Cyclic-Sixteen Class Fields for $\mathbb{Q}(-p)^{1/2}$ by Modular Arithmetic

By Harvey Cohn*

Abstract. Numerical experiments result in the construction of cyclic-sixteen class fields for $\mathbb{Q}(-p)^{1/2}$, $p$ prime < 2000, by radicals involving quadratic and biquadratic parameters. These fields are characterized by rational factorization properties modulo a variable prime; but it suffices to use only three primes selected and checked by computer to verify the class field, if earlier work (jointly with Cooke) on the cyclic-eight class field is utilized.

1. Introduction. To give a specific example of a new result in rational arithmetic, the current computation shows that a (large) prime $q$ satisfies $q = x^2 + 257y^2$ (in $\mathbb{Z}$) exactly when a certain equation over $\mathbb{Q}$ of degree 32 splits into 32 (different) linear factors modulo $q$. The general root of this equation is expressible (with “too many conjugates”) as $\Lambda_0^{1/2}$, where

$$\Lambda_0 = (-5 + 2(-257)^{1/2})(1 + (1 + 16i)^{1/2})$$
$$\cdot \left( \frac{-9 + (-257)^{1/2}}{1 - i} \right) \left( 16 + 257^{1/2} \right)^{1/2},$$

so that the radicals in $\Lambda_0$ must be chosen with correct signs. It will prove advantageous to replace a rather appalling equation of degree 32 by the following system of five quadratic congruences in which the signs are implicitly specified:

$$\begin{cases}
  x_1^2 \equiv -257, & x_2^2 \equiv -1, & x_3^2 \equiv 16 - x_1 x_2, \\
  x_4^2 \equiv (-9 + x_1)x_3/(1 - x_2), & \quad \pmod{q}.
\end{cases}$$

Now the system (1.2) is solvable for just those primes $q (> 13)$ which satisfy $q = x^2 + 257y^2$.

In terms of definitions given below, it will be clear that we are constructing cyclic-sixteen class fields of $k_2 = \mathbb{Q}(-p)^{1/2}$ for those primes $p$ for which $h$, the class number of $k_2$, is divisible by 16. In principle, this construction is finitary but not routine (see [1a]); and the generator $\Lambda_0$ is far from unique (in fact, another value is more convenient later in Section 3 below). Yet this construction is especially amenable to com-

Received October 17, 1978.


*Research partially supported by NSF Grant MCS 76-06744.

© 1979 American Mathematical Society
0025-5718/79/0000-0165/$03.50

1307
puters because, as we shall see, once a correct guess is made, it is sufficient to test three mechanically chosen primes \( q \) to establish the congruence properties like those just described for \( x^2 + 257y^2 \).

2. The Class Fields. We start with \( \text{Cl} \), the ideal class group of order \( h \) for the field

\[
k_2 = \mathbb{Q}(-p)^{1/2} \quad (\text{prime}) \; p \equiv 1 \pmod{8}.
\]

The 2-Sylow subgroup \( \text{Cl}_2 \) is known to be cyclic \( C(2^T) \), for some \( T \geq 2 \). We call the \( 2^m \text{-class group} \) \((0 < m \leq T)\) the subgroup \( \text{Cl}^{2m} \) of \( \text{Cl} \) consisting of those classes of \( \text{Cl} \) which are \( 2^m \)-powers; then the even part of the \( 2^m \text{-class group} \) is \( C(2^{T-m}) \).

The \( 2^m \text{-class field} \) \( k_{2m+1} \) is defined uniquely as that normal extension of \( k_2 \) for which a prime ideal \( q \) in \( k_2 \) (of prime norm \( q \)) splits completely in \( k_{2m+1} \) precisely when \( q \) belongs to a class in \( \text{Cl}^{2m} \). Then \( \text{Gal} \; k_{2m+1}/k_2 = \text{Cl}/\text{Cl}^{2m} \) and \( [k_{2m+1} : k_2] = 2^m \). Another characterization of \( k_{2m+1} \) is that it is the unique unramified normal extension of \( k_2 \) of degree \( 2^m \).

For notation we use Latin letters for rational integers and Greek for algebraic, while subscripts or German letters denote ideals (always) in \( k_2 \), e.g., \((2) = 2^2\), \((e) = \epsilon_1 \epsilon_2\), etc. We summarize an earlier paper which goes as far as \( k_4 \), (see [2]). For \( \text{Cl}^2 \) we have genus theory, and

\[
k_4 = k_2(i).
\]

