A congruence for the index of a unit
of a real abelian number field

by

KENNETH S. WILLIAMS* and KENNETH HARDY ** (Ottawa, Ont., Canada)

1. Introduction. Let $K$ be a real abelian extension of the rational number field $\mathbb{Q}$. As $K$ is abelian, by the Kronecker–Weber theorem, $K$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$, $n \equiv 2 \pmod{4}$. We let $\mathbb{Q}(\zeta_n)$ be the smallest such field containing $K$, so that $n$ is the conductor of $K$. The ring of integers of $\mathbb{Q}(\zeta_n)$ is

$$R = \left\{ \sum_{j=0}^{\varphi(n)-1} a_j \zeta_n^j : a_j \in \mathbb{Z}, \quad 0 \leq j \leq \varphi(n)-1 \right\},$$

where $\varphi$ denotes Euler’s totient function and $\mathbb{Z}$ denotes the domain of rational integers.

Now let $p$ be a prime $\equiv 1 \pmod{n}$, say, $p = nf+1$. Let $g$ be a fixed primitive root modulo $p$. The cyclotomic polynomial of index $n$ has $\varphi(n)$ distinct roots modulo $p$. One of these roots is $g^f$. Thus, by Kummer’s theorem, the ideal

$$P = pR + (\zeta_n - g^f)R$$

of $R$ is a prime ideal of norm $p$ which divides $pR$. Thus the canonical homomorphism

$$\lambda: R \to R/p \cong \mathbb{Z}/p\mathbb{Z}$$

maps $\zeta_n$ onto $g^f \pmod{p}$. We have thus shown that for any given primitive root $g \pmod{p}$ there is a unique homomorphism $\lambda: R \to \mathbb{Z}/p\mathbb{Z}$ satisfying $\lambda(\zeta_n) \equiv g^f \pmod{p}$. This homomorphism is central to the rest of this paper.

For any integer $a$ not divisible by $p$, the least non-negative integer $b$ such that $a \equiv g^b \pmod{p}$ is called the index of $a$ with respect to $g$ and is denoted by $\text{ind} a$. (We re-emphasize that $g$ is regarded as fixed.) The purpose

* Research supported by Natural Sciences and Engineering Research Council Canada Grant A-7233.
** Research supported by Natural Sciences and Engineering Research Council Canada Grant A-8049.
of this paper is to obtain a congruence modulo a certain divisor of n for \( e = \text{ind} \lambda (e) \), where e is a unit of \( K \) (see Theorem 1).

Taking \( K \) to be the real quadratic field \( \mathbb{Q}((\sqrt{D}) \) of discriminant \( D \), we obtain, as a special case of Theorem 1, a congruence for \( \varepsilon_p = \lambda (e_p) \) modulo \( \text{GCD}(D, h_p) \), where \( e_p \) denotes the fundamental unit (\( > 1 \)) of \( \mathbb{Q}((\sqrt{D}) \) and \( h_p \) denotes the class number of \( \mathbb{Q}((\sqrt{D}) \) (see Theorem 2).

The congruences in Theorems 1 and 2 are given in terms of the cyclotomic numbers \( (h, k)_n \) of order \( n \), where for any integers \( h \) and \( k \) the cyclotomic number \( (h, k)_n \) is defined to be the number of solutions \( (r, s) \) of

\[
\begin{align*}
1 + g^{r+s} & \equiv g^{r+s}(\text{mod } p), \\
1 \leq r \leq f-1, \quad 1 \leq s \leq f-1.
\end{align*}
\]

The basic properties of cyclotomic numbers are given for example in [14].

Finally, as explicit expressions are known for the cyclotomic numbers of orders 8, 12, 5 (see [6], [16], [15] respectively), Theorem 2 can be applied to the real quadratic fields \( \mathbb{Q}((\sqrt{2}) \) (of conductor 8), \( \mathbb{Q}((\sqrt{3}) \) (of conductor 12), \( \mathbb{Q}((\sqrt{5}) \) (of conductor 5), to obtain explicit congruences for \( \text{ind} (1 + \sqrt{2}) \)(mod 8), \( \text{ind} (2 + \sqrt{3}) \)(mod 12), \( \text{ind} (\frac{1}{2}(1 + \sqrt{5})) \)(mod 5). This is done in Sections 4, 5 and 6 respectively. Theorem 2 can also be applied to \( \mathbb{Q}((\sqrt{6}) \) (of conductor 24) as the cyclotomic numbers of order 24 are known explicitly [5]. However, in this case the amount of elementary algebra needed to compute the right-hand side of Theorem 2 is extremely onerous so this was not done. For \( D \neq 5, 8, 12, 24 \) explicit expressions are not known for the cyclotomic numbers of order \( D \) and so are not available for use in Theorem 2.

For example for \( K = \mathbb{Q}((\sqrt{7}) \), we have \( D = 28 \), and although the cyclotomic numbers of orders 7 and 14 have been evaluated ([10], [11]) this is not the case for those of order 28.

2. Proof of Theorem 1. Let \( U(K) \) denote the group of units of \( K \) and let \( C(K) \) denote the group of cyclotomic units of \( K \). \( C(K) \) is a subgroup of \( U(K) \) of finite index and we set \( i(K) = [U(K) : C(K)] \). It is known that \( i(K) \) is related to the class number \( h(K) \) of \( K \) (see for example [13]).

