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 \( p \)-th 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 \( g^n \equiv g_n \pmod{p} \) \((0 < g_n < p) \) \((0 \leq n < p - 1)\). Denote by \( F = F_p \) the polynomial

\[
F_p(x) = \sum_{n=0}^{p-2} g_n x^n.
\]

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 \[3, p. 358, formula (5.6)\]

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

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 \( M = 2^\omega \omega, \omega \) odd, be any positive integer and let \( Q_k(x) \) be the cyclotomic polynomial whose roots are the primitive \( k \)-th 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. \( \Omega_M(x) = \prod_{d \mid M} Q_d(x) \).

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
\Omega_M(x) = \prod_{n=1, M \, \text{odd}}^{M} (x - \rho^n) = \prod_{\delta \mid M} \prod_{\omega \mid (\mathbb{Z}/\delta) = 1} (x - \rho^{\delta\omega}) = \prod_{\delta \mid M} Q_M(\delta)(x).

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

\[
Q_k^*(P) = \prod_{i=1}^{r} Q_k(\beta_i),
\]

where \( \beta_i \) 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

\[
G_p(x) = \sum_{n=0}^{p-2} g_n x^{p-n-2}.
\]

Then

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

**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

\[
\lambda = (p-3)/2 - \nu.
\]

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 \( \lambda \) 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 \( \nu \) and \( \lambda \) are distinct. If they are equal, their value is \( (p-3)/4 \), which can happen only when \( p \equiv -1 \) (mod 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 \( p \equiv 3 \) (mod 4)

\[
G_p(-1) = ph,
\]

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

\[
G_p(-1) = \sum_{n=0}^{p-2} g_n(-1)^{p-n-2} = - \sum_{\nu=1}^{p-1} \frac{\nu^{(p-1)/p}}{p},
\]
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 follow-
ing 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 $\omega$ is odd. Then
the right-hand member of

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

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

$$R(G_p, \Omega_{p-1}) = (-1)^{(p-2)(p-1)/2} R(\Omega_{p-1}, G_p)$$

$$= (-1)^{(p-1)/2} \prod_{i=1}^{p-2} \Omega_{p-1}(\alpha_i) \quad (G_p(\alpha_i) = 0)$$

$$= (-1)^{(p-1)/2} \prod_{d \mid \omega} Q_{2^\lambda d}^*(G_p)$$

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 dis-
cussed 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 $\pi^k$ be the highest power of a characteristic prime $\pi$ dividing
$Q_n^*(p)$. Let $\mu$ be the least positive exponent for which $\pi^\mu \equiv 1 \pmod{n}$. Then $\mu | k$.

**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

$$q_i \equiv 1 \pmod{2^\lambda d} \quad (i = 1(1)t).$$
Proof. Using Lemma 3 with $\pi^k = q_l$, $n = 2^k d$, $P = G_p$ and writing $k = \mu j$, we have at once

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

To search for the prime factors of $P_d$, we therefore try as divisors of $P_d$ only the numbers in the arithmetic progression $2^k dx + 1$ ($x = 1, 2, 3, \ldots$). 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.
- $\tau = e/(\phi(e), g, 2)$.
- $\alpha = \exp\{2\pi i/e\}$.
- $\chi(k) = \chi_e(k) = \alpha^{\text{ind}_e k} \quad (\chi_e(0) = 0)$.
- $M_e(p) = \sum_{k=1}^{p-1} k\chi_e(k)$.
- $m_e(p) = \sum_{k=1}^{(p-1)/2} \chi_e(k)$.

Lemma 4. Let $r$ be any integer and let $(r, e) = 1$ so that $e = \delta e_1$. Then

$$(9) \quad \prod_{1 \leq r \leq e : (r, e) = 1} \{x - \exp(2\pi i rt/e)\} = (Q_{e_1}(x))\phi(e)/\phi(e_1),$$

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 $e_1$th roots of unity each with the same multiplicity $\nu$, 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 $e$th roots of unity is

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

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

Lemma 6. $2 - \chi_e(2); M_e(p) = -p m_e(p)$.

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

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

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
\[ (10) \quad M_e(p) = -p m_e(p) + 2 M'. \]

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
\[ (11) \quad \chi_e(2) M_e(p) = 4 M' - p m_e(p). \]

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

**Theorem 3.**
\[ (12) \quad Q_e^*(G_p) = (-1)^\phi(e) p^{\phi(e)} N_e(m_e(p))/\phi(e)/\phi(r). \]

**Proof.** By definition (3), we have
\[ Q_e^*(G_p) = Q_e^*(G_p) = (-1)^\phi(e) R(G_p, Q_e) = (-1)^\phi(e) \prod_{r < e: (t, e) = 1} G_p(\alpha^r) \]
\[ = (-1)^\phi(e) \prod_{t < e: (t, e) = 1} \sum_{n=1}^{p-1} g_n \alpha^{(p-n-2)} \]
\[ = (-1)^\phi(e) \prod_{t < e: (t, e) = 1} \alpha^{(p-2)} \prod_{n=1}^{p-1} g_n \alpha^{-tn} \]
\[ = \prod_{t < e: (t, e) = 1} \sum_{n=1}^{p-1} g_n \alpha^{tn} = \prod_{r < e: (t, e) = 1} \sum_{k=1}^{p-1} k \chi_e(k). \]

