu - \sum \alpha^\nu$$

$$= 2\{\sum \epsilon_\nu \alpha^\nu - 1/(1-\alpha)\}.$$

Multiplying by $(1-\alpha)$, we have

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

since $\epsilon_{p'} = 0$. From this the lemma follows.

LEMMA 8. $N_e(m_e(p)) = N(W_e(p, 1))2^{J(e)}$ *where*

$$J(e) = \begin{cases} \phi(e) & \text{if } e \neq 2^k \\ & (k \geqslant 1). \\ \phi(e) - 1 & \text{if } e = 2^k \end{cases}$$

Proof. This follows at once by taking norms of both sides in Lemma 7. Use is made of a theorem of Lebesgue [4] in writing

$$\prod_{(t,e)=1} (1-\alpha^t) = Q_e(1) = 2 \quad \text{or} \quad 1$$

according as e is a power of an (even) prime or not.

6. Main Theorem. We are now prepared to give a formula for the class number $h^*(p)$ as a product of norms of exponential sums of the type $W_e(p)$, divided by certain cyclotomic polynomials evaluated at the point 2. In stating the result there is some recapitulation of notation.

THEOREM 4. *Let p be an odd prime with g any primitive root. Let e range over all divisiors of $p-1$ whose codivisors are odd. Let*

$$\tau = \tau(e) = e/(e, \operatorname{ind}_g 2),$$

and let $h_e(p) = p^{[e/(p-1)]} N_e(W_e(p))/\{Q_{\tau(e)}(2)\}^\gamma$, where

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

Then

$$h^*(p) = \prod_e h_e(p). \tag{14}$$

Proof. This follows at once from putting together Theorem 1, Theorem 3, and Lemma 8, using $e = 2^\lambda d$, $\tau = \tau(d)$, and the fact that

$$\sum_{d|\omega} \phi(2^\lambda d) = \frac{p-1}{2}.$$

At first sight, it would appear from (14) that $h^*(p)$ is always divisible by p. Of course, this is not so. The explanation is that p divides the denominator, $Q_{\tau(\omega)}(2)$. To see this we note [5] that

$$\tau(\omega) = (p-1)/((p-1), \text{ind } 2)$$

is the exponent or order of 2 modulo p. Hence p is a divisor of $Q_{\tau(\omega)}(2)$. Otherwise, it is the responsibility of the numerator N of each factor to be divisible by the denominator Q^γ. This affords an excellent check on calculation of N.

To illustrate Theorem 4 we give the simple example of $p = 31$. Here we have $g = 3$, $\lambda = 1$, $\omega = 15$, $\text{ind}_3 2 = 24$. The various elements in each factor may be tabulated thus.

e	$\tau(e)$	$\gamma(e)$	$\{Q_\tau(2)\}^\gamma$	$N_e(W)$
2	1	1	1	3
6	1	2	1	3
10	5	1	31	31
30	5	2	31^2	31

Hence

$$h^*(31) = 31 \cdot 3 \cdot 3 \cdot \frac{31}{31} \cdot \frac{31}{31^2} = 9.$$

7. **Simple Special Cases.** When the greatest common divisor $(2^\lambda d, \text{ ind } 2) = \delta$, is specified, the parameters τ and γ can be tabulated as follows. Here we have written e for $2^\lambda d$ and q is an odd prime.

δ	τ	γ
1	e	1
2	$e/2$	$\begin{cases} 1 & \text{if } 2 \parallel e \\ 2 & \text{otherwise} \end{cases}$
4	$e/4$	$\begin{cases} 2 & \text{if } 4 \parallel e \\ 4 & \text{otherwise} \end{cases}$
q	e/q	$\begin{cases} q-1 & \text{if } q \parallel e \\ q & \text{otherwise} \end{cases}$
$2q$	$e/(2q)$	$\begin{cases} 2 & \text{if } 2 \parallel e,\ q \parallel e \\ q & \text{if } 2 \parallel e,\ q^2 \mid e \\ 2q-2 & \text{if } 4 \mid e,\ q \parallel e \\ 2q & \text{otherwise} \end{cases}$

The case where p is a Fermat prime results in (14) having but a single factor. Setting $p = 2^{2^\nu} + 1$, we find $q = 3$, $\lambda = 2^\nu$, $\omega = 1$, $e = 2^{2^\nu}$, so $\tau(e) = 2^{\nu+1}$, $\gamma(e) = 2^{2^\nu-\nu-1}$, $Q_\tau(2) = 2^{2^\nu} + 1 = p$. For example, for $p = 257$ we have $\nu = 3$ so $\gamma(e) = 16$. This means that $N_{256}(W_{256}(257))$ must be divisible by 257^{15} and since 257 is an irregular prime, we can expect 257^{16}. In fact,

$$h^*(257) = 257 \cdot 20738946049 \cdot$$
$$1022997744563911961561298698183419037149697$$

a factorization into primes.

This alarmingly large value of γ is unusual for primes p in general. Ordinarily, γ rarely exceeds 2 and the denominator Q^γ is very small compared with the numerator $N(W)$ in (14).