Let \( \varepsilon \) be a unit of \( K \). Then we have \( \varepsilon^{i(K)} \in C(K) \), and so there exist integers \( a (= 0, 1), b (= 0, 1, \ldots, n-1), c_j \) and \( d_j (= 0, 1, \ldots, n-1), \)
\[
(1.1) \quad i^{i(K)} = (-1)^a c_b \prod_{j=1}^{k} (c_j^n - 1)^{d_j}.
\]

Applying the homomorphism \( \lambda : R \rightarrow \mathbb{Z}/p\mathbb{Z} \) to \( 1.1 \), we obtain

\[
(2.2) \quad \varepsilon^{i(K)} \equiv (-1)^a c_b \prod_{j=1}^{k} (g^{d_j} - 1)^{d_j}(\text{mod } p).
\]
Taking the index of both sides of the congruence (2.2), we obtain, as \( \text{ind}(-1) = n/2 \),

\[
(2.3) \quad i(K) \text{ind } \bar{e} = \frac{1}{2} na + bf + \sum_{j=1}^{k} c_j \text{ind}(g^{d_j}) - 1 \pmod{p-1}.
\]

Now by a result of Muskat ([12], p. 499), we have

\[
\text{ind}(g^{d_j} - 1) = \sum_{l=1}^{n-1} l(1, d)_n \pmod{n},
\]

so that

\[
i(K) \text{ind } \bar{e} = \frac{1}{2} na + bf + \sum_{j=1}^{k} c_j \sum_{l=1}^{n-1} l(1, d)_n \pmod{n}.
\]

We have thus proved the following congruence for \( \text{ind } \bar{e} \) modulo \( n/\text{GCD}(n, i(K)) \).

**Theorem 1.**

\[
\frac{i(K)}{\text{GCD}(n, i(K))} \text{ind } \bar{e} \equiv \left(\frac{1}{2} na + b f + \sum_{j=1}^{k} c_j \sum_{l=1}^{n-1} l(1, d)_n \right) \pmod{\text{GCD}(n, i(K))}.
\]

**3. Proof of Theorem 2.** We take \( K \) to be the real quadratic field \( \mathbb{Q}(\sqrt{D}) \) of discriminant \( D \). It is well-known that the conductor \( n \) of \( \mathbb{Q}(\sqrt{D}) \) is \( D \) and that \( i(\mathbb{Q}(\sqrt{D})) = h(\mathbb{Q}(\sqrt{D})) = h_D \). The character \( \chi_D \) of the field \( \mathbb{Q}(\sqrt{D}) \) is given by \( \chi_D(j) = \left(\frac{D}{j}\right) \), where \( \left(\frac{D}{j}\right) \) is the Kronecker symbol.

Dirichlet’s class number formula (see for example [4], p. 344) for \( h_D \) can be written in the form

\[
(3.1) \quad \varepsilon_D^h = \prod_{0 < j < D/2} (\sin \pi j/D)^{\chi_D(j)}.
\]

We note that there are \( \frac{1}{4} \varphi(D) \) values of \( j \) in the range \( 0 < j < D/2 \) for which \( \chi_D(j) = 1 \), and \( \frac{1}{4} \varphi(D) \) values for which \( \chi_D(j) = -1 \). The remaining values of \( j \), namely those for which \( \text{GCD}(j, D) > 1 \), are such that \( \chi_D(j) = 0 \). Replacing \( \sin \pi j/D \) by \( -\varepsilon_D^{-\pi j/D} (\zeta_D - 1)^{\chi_D(j)} \) in (3.1), we obtain

\[
(3.2) \quad \varepsilon_D^h = \zeta_D^{-\pi j/D^2} \prod_{0 < j < D/2} (\zeta_D - 1)^{\chi_D(j)},
\]

where

\[
(3.3) \quad \Sigma_D = \sum_{0 < j < D/2} j\chi_D(j).
\]

If \( D \equiv 0(\mod 4) \), it is easily shown that \( \Sigma_D \equiv 0(\mod 2) \) so that the exponent \( \Sigma_D/2 \) in (3.2) is an integer. If \( D \equiv 1(\mod 4) \), \( \Sigma_D \) can be either even or odd, so
in this case we write \( \zeta_{D}^{D/2} \) in (3.2) in the form
\[
(3.4) \quad \zeta_{D}^{D/2} = (\zeta_{D}^{1/2})^{D} = - (\zeta_{D}^{(D+1)/2})^{D} = (-1)^{\frac{D(D+1)}{2}} \zeta_{D}^{(D+1)/2}.
\]

Then (3.2) has the form (2.1) with
\[
(3.5) \quad n = D, \quad i(K) = h_{p}, \quad e = e_{p},
\]

\[
(3.6) \quad a = \begin{cases} 0, & \text{if } D \equiv 0 \pmod{4}, \\ \Sigma_{p}, & \text{if } D \equiv 1 \pmod{4}, \end{cases}
\]

\[
(3.7) \quad b = \begin{cases} \frac{1}{2} \Sigma_{p}, & \text{if } D \equiv 0 \pmod{4}, \\ \frac{1}{2} (D+1) \Sigma_{p}, & \text{if } D \equiv 1 \pmod{4}, \end{cases}
\]

\[
(3.8) \quad k = \begin{cases} D/2, & \text{if } D \equiv 0 \pmod{4}, \\ (D-1)/2, & \text{if } D \equiv 1 \pmod{4}, \end{cases}
\]

and for \( j = 1, 2, \ldots, k \)
\[
(3.9) \quad c_{j} = - \chi_{p}(j), \quad d_{j} = j.
\]

Appealing to Theorem 1 we obtain the following congruence for \( \text{ind} \, \zeta_{D} \) modulo \( D/\text{GCD}(D, h_{p}) \).