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
\[ W_e(p) = W_e(p, t) = \sum_{n=1}^{(p-1)/2} (\epsilon_n - \epsilon_{n-1}) \alpha^{nt} \]
\[ (13) \quad \text{where } \epsilon_n = \begin{cases} 1 & \text{if } g_n < p/2, \\ 0 & \text{otherwise.} \end{cases} \]
Thus the coefficients of \( W_e \) are \( \pm 1 \) 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 \( g_{n+p'} = g_n \equiv -g_n \pmod{p} \), then \( g_{n+p'} = p - g_n \) so that \( \epsilon_{p'}g_n = 1 - \epsilon_n \). In what follows the summation index \( \nu \) ranges over \( 0 < \nu < (p - 3)/2 \). From the above we can write

\[
m_e(p) = \sum_{k=1}^{p'} \alpha^{\text{ind}_g k} = \sum_{r=0}^{p-2} \epsilon_r \alpha^r = \sum (\epsilon_r \alpha^r + \epsilon_{p'+\nu} \alpha^{p'+\nu})
\]

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

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

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

\[
J(e) = \begin{cases} 
\phi(e) & \text{if } e \neq 2^k \\
\phi(e) - 1 & \text{if } e = 2^k
\end{cases} \quad (k \geq 1).
\]

**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

\[
\prod_{(\tau, e) = 1} (1 - \alpha^\tau) = Q_\epsilon(1) = 2 \quad \text{or} \quad 1
\]

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 divisors of \( p - 1 \) whose codivisors are odd. Let

\[
\tau = \tau(e) = e/(\text{ind}_g 2),
\]

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
PRIME FACTORS OF CYCLOTOMIC CLASS NUMBERS

\[ h^*(p) = \prod_{e} h_e(p). \]

**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 \( Q' \). 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.

<table>
<thead>
<tr>
<th>( e )</th>
<th>( \tau(e) )</th>
<th>( \gamma(e) )</th>
<th>( (Q_{\tau(2)})^\gamma )</th>
<th>( N_e(W) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>1</td>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>30</td>
<td>5</td>
<td>2</td>
<td>31^2</td>
<td>31</td>
</tr>
</tbody>
</table>

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 \( \tau \) and \( \gamma \) can be tabulated as follows. Here we have written \( e \) for \( 2^\lambda d \) and \( q \) is an odd prime.

<table>
<thead>
<tr>
<th>( \delta )</th>
<th>( \tau )</th>
<th>( \gamma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( e )</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>( e/2 )</td>
<td>( \begin{cases} 1 &amp; \text{if } 2 \parallel e \ 2 &amp; \text{otherwise} \end{cases} )</td>
</tr>
<tr>
<td>4</td>
<td>( e/4 )</td>
<td>( \begin{cases} 2 &amp; \text{if } 4 \parallel e \ 4 &amp; \text{otherwise} \end{cases} )</td>
</tr>
<tr>
<td>( q )</td>
<td>( e/q )</td>
<td>( \begin{cases} q - 1 &amp; \text{if } q \parallel e \ q &amp; \text{otherwise} \end{cases} )</td>
</tr>
<tr>
<td>( 2q )</td>
<td>( e/(2q) )</td>
<td>( \begin{cases} 2q - 2 &amp; \text{if } 4 \parallel e, q \parallel e \ q &amp; \text{if } 2 \parallel e, q^2 \parallel e \end{cases} )</td>
</tr>
</tbody>
</table>
The case where $p$ is a Fermat prime results in (14) having but a single factor. Setting $p = 2^{2^v} + 1$, we find $q = 3, \lambda = 2^v, \omega = 1, e = 2^{2^v}, \tau(e) = 2^{2^v-\nu-1}, Q_e(2) = 2^{2^v} + 1 = p$. For example, for $p = 257$ we have $v = 3$ 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,

$$h^*(257) = 257\cdot20738946049\cdot1022997744563911961561298698183419037149697$$

a factorization into primes.

This alarmingly large value of $\gamma$ is unusual for primes $p$ in general. Ordinarily, $\gamma$ rarely exceeds 2 and the denominator $Q^7$ 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

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

we have

$$(Q_{eq}^*)^q = \prod_{(t,eq)=1} \sum_{n=1}^{q-1} g_n \alpha_1^{tn} + q\Phi,$$

where $\Phi$ is a symmetric polynomial in the powers of $\alpha_1$ with integer coefficients. Thus we have

$$Q_{eq}^* = \left\{ \prod_{t<e; (t,e)=1} \sum_{n=1}^{p-1} g_n \alpha_1^{tn}\right\}^{\phi(eq)/\phi(e)} \pmod{q}$$

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 $q \mid Q_{eq}^*$ if and only if $q \mid Q_e^*$. 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 \( 2^{\nu} \) where \( \nu \) is the exponent of 2 \pmod{d} and \( j \geq 0 \). Since \( \nu > 2 \), Newman's conjecture follows at once. That \( j \) can be greater than 1 is evidenced by

\[
h_{6^2}(311) = 2^{10} \cdot 991896461,
\]

whereas the exponent of 2 \pmod{31} is 5. Since

\[
2^{\nu} \equiv 1 \pmod{d},
\]

the factor \( 2^{\nu} \) 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] \((p < 257)\) 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

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