For \( \text{Cl}^4 \) we have

\[
k_8 = k_4(e^{1/2}),
\]

where \( e \) is a fundamental unit of \( \mathbb{Q}(p^{1/2}) \), (see table in [5]),

\[
(2.4a) \quad e = s + tp^{1/2}, \quad e' = s - tp^{1/2},
\]

\[
(2.4b) \quad s^2 - t^2p = -1, \quad s > 0, t > 0.
\]
For $\text{Cl}^8$ (when $8 \mid h$) we have

$$k_{16} = k_8(\Gamma^{1/2})$$

where $\Gamma$ is defined by the relations

$$-p = f^2 - 2e^2, \quad f \equiv -1 \pmod{4}, e > 0,$$

$$\Gamma = (f + (-p)^{1/2})e^{1/2}/(1 - i).$$

3. Input Data for Cyclic-Sixteen Class Fields. We continue to define new parameters for when $8 \mid h$. First of all we solve

$$ew^2 = u^2 + pv^2, \quad v > 0, w > 0, u \equiv fv \pmod{e}.$$  

The solvability of this equation follows from the fact that in $k_2$ $(2) = 2_1^2$ so $2_1$ is an ideal whose class is of order 2, while by (2.6) $e = N\epsilon_1$, where $\epsilon_1$ is in a class of order 4. Similarly, $w = N\nu_1$, so $\nu_1$ is in a class of order 8. The congruence conditions of $u$ and $v$ guarantee that $\epsilon_1^1 \mid f + (-p)^{1/2}$, while $\epsilon_1 \mid u + v(-p)^{1/2}$ (this is important when $e$ is composite). The actual computation is done by machine after preliminary calculations show that $v$ cannot always be assumed to be one. For the current run we can take $v \leq 5$.

We also need to assign signs to radicals. We begin by arbitrarily assigning signs to

$$(-p)^{1/2}, i, e^{1/2}, \Gamma^{1/2},$$

subject to $p^{1/2} = -(-p)^{1/2}i$ in the computation of $e$ (see (2.4)) and

$$e'^{1/2} = i/e^{1/2}.$$  

Other radicals are now determined. For example, by squaring both sides,

$$(1 + si)^{1/2} = (e^{1/2} - e'^{1/2})(1 - i).$$

Furthermore, if we decompose

$$p = a^2 + b^2, \quad (\text{odd}) a > 0, (\text{even}) b,$$

we can choose the sign of $b$ so that for suitable integers, $z_1$ and $z_2$

$$(1 + si) = (a + bi)(z_1 + z_2i)^2, \quad z_1 > 0, z_2 > 0$$

(note $z_1^2 + z_2^2 = t$). This is done by using a double-precision complex square-root of the two fractions $(1 + si)/(a \pm bli)$ to find which one is closer to a Gaussian integer. Therefore,

$$(a + bi)^{1/2} = (e^{1/2} - e'^{1/2})(1 - i)(z_1 + z_2i).$$

We finally read in from a table of units [6] the fundamental unit for the Gauss-Pell equation

$$\Omega_0 = t_1 + it_2 + (u_1 + iu_2)(a + bi)^{1/2}/2,$$
<table>
<thead>
<tr>
<th>$p$</th>
<th>$h$</th>
<th>$e$</th>
<th>$f$</th>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
<th>$a$</th>
<th>$b$</th>
<th>$s$</th>
<th>$t$</th>
<th>$z_1$</th>
<th>$z_2$</th>
<th>$t_1$</th>
<th>$t_2$</th>
<th>$u_1$</th>
<th>$u_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>257</td>
<td>16</td>
<td>13</td>
<td>-9</td>
<td>-5</td>
<td>2</td>
<td>9</td>
<td>1</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>-43</td>
<td>75</td>
<td>5</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>353</td>
<td>16</td>
<td>17</td>
<td>15</td>
<td>32</td>
<td>1</td>
<td>9</td>
<td>17</td>
<td>-8</td>
<td>71264</td>
<td>3793</td>
<td>33</td>
<td>52</td>
<td>-5</td>
<td>-3</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>409</td>
<td>16</td>
<td>17</td>
<td>-13</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>20</td>
<td>11, 19217, 96968</td>
<td>55341</td>
<td>76685</td>
<td>74186</td>
<td>5533</td>
<td>-73</td>
<td>133</td>
<td>7</td>
</tr>
<tr>
<td>521</td>
<td>32</td>
<td>21</td>
<td>19</td>
<td>-2</td>
<td>1</td>
<td>5</td>
<td>11</td>
<td>-20</td>
<td>1283, 77240</td>
<td>56, 24309</td>
<td>590</td>
<td>2297</td>
<td>-2489</td>
<td>-1309</td>
<td>-309</td>
<td>-501</td>
</tr>
<tr>
<td>809</td>
<td>32</td>
<td>25</td>
<td>-21</td>
<td>404</td>
<td>1</td>
<td>81</td>
<td>5</td>
<td>28</td>
<td>43, 38520, 26040</td>
<td>52534</td>
<td>24933</td>
<td>23023</td>
<td>1898</td>
<td>29477</td>
<td>-6753</td>
<td>3425</td>
</tr>
<tr>
<td>857</td>
<td>32</td>
<td>21</td>
<td>-5</td>
<td>11</td>
<td>2</td>
<td>13</td>
<td>29</td>
<td>4</td>
<td>81, 18568</td>
<td>2, 77325</td>
<td>397</td>
<td>346</td>
<td>-7123</td>
<td>-4551</td>
<td>-1371</td>
<td>-749</td>
</tr>
<tr>
<td>953</td>
<td>32</td>
<td>29</td>
<td>27</td>
<td>-33</td>
<td>2</td>
<td>13</td>
<td>13</td>
<td>28</td>
<td>27468, 64744</td>
<td>889, 79677</td>
<td>9211</td>
<td>2034</td>
<td>23</td>
<td>-5</td>
<td>3</td>
<td>-3</td>
</tr>
<tr>
<td>1129</td>
<td>16</td>
<td>25</td>
<td>-1</td>
<td>564</td>
<td>1</td>
<td>113</td>
<td>27</td>
<td>20</td>
<td>168</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>-3901</td>
<td>-2551</td>
<td>-777</td>
<td>-207</td>
</tr>
<tr>
<td>1153</td>
<td>16</td>
<td>29</td>
<td>23</td>
<td>17</td>
<td>2</td>
<td>13</td>
<td>33</td>
<td>-8</td>
<td>102, 47504</td>
<td>3, 01789</td>
<td>339</td>
<td>431</td>
<td>-12533</td>
<td>49579</td>
<td>-3145</td>
<td>8193</td>
</tr>
<tr>
<td>1201</td>
<td>16</td>
<td>25</td>
<td>7</td>
<td>596</td>
<td>3</td>
<td>121</td>
<td>25</td>
<td>-24</td>
<td>2490, 13832, 32746</td>
<td>85416, 85609</td>
<td>59261</td>
<td>79793</td>
<td>463</td>
<td>7663</td>
<td>39551</td>
<td>2841</td>
</tr>
<tr>
<td>1217</td>
<td>32</td>
<td>33</td>
<td>31</td>
<td>91</td>
<td>4</td>
<td>29</td>
<td>31</td>
<td>16</td>
<td>276, 28256</td>
<td>7, 91969</td>
<td>760</td>
<td>463</td>
<td>7663</td>
<td>39551</td>
<td>2841</td>
<td>6201</td>
</tr>
<tr>
<td>1249</td>
<td>32</td>
<td>25</td>
<td>-1</td>
<td>624</td>
<td>1</td>
<td>125</td>
<td>15</td>
<td>32</td>
<td>3292, 32746</td>
<td>81326, 40028, 57788, 2841</td>
<td>1, 3146, 53389, 88887</td>
<td>10171</td>
<td>59037</td>
<td>03685</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1657</td>
<td>16</td>
<td>29</td>
<td>-5</td>
<td>82</td>
<td>1</td>
<td>17</td>
<td>19</td>
<td>36</td>
<td>10725, 88716</td>
<td>263, 49475, 4982, 1234</td>
<td>18011</td>
<td>65485</td>
<td>26329</td>
<td>15735</td>
<td>-10057</td>
<td></td>
</tr>
</tbody>
</table>
where \((a + bi)^{1/2}\) has a sign already specified by (3.5c). According to general methods of Dirichlet [3] (in analogy with the "ordinary" case (2.4)),