**Theorem 2.**
\[
\frac{h_{p}}{\text{GCD}(D, h_{p})} \text{ind} \, \zeta_{D} \equiv \sum_{0 < j < D/2} \chi_{D}(j) \left( \frac{1}{2}j - \sum_{l=1}^{D-1} \frac{1}{l} \right) \left( \text{mod} \frac{D}{\text{GCD}(D, h_{p})} \right).
\]

We remark that in Theorem 2 if we set
\[
(3.10) \quad e_{p} = \frac{1}{2} (T + U \sqrt{D}), \quad T \equiv U \pmod{2},
\]

then appealing to the result [1]; p. 319
\[
(3.11) \quad \sqrt{D} = \sum_{0 < r < D}^{D-1} \chi_{D}(r) \zeta_{D},
\]

we have
\[
(3.12) \quad \lambda(\sqrt{D}) \equiv \sum_{0 < r < D}^{D-1} \chi_{D}(r) g^{rf} \pmod{p},
\]

and
\[
(3.13) \quad \zeta_{D} \equiv \lambda(\epsilon_{p}) \equiv \frac{1}{2} (T + \frac{1}{2} U \sum_{0 < r < D}^{D-1} \chi_{D}(r) g^{rf}) \pmod{p}.
\]
The congruence for the index of a unit of $K$ is

4. $K = \mathbb{Q}(\sqrt{2})$. In this case $n = D = 8$, $v_D = 1 + \sqrt{2}$, $h_D = 1$, and for $k$ odd

$$\chi_D(k) = \left(\frac{8}{k}\right) = \left(\frac{2}{k}\right) \begin{cases} +1, & \text{if } k \equiv 1, 7 \pmod{8}, \\ -1, & \text{if } k \equiv 3, 5 \pmod{8}. \end{cases}$$

Let $p = 8f + 1$ be a prime with primitive root $g$. Interpreting $\sqrt{2} = \frac{1}{2} \sqrt{8}$ modulo $p$ as $\lambda(\sqrt{2}) \equiv \frac{1}{2} \lambda(\sqrt{8}) \equiv \frac{1}{2} (g^{f} - g^{3f} - g^{5f} + g^{7f})(\mod p)$, Theorem 2 gives

$$\text{(4.1)} \quad \text{ind}(1 + \sqrt{2}) \equiv -f + \sum_{l=1}^{7} l(\langle l, 3 \rangle - \langle l, 1 \rangle) \pmod{8}.$$ 

Next we define integers $x$ and $y$ by

$$\text{(4.2)} \quad \sum_{m=2}^{p-1} \exp \left\{ \frac{2\pi i}{4} (\text{ind } m + \text{ind } (1-m)) \right\} = -x + 2y \sqrt{-1}$$

and integers $a$ and $b$ by

$$\text{(4.3)} \quad \sum_{m=2}^{p-1} \exp \left\{ \frac{2\pi i}{8} (\text{ind } m + 3\text{ind } (1-m)) \right\} = -a + b \sqrt{-2}.$$

It is known (see for example [3]) that

$$\text{(4.4)} \quad p = x^2 + 4y^2, \quad x \equiv 1 \pmod{4},$$

$$\text{(4.5)} \quad p = a^2 + 2b^2, \quad a \equiv (-1)^{p-1}y^8 \pmod{4}.$$ 

Emma Lehmer ([6], pp. 115–117) has expressed the values of the cyclotomic numbers $\langle l, m \rangle$ in terms of $p$, $x$, $y$, $a$, and $b$. It should be noted that in order to make her formulae conform to the definitions of $x$, $y$, $a$, $b$ given in (4.2) and (4.3), it is necessary to change the sign of $a$ in her tables for the case $p \equiv 9 \pmod{16}$. Making use of her tables we obtain

$$\text{(4.6)} \quad 4 \sum_{l=1}^{7} l(\langle l, 3 \rangle - \langle l, 1 \rangle)$$

$$= \begin{cases} -1 + 3x + 4y - 2a - 2b, & \text{if } p \equiv 1 \pmod{16}, \text{ ind } 2 \equiv 0 \pmod{4}, \\ -1 - x + 4y + 2a - 2b, & \text{if } p \equiv 1 \pmod{16}, \text{ ind } 2 \equiv 2 \pmod{4}, \\ -1 + 3x + 12y + 2a + 2b, & \text{if } p \equiv 9 \pmod{16}, \text{ ind } 2 \equiv 0 \pmod{4}, \\ -1 - x - 4y - 2a + 2b, & \text{if } p \equiv 9 \pmod{16}, \text{ ind } 2 \equiv 2 \pmod{4}. \end{cases}$$
As
\[
\begin{align*}
    x &\equiv 4f + 1 \pmod{32}, & a &\equiv 4f + 1 \pmod{16}, \\
    y &\equiv 0 \pmod{4}, & b &\equiv 0 \pmod{4}, \\
    x &\equiv 4f + 25 \pmod{32}, & a &\equiv 12f + 5 \pmod{16}, \\
    y &\equiv 2 \pmod{4}, & b &\equiv 2 \pmod{4}, \\
    x &\equiv 4f + 17 \pmod{32}, & a &\equiv 12f + 7 \pmod{16}, \\
    y &\equiv 2 \pmod{4}, & b &\equiv 0 \pmod{4},
\end{align*}
\]

(4.7)

we obtain
\[
4 \sum_{i=1}^{7} l((l, 3)_n - (l, 1)_n) = \begin{cases}
    4f - 4y - 2b \pmod{32}, & \text{if } p \equiv 1 \pmod{16} \\
    16 + 4f + 4y + 2b \pmod{32}, & \text{if } p \equiv 9 \pmod{16}
\end{cases}
\]

(4.8)

and so by (4.1) we obtain
\[
\text{ind}(1 + \sqrt{2}) = \begin{cases}
    -y - \frac{1}{2}b \pmod{8}, & \text{if } p \equiv 1 \pmod{16} \\
    4 + y + \frac{1}{2}b \pmod{8}, & \text{if } p \equiv 9 \pmod{16}
\end{cases}
\]

(4.9)

We have thus proved

Theorem 3. Let \( p = 8f + 1 \) be a prime. Let \( g \) be a primitive root \( \pmod{p} \).