8. Odd Intrinsic Factors of $h_e(p)$. For those odd primes q which divide both e and $h_e(p)$ there is a "law of repetition", namely

THEOREM 5. *Let $p - 1 = ef$ where f is odd. Let q be a prime factor of f. Then $h_{eq}(p)$ is divisible by q if and only if $h_e(p)$ is divisible by q.*

Proof. By (12) and (8) it suffices to prove the same fact about Q^*_{eq} and Q^*_e. Now

$$Q^*_{eq} = N_{eq}(M_{eq}(p)) = \prod_{(t,eq)=1;t<eq} \sum_{n=1}^{q-1} g_n \alpha_1^{tn}$$

where we have set $\alpha_1 = \exp\{2\pi i/(eq)\}$ so that $\alpha_1^q = \alpha$. If we use the multinomial theorem identity

$$(x_1 + x_2 + \cdots + x_{p-1})^q = x_1^q + x_2^q + \cdots + x_{p-1}^q + qF(x_1, \ldots, x_{p-1}),$$

we have

$$(Q^*_{eq})^q = \prod_{(t,eq)=1} \sum_{n=1}^{q-1} g_n^q \alpha^{tn} + q\Phi,$$

where Φ is a symmetric polynomial in the powers of α_1 with integer coefficients. Thus we have

$$Q^*_{eq} \equiv \left\{ \prod_{t\leqslant e;(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{tn} \right\}^{\phi(eq)/\phi(e)} \pmod q$$

or

$$Q^*_{eq} \equiv (Q^*_e)^\theta \pmod q,$$

where

$$\theta = \begin{cases} 1 & \text{if } q \mid e, \\ q - 1 & \text{otherwise.} \end{cases}$$

Thus $q | Q^*_{eq}$ if and only if $q | Q^*_e$. This proves the theorem.

Example. Take $p = 379, p - 1 = 2 \cdot 3^3 \cdot 7$. Here $3|h_2 = 3$. Hence $3|h_6 = 3 \cdot 13, 3|h_{18} = 3 \cdot 991$ and $3|h_{54} = 3 \cdot 29997973$. This theorem includes a theorem of Metsänkylä [6] for $e = 2^\lambda$.

9. The Intrinsic Factor 2. It is well known that for $p \equiv 3 \pmod 4$, $h_2(p)$ is always odd. For $e \neq 2$, however, $h_e(p)$ can be even, as witness

$$h_{28}(29) = 8, \quad h_6(163) = 4, \quad h_{14}(491) = 2^6 \cdot 29.$$

Newman [8] conjectured and Metsänkylä [6] proved that if h_p^* is even it is a multiple of 4. The latter's results show that when $e = 2^\lambda$, $h_e(p)$ is odd and that when $e = 2^\lambda d$ with $d > 1$ then the highest power of 2 dividing $h_e(p)$ is $2^{j\nu}$ where ν is the exponent of 2 (mod d) and $j \geqslant 0$. Since $\nu \geqslant 2$, Newman's conjecture follows at once. That j can be greater than 1 is evidenced by

$$h_{62}(311) = 2^{10} \cdot 9918966461,$$

whereas the exponent of 2 (mod 31) is 5. Since

$$2^{j\nu} \equiv 1 \pmod d,$$

the factor $2^{j\nu}$ of $h_e(p)$ behaves somewhat like a characteristic prime power factor of $h_e(p)$, being of the form $dx + 1$ rather than $2^\lambda dx + 1$.

10. Application. The preceding results have been used to obtain the prime factorization of $h^*(p)$ in the published tables of Newman [8] ($p < 200$) and Schrutka [7] ($p \leqslant 257$) and in the as yet unpublished table of Lehmer and Masley [9] ($p < 512$). Computational methods and results will appear in [9].

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

1. E. KUMMER, "Bestimmung der Anzahl nicht äquivalenter Classen für die aus λ ten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben," *J. Reine Angew. Math.*, v. 40, 1850, pp. 43–116 (p. 110, formula 38).

2. D. H. LEHMER, "Factorization of certain cyclotomic functions," *Ann. of Math.* (2) v. 34, 1933, pp. 461–479 (p. 463, Theorem 3).

3. Z. I. BOREVICH (BOREVIČ) & I. R. SHAFAREVICH (ŠAFAREVIČ), *Number Theory*, "Nauka", Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR **30** #1080; **33** #4001.

4. V. A. LEBESGUE, "Dimostrazione dell'irreduttibilitá dell'equazione formata con le radici primitive dell'unitá," *Ann. Mat. Pura Appl.*, v. 2, 1859, pp. 232–237.

5. W. J. LEVEQUE, *Topics in Number Theory*, Vol. 1, Addison-Wesley, Reading, Mass., 1956, p. 48 (Theorem 4.1). MR **18**, 283.

6. T. METSÄNKYLÄ, "On prime factors of the relative class numbers of cyclotomic fields," *Ann. Univ. Turku. Ser. A I*, No. 149, 1971, 8 pp. MR **44** #178.

7. G. SCHRUTKA V. RECHTENSTAMM, "Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, deren ϕ-Funktion des Wurzelexponenten (Grad) nicht grösser als 256 ist," *Abh. Deutsch. Akad. Wiss. Berlin Kl. Math. Phys. Tech.*, 1964, no. 2, 64 pp. MR **29** #4918.

8. M. NEWMAN, "A table of the first factor for prime cyclotomic fields," *Math. Comp.*, v. 24, 1970, pp. 215–219. MR **41** #1684.

9. D. H. LEHMER & J. M. MASLEY, "Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 512$." (To appear.)