Define \( \sqrt{2} \) modulo \( p \) by
\[
2\sqrt{2} \equiv g^f - g^{3f} - g^{5f} + g^{7f} \pmod{p}.
\]

Let \((x, y)\) be the solution of
\[
p = x^2 + 4y^2, \quad x \equiv 1 \pmod{4},
\]
given by (4.2), and let \((a, b)\) be the solution of
\[
p = a^2 + 2b^2, \quad a \equiv (-1)^{(p-1)/8} \pmod{4},
\]
given by (4.3). Then we have
\[
\text{ind}(1 + \sqrt{2}) = \begin{cases}
    -y - \frac{1}{2}b \pmod{8}, & \text{if } p \equiv 1 \pmod{16} \\
    4 + y + \frac{1}{2}b \pmod{8}, & \text{if } p \equiv 9 \pmod{16}
\end{cases}
\]
A congruence for the index of a unit of $K$

A few values of $p, g, a, b, x, y$ are given in Table 1 to illustrate Theorem 3.

<table>
<thead>
<tr>
<th>$p = 1 \pmod{8}$</th>
<th>$p \pmod{16}$</th>
<th>$g$</th>
<th>$x$</th>
<th>$y$</th>
<th>$a$</th>
<th>$b$</th>
<th>$\text{ind}(1 + \sqrt{2}) \pmod{8}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p &lt; 500$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$-y - \frac{1}{2}b \pmod{8}$</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>-3</td>
<td>2</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>41</td>
<td>9</td>
<td>6</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>-4</td>
<td>4</td>
</tr>
<tr>
<td>73</td>
<td>5</td>
<td>-3</td>
<td>4</td>
<td>-1</td>
<td>-6</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>89</td>
<td>9</td>
<td>3</td>
<td>5</td>
<td>-9</td>
<td>-2</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>97</td>
<td>1</td>
<td>5</td>
<td>-2</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>113</td>
<td>1</td>
<td>3</td>
<td>-7</td>
<td>9</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>137</td>
<td>9</td>
<td>3</td>
<td>-11</td>
<td>3</td>
<td>8</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>193</td>
<td>1</td>
<td>5</td>
<td>-7</td>
<td>6</td>
<td>-11</td>
<td>-6</td>
<td>5</td>
</tr>
<tr>
<td>233</td>
<td>9</td>
<td>3</td>
<td>13</td>
<td>-4</td>
<td>15</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>241</td>
<td>1</td>
<td>7</td>
<td>-15</td>
<td>2</td>
<td>13</td>
<td>-6</td>
<td>1</td>
</tr>
<tr>
<td>257</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>8</td>
<td>-15</td>
<td>-4</td>
<td>2</td>
</tr>
<tr>
<td>281</td>
<td>9</td>
<td>3</td>
<td>5</td>
<td>-8</td>
<td>-9</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>313</td>
<td>9</td>
<td>10</td>
<td>13</td>
<td>-6</td>
<td>-5</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>337</td>
<td>1</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>-7</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>353</td>
<td>1</td>
<td>3</td>
<td>17</td>
<td>4</td>
<td>-15</td>
<td>-8</td>
<td>0</td>
</tr>
<tr>
<td>401</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>-10</td>
<td>-3</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>409</td>
<td>9</td>
<td>21</td>
<td>-3</td>
<td>10</td>
<td>11</td>
<td>-12</td>
<td>0</td>
</tr>
<tr>
<td>433</td>
<td>1</td>
<td>5</td>
<td>17</td>
<td>-6</td>
<td>-19</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>449</td>
<td>1</td>
<td>3</td>
<td>-7</td>
<td>10</td>
<td>21</td>
<td>-2</td>
<td>7</td>
</tr>
<tr>
<td>457</td>
<td>9</td>
<td>13</td>
<td>21</td>
<td>2</td>
<td>-13</td>
<td>12</td>
<td>4</td>
</tr>
</tbody>
</table>

Remark 1. As $y \equiv 0 \pmod{2}$, by Theorem 3, we have

$$\text{ind}(1 + \sqrt{2}) \equiv 0 \pmod{2} \iff b \equiv 0 \pmod{4},$$

which is a result of Barrucand and Cohn [2]. From (4.7) we see that

$$y \equiv b + 2f \pmod{4},$$

so that (4.10) can also be formulated

$$\text{ind}(1 + \sqrt{2}) \equiv 0 \pmod{2} \iff y \equiv \frac{1}{2}(p - 1) \pmod{4}.$$

Remark 2. If $b \equiv 0 \pmod{4}$, by Theorem 3, we have

$$\text{ind}(1 + \sqrt{2}) \equiv 0 \pmod{4} \iff y + \frac{1}{2}b \equiv 0 \pmod{4}$$

$$\iff y \equiv \frac{1}{2}b \pmod{4}$$

$$\iff \frac{1}{2}b + 2f \equiv 0 \pmod{4},$$
that is
\[(4.13) \quad \text{ind}(1 + \sqrt{2}) \equiv 0 \pmod{4} \iff \frac{1}{2}b + f \equiv 0 \pmod{2},\]
which is Theorem 1 of [9].

**Remark 3.** By Theorem 3 we have
\[(4.14) \quad \text{ind}(1 + \sqrt{2}) \equiv 0 \pmod{8} \iff \begin{cases} y + \frac{1}{2}b \equiv 0 \pmod{8}, & \text{if } p \equiv 1 \pmod{16}, \\ y + \frac{1}{2}b \equiv 4 \pmod{8}, & \text{if } p \equiv 9 \pmod{16}. \end{cases}\]
The case \(p \equiv 1 \pmod{16}\) of (4.14) is Theorem 2 of [9].

5. \(K = \mathbb{Q}(\sqrt{3})\). In this case \(n = D = 12\), \(c_D = 2 + \sqrt{3}\), \(h_D = 1\), and for \(k\) satisfying \((k, 12) = 1\)
\[\chi_D(k) = \begin{pmatrix} 12 \\ k \end{pmatrix} = \begin{cases} +1, & \text{if } k \equiv 1, 11 \pmod{12}, \\ -1, & \text{if } k \equiv 5, 7 \pmod{12}. \end{cases}\]
Let \(p = 12f + 1\) be a prime with primitive root \(g\). Interpreting \(\sqrt{3} = \frac{1}{2}\sqrt{12}\) modulo \(p\) as \(\zeta(\sqrt{3}) = \frac{1}{2}\zeta(\sqrt{12}) \equiv \frac{1}{2}(g^f - g^{5f} - g^{7f} + g^{11f}) \pmod{p}\), Theorem 2 gives
\[(5.1) \quad \text{ind}(2 + \sqrt{3}) \equiv -2f + \sum_{l=1}^{11} l((l, 5)_{12} - (l, 1)_{12}) \pmod{12}.\]

Next we define integers \(x\) and \(y\) by
\[(5.2) \quad \sum_{m=2}^{p-1} \exp\left\{ \frac{2\pi i}{4} (\text{ind} m + \text{ind} (1 - m)) \right\} = -x + 2yi\]
and integers \(A\) and \(B\) by
\[(5.3) \quad \sum_{m=2}^{p-1} \exp\left\{ \frac{2\pi i}{6} (2\text{ind} m + \text{ind} (1 - m)) \right\} = -A + B\sqrt{-3}\]
(see for example [16], p. 61). It is known that
\[(5.4) \quad p = x^2 + 4y^2, \quad x \equiv 1 \pmod{4},\]
\[(5.5) \quad p = A^2 + 3B^2, \quad A \equiv 1 \pmod{6}.\]
Whiteman [16] has expressed the values of the cyclotomic numbers of order twelve in terms of \(p, A, B, x\) and \(y\). There are twenty-four different sets of formulae depending upon \(p \pmod{24}\), \(\text{ind} 2 \pmod{6}\), \(\text{ind} 3 \pmod{4}\), and the value of a certain quantity \(c\), whose precise definition is not needed in this paper ([16], eqn. (5.7), p. 64). Using these formulae we obtain the following
table of values for \[ 6 \sum_{l=1}^{11} l((l, 5)_{12}-(l, 1)_{12}): \]

<table>
<thead>
<tr>
<th>Case</th>
<th>[ 6 \sum_{l=1}^{11} l((l, 5)<em>{12}-(l, 1)</em>{12}) ] ( (\text{mod } 24) )</th>
<th>( p ) ( (\text{mod } 24) )</th>
<th>( c ) ( (\text{ind } 2 \text{ mod } 6) )</th>
<th>( \text{ind } 3 ) ( (\text{mod } 4) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(-2+8.4+9B-6x-8y)</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>(-2+2.4+3B-4y)</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>(-2+2.4+3B+4y)</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>(-2-4.4-3B+6x+8y)</td>
<td>1</td>
<td>-1</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>(-2+5.4+15B-3x-20y)</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>(-2-A+9B+3x-16y)</td>
<td>1</td>
<td>-1</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>(-2+8.4+9B+2x+12y)</td>
<td>1</td>
<td>( \text{i} )</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>(-2+2.4+3B+4x)</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>(-2+2.4+3B-4x)</td>
<td>1</td>
<td>( \text{i} )</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>(-2-4.4-3B-2x-12y)</td>
<td>1</td>
<td>-1</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>(-2+5.4+15B-x+24y)</td>
<td>1</td>
<td>( \text{i} )</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>(-2-A+9B+x+12y)</td>
<td>1</td>
<td>-1</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>(-2+11.4+15B-5x)</td>
<td>13</td>
<td>( \text{i} )</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>(-2+5.4-3B-7x-12y)</td>
<td>13</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>(-2+2.4+9B+4x)</td>
<td>13</td>
<td>( \text{i} )</td>
<td>3</td>
</tr>
<tr>
<td>16</td>
<td>(-2-4.4-9B+2x-12y)</td>
<td>13</td>
<td>-1</td>
<td>3</td>
</tr>
<tr>
<td>17</td>
<td>(-2+2.4+21B+4x)</td>
<td>13</td>
<td>( \text{i} )</td>
<td>5</td>
</tr>
<tr>
<td>18</td>
<td>(-2-4.4+3B+2x-12y)</td>
<td>13</td>
<td>-1</td>
<td>5</td>
</tr>
<tr>
<td>19</td>
<td>(-2+5.4-3B+3x+8y)</td>
<td>13</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>(-2+11.4+15B+9x+4y)</td>
<td>13</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>(-2-4.4-9B-6x+8y)</td>
<td>13</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>22</td>
<td>(-2+2.4+9B+4y)</td>
<td>13</td>
<td>-1</td>
<td>3</td>
</tr>
<tr>
<td>23</td>
<td>(-2-4.4+3B-6x+8y)</td>
<td>13</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>24</td>
<td>(-2+2.4+21B+4y)</td>
<td>13</td>
<td>-1</td>
<td>5</td>
</tr>
</tbody>
</table>

Treating the equations given by Whiteman for the cyclotomic numbers as congruences mod 16, we obtain

\[
A \equiv \begin{cases} 
  \frac{1}{2}(p+1)(\text{mod } 8), & \text{if } \ p \equiv 1 \text{ (mod } 24), \quad \text{ind } 3 \equiv 0 \text{ (mod } 4), \\
  \frac{1}{2}(p-3)(\text{mod } 8), & \text{if } \ p \equiv 1 \text{ (mod } 24), \quad \text{ind } 3 \equiv 2 \text{ (mod } 4), \\
  \frac{1}{2}(p+5)(\text{mod } 8), & \text{if } \ p \equiv 13 \text{ (mod } 24), \quad \text{ind } 3 \equiv 0 \text{ (mod } 4), \\
  \frac{1}{2}(p+1)(\text{mod } 8), & \text{if } \ p \equiv 13 \text{ (mod } 24), \quad \text{ind } 3 \equiv 2 \text{ (mod } 4),
\end{cases}
\]

\[
B \equiv \begin{cases} 
  0 \text{ (mod } 4), & \text{if } \ p \equiv 1 \text{ (mod } 24), \\
  2 \text{ (mod } 4), & \text{if } \ p \equiv 13 \text{ (mod } 24),
\end{cases}
\]

\[
x \equiv \begin{cases} 
  \frac{1}{2}(p+1)(\text{mod } 8), & \text{if } \ p \equiv 1 \text{ (mod } 24), \\
  \frac{1}{2}(p-3)(\text{mod } 8), & \text{if } \ p \equiv 13 \text{ (mod } 24),
\end{cases}
\]

\[
y \equiv \begin{cases} 
  0 \text{ (mod } 2), & \text{if } \ p \equiv 1 \text{ (mod } 24), \\
  1 \text{ (mod } 2), & \text{if } \ p \equiv 13 \text{ (mod } 24),
\end{cases}
\]
Similarly reducing the equations modulo 9 we obtain

\[
\begin{cases}
2p - 1 \pmod{9}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 2 \equiv 0 \pmod{6} \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 2 \equiv 3 \pmod{6},
\end{cases}
\]

\[A \equiv \begin{cases}
2p + 2 \pmod{9}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 2 \equiv 2, 4 \pmod{6} \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 2 \equiv 1, 5 \pmod{6},
\end{cases}\]

\[B \equiv - \text{ind } 2 \pmod{3},\]

\[
\begin{cases}
0 \pmod{3}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 3 \equiv 2 \pmod{4} \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 3 \equiv 0 \pmod{4},
\end{cases}
\]

\[x \equiv \begin{cases}
2p - 1 \pmod{9}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 3 \equiv 2 \pmod{4} \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 3 \equiv 2 \pmod{4}, \quad c = -1.
\end{cases}\]

\[
\begin{cases}
p - 2 \pmod{9}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 3 \equiv 0 \pmod{4}, \quad c = -1 \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 3 \equiv 2 \pmod{4}, \quad c = +1,
\end{cases}
\]

\[
\begin{cases}
0 \pmod{3}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 3 \equiv 0 \pmod{4} \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 3 \equiv 2 \pmod{4},
\end{cases}
\]

\[y \equiv \begin{cases}
2p + 2 \pmod{9}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 3 \equiv 2 \pmod{4}, \quad c = +i \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 3 \equiv 0 \pmod{4}, \quad c = -i,
\end{cases}\]

\[
\begin{cases}
p + 4 \pmod{9}, & \text{if } \quad p \equiv 1 \pmod{24}, \quad \text{ind } 3 \equiv 2 \pmod{4}, \quad c = -i \\
\quad \text{or} \quad \\
p \equiv 13 \pmod{24}, \quad \text{ind } 3 \equiv 0 \pmod{4}, \quad c = +i.
\end{cases}
\]

Appealing to (5.1), Table 2, and the congruences (5.6)-(5.13), we obtain congruences for \(\text{ind } (2 + \sqrt{3}) \pmod{8}\) and \(\text{mod } 9\) in each of the twenty-four cases. We just give the details in case 1 as the rest of the cases can be treated
similarly. By (5.1) and case 1 of Table 2 we have

\[(5.14)\quad 6\text{ind}(2 + \sqrt{3}) \equiv -12f - 2 + 8A + 9B - 6x - 8y \pmod{72}.\]

Reducing (5.14) modulo 8 we obtain, as \(f\) is even in this case,

\[-2\text{ind}(2 + \sqrt{3}) \equiv -2 + B + 2x \pmod{8}.\]

Appealing to (5.7) and (5.8) we obtain

\[-2 + B + 2x \equiv -B \pmod{8},\]

so that

\[(5.15)\quad \text{ind}(2 + \sqrt{3}) \equiv B/2 \pmod{4}.\]

Reducing (5.14) modulo 9, we obtain

\[-3\text{ind}(2 + \sqrt{3}) \equiv -3f - 2 - A + 3x + y \pmod{9}.\]

Appealing to (5.10) and (5.12) we obtain

\[-3f - 2 - A + 3x + y \equiv y \pmod{9},\]

so that

\[(5.16)\quad \text{ind}(2 + \sqrt{3}) \equiv -y/3 \pmod{3}.\]

Putting all the twenty-four cases together we obtain

**Theorem 4.** Let \(p = 12\alpha + 1\) be a prime. Let \(g\) be a primitive root \((\mod p)\). Define \(\sqrt{3}\) modulo \(p\) by

\[2\sqrt{3} \equiv g^f - g^{4f} - g^{7f} + g^{11f} \pmod{p}.\]

Let \((x, y)\) be the solution of

\[p = x^2 + 4y^2, \quad x \equiv 1 \pmod{4},\]

given by (5.2), and let \((A, B)\) be the solution of

\[p = A^2 + 3B^2, \quad A \equiv 1 \pmod{6},\]

given by (5.3). Then we have

\[(5.17)\quad \text{ind}(2 + \sqrt{3}) \equiv (-1)^{\text{ind}3/2 + f - 1} xy/3 \pmod{3}\]

and

\[(5.18)\quad \text{ind}(2 + \sqrt{3}) \equiv (-1)^{f(1 + \text{ind}3/2)} B/2 \pmod{4}.\]

A few values of \(p, g, A, B, x, y\) are given in Tables 3 and 4 to illustrate Theorem 4.
### Table 3

<table>
<thead>
<tr>
<th>$p = 1 \pmod{12}$</th>
<th>$p &lt; 500$</th>
<th>$f$ (mod 2)</th>
<th>$g$</th>
<th>$A$</th>
<th>$B$</th>
<th>$\text{ind} 3$ (mod 4)</th>
<th>$\text{ind}(2 + \sqrt{3})$ (mod 4)</th>
<th>$(-1)^{\frac{f(1 + \text{ind} 3) + B}{2}}$ (mod 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>1</td>
<td>2</td>
<td>+1</td>
<td>+2</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>1</td>
<td>2</td>
<td>−5</td>
<td>+2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>1</td>
<td>2</td>
<td>+7</td>
<td>+2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>0</td>
<td>5</td>
<td>−5</td>
<td>+4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>0</td>
<td>5</td>
<td>+7</td>
<td>−4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>1</td>
<td>6</td>
<td>+1</td>
<td>−6</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>157</td>
<td>1</td>
<td>5</td>
<td>+7</td>
<td>−6</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>181</td>
<td>1</td>
<td>2</td>
<td>+13</td>
<td>+2</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>193</td>
<td>0</td>
<td>5</td>
<td>+1</td>
<td>+8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>229</td>
<td>1</td>
<td>6</td>
<td>−11</td>
<td>−6</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>241</td>
<td>0</td>
<td>7</td>
<td>+8</td>
<td>+2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>1</td>
<td>5</td>
<td>+13</td>
<td>+6</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>313</td>
<td>0</td>
<td>10</td>
<td>−11</td>
<td>+8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>337</td>
<td>0</td>
<td>10</td>
<td>−17</td>
<td>−4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>1</td>
<td>2</td>
<td>+7</td>
<td>−10</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>373</td>
<td>1</td>
<td>2</td>
<td>+19</td>
<td>+2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>1</td>
<td>5</td>
<td>−17</td>
<td>+6</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>409</td>
<td>0</td>
<td>21</td>
<td>+19</td>
<td>−4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>421</td>
<td>1</td>
<td>2</td>
<td>−11</td>
<td>−10</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>433</td>
<td>0</td>
<td>5</td>
<td>+1</td>
<td>+12</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>457</td>
<td>0</td>
<td>13</td>
<td>−5</td>
<td>+12</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

### Table 4

<table>
<thead>
<tr>
<th>$p = 1 \pmod{12}$</th>
<th>$p &lt; 500$</th>
<th>$f$ (mod 2)</th>
<th>$g$ (mod 4)</th>
<th>$\text{ind} 3$ (mod 4)</th>
<th>$x$</th>
<th>$y$</th>
<th>$\text{ind}(2 + \sqrt{3})$ (mod 3)</th>
<th>$(-1)^{\text{ind} 3/2 + f^{-1} x y/3}$ (mod 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>−3</td>
<td>−1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>37</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>61</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>73</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>−3</td>
<td>−2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>97</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>9</td>
<td>−2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>109</td>
<td>1</td>
<td>6</td>
<td>0</td>
<td>−3</td>
<td>−5</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>157</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>−11</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>181</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>9</td>
<td>−5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>193</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>−7</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>229</td>
<td>1</td>
<td>6</td>
<td>0</td>
<td>−15</td>
<td>−1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>241</td>
<td>0</td>
<td>7</td>
<td>2</td>
<td>−15</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>277</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>9</td>
<td>−7</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>313</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>13</td>
<td>−6</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>337</td>
<td>0</td>
<td>10</td>
<td>2</td>
<td>9</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>349</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>−9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>373</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>−7</td>
<td>−9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>397</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>−19</td>
<td>−3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>409</td>
<td>0</td>
<td>21</td>
<td>2</td>
<td>−3</td>
<td>10</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>421</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>−15</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>433</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>17</td>
<td>−6</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>457</td>
<td>0</td>
<td>13</td>
<td>2</td>
<td>21</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Remark 1. If \( p \equiv 1 \pmod{24} \) (so that \( f \equiv 0 \pmod{2} \)) by Theorem 4 we have
\[
\text{ind}(2 + \sqrt{3}) \equiv 0 \pmod{4} \iff \frac{1}{2}B \equiv 0 \pmod{4} \iff B \equiv 0 \pmod{8},
\]
which is a result of Emma Lehmer ([9], Theorem 3).

Remark 2. Since
\[
2(2 + \sqrt{3}) = (1 + \sqrt{3})^2,
\]
the congruences in Theorem 4 give congruences for \( \text{ind}(1 + \sqrt{3}) \) modulo both 2 and 3.

Remark 3. From Theorem 4 we have
\[
\text{ind}(2 + \sqrt{3}) \equiv 0 \pmod{3} \iff \frac{x}{3} \equiv 0 \pmod{3}.
\]
If \( p \equiv 1 \pmod{24} \), \( \text{ind}3 \equiv 2 \pmod{4} \) or \( p \equiv 13 \pmod{24} \), \( \text{ind}3 \equiv 0 \pmod{4} \), by (5.12) and (5.13), we have \( x \equiv 0 \pmod{3} \), \( y \not\equiv 0 \pmod{3} \), so that (5.20) becomes in this case
\[
\text{ind}(2 + \sqrt{3}) \equiv 0 \pmod{3} \iff x \equiv 0 \pmod{9}.
\]
If \( p \equiv 1 \pmod{24} \), \( \text{ind}3 \equiv 0 \pmod{4} \) or \( p \equiv 13 \pmod{24} \), \( \text{ind}3 \equiv 2 \pmod{4} \), by (5.12) and (5.13), we have \( x \not\equiv 0 \pmod{3} \), \( y \equiv 0 \pmod{3} \), so that (5.20) becomes in this case
\[
\text{ind}(2 + \sqrt{3}) \equiv 0 \pmod{3} \iff y \equiv 0 \pmod{9}.
\]
Congruences (5.21) and (5.22) are due to Barrucand (see for example [8], p. 385).

6. \( K = \mathbb{Q}(\sqrt{5}) \). In this case \( n = D = 5 \), \( \epsilon_p = \frac{1}{2}(1 + \sqrt{5}) \), \( h_p = 1 \), and for \( k \) satisfying \( (k, 5) = 1 \)
\[
\chi_p(k) = \left( \frac{5}{k} \right) = \begin{cases} +1, & \text{if } k \equiv 1, 4 \pmod{5}, \\ -1, & \text{if } k \equiv 2, 3 \pmod{5}. \end{cases}
\]
Let \( p = 5f + 1 \) be a prime with primitive root \( g \). Interpreting \( \sqrt{5} \) modulo \( p \) as \( \lambda(\sqrt{5}) \equiv g^f - g^{2f} - g^{3f} + g^{4f} \pmod{p} \), Theorem 2 gives
\[
\text{ind}(\frac{1}{2}(1 + \sqrt{5})) \equiv \frac{-f}{2} + \sum_{i=1}^{4} l((l, 2)_5 -(l, 1)_5) \pmod{5}.
\]
Following Whiteman ([15], pp. 100–101), we may define integers \( x, u, v, w \) by
\[
\sum_{m=2}^{p-1} \beta^{	ext{ind}(m) + \text{ind}(1 - m)} = (-x + 2u + 4v + 5w)\beta + (-x + 4u - 2v - 5w)\beta^2 + \\
+ (-x - 4u + 2v - 5w)\beta^3 + (-x - 2u - 4v + 5w)\beta^4,
\]
where \( \beta = e^{2\pi i / 5} \), or equivalently by

\[
\begin{align*}
3x &= -p + 14 + 25(0,0)_5, \\
u &= (0,2)_5 - (0,3)_5, \\
v &= (0,1)_5 - (0,4)_5, \\
w &= (1,3)_5 - (1,2)_5.
\end{align*}
\]

(6.3)

The 4-tuple \((x,u,v,w)\) is a solution of Dickson's system

\[
\begin{align*}
16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \\
xw &= v^2 - 4uw - u^2.
\end{align*}
\]

(6.4)

Whiteman has given the cyclotomic numbers of order 5 in terms of \(p, x, u, v, w\) (see [15], (4.9)). Using these in (6.1) we obtain

\[
\text{ind}_{5/4}(1 + \sqrt[5]{5}) \equiv -u + 3v \pmod{5}.
\]

We have thus proved

**Theorem 5.** Let \( p = 5f + 1 \) be a prime. Let \( g \) be a primitive root \((\mod p)\). Define \( \sqrt[5]{5} \) modulo \( p \) by

\[
\sqrt[5]{5} \equiv g^f - g^{2f} - g^{3f} + g^{4f} \pmod{p}.
\]

<table>
<thead>
<tr>
<th>( p \equiv 1 \pmod{5} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p &lt; 500 )</td>
</tr>
<tr>
<td>( g )</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>31</td>
</tr>
<tr>
<td>41</td>
</tr>
<tr>
<td>61</td>
</tr>
<tr>
<td>71</td>
</tr>
<tr>
<td>101</td>
</tr>
<tr>
<td>131</td>
</tr>
<tr>
<td>151</td>
</tr>
<tr>
<td>181</td>
</tr>
<tr>
<td>191</td>
</tr>
<tr>
<td>211</td>
</tr>
<tr>
<td>241</td>
</tr>
<tr>
<td>251</td>
</tr>
<tr>
<td>271</td>
</tr>
<tr>
<td>281</td>
</tr>
<tr>
<td>311</td>
</tr>
<tr>
<td>331</td>
</tr>
<tr>
<td>401</td>
</tr>
<tr>
<td>421</td>
</tr>
<tr>
<td>431</td>
</tr>
<tr>
<td>461</td>
</tr>
<tr>
<td>491</td>
</tr>
</tbody>
</table>
Let \((x, u, v, w)\) be the solution of (6.4) given by (6.2) or equivalently by (6.3). Then we have

\[
\text{ind} 1/2(1 + \sqrt{5}) \equiv -u + 3v \pmod{5}.
\]

A few values of \(p, g, x, u, v, w\) are given in Table 5 to illustrate Theorem 5.

Remark 1. The congruence (6.5) can also be deduced from the theorem proved in [17].

Remark 2. From the second equation in (6.4), we have, as \(x \not\equiv 0 \pmod{5}\),

\[
u \equiv 3v \pmod{5} \iff w \equiv 0 \pmod{5}.
\]

Thus \(1/2(1 + \sqrt{5})\) is a fifth power \(\pmod{p}\) if and only if \(w \equiv 0 \pmod{5}\). This result is due to Emma Lehmer [7].

7. Acknowledgements. The authors would like to thank Control Data Canada Ltd. for providing the computer resources used in the preparation of this paper, and an unknown referee whose suggestions significantly improved the presentation of this paper.

References


DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA
K1S 5B6

Received on 10.5.1984
and in revised form on 25.10.1984 (1425)