\[
N_{Q(i)}\Omega_0 = ((t_1 + it_2)^2 - (u_1 + iu_2)^2(a + bi))/4 = \pm 1.
\]

(Often there is a more convenient \(\Omega_1\) in \(Q(a + bi)^{1/2}\) of norm \(i\xi^2, \xi \in Q(i)\), which differs from \(\Omega_0\) by a square factor. Thus when \(p = 257\), we can use \(\Omega_1 = (1 + (1 + 16i)^{1/2})\) instead; see (1.1).)

The entries of Table I are now completely accounted for.

**Conjecture 3.8.** When \(16 \mid h\), the radicand of the 16-class field

\[
k_{32} = k_{16}(\Lambda^{1/2})
\]

may be taken as

\[
\Lambda = (u + v(-p)^{1/2})\Omega\Gamma^{1/2},
\]

where \(\Omega\) is either \(\Omega_0\) or \(i\Omega_0\) (as remains to be determined).

We verify this conjecture for the fourteen \(p < 2000\) where \(16 \mid h\). There either \(h = 16\) and \(Cl^{16}\) consists only of principal classes, or \(h = 32\) and \(Cl^{16}\) also contains those equivalent to \(2_1\). Thus, in any case, for \(q = Nq\) and \(q \in Cl^{16}\), we can write

\[
f_0q = x^2 + py^2, \quad 16f_0 \mid h.
\]

We must show that for exactly such (large) \(q\) the defining equation for \(\Lambda^{1/2}\) splits modulo \(q\) into 32 factors once we have chosen the right \(\Omega\) (= \(\Omega_0\) or \(i\Omega_0\)).

**4. Galois Group Considerations.** We must have \(k_{32}/k_2\) cyclic and \(k_{32}/Q\) dihedral. Thus, we want (compare [2])

\[
Gal k_{32}/Q = \langle \sigma, \tau | \sigma^{16} = \tau^2 = (\sigma\tau)^2 = 1 \rangle,
\]

where \(\sigma\) and \(\tau\) may be chosen as follows:

\[
(4.2a) \quad \sigma: \begin{cases} 
(-p)^{1/2} \rightarrow (-p)^{1/2}, & p^{1/2} \rightarrow -p^{1/2}, & i \rightarrow -i, \\
e^{1/2} \rightarrow e'^{1/2}, & e'^{1/2} \rightarrow -e^{1/2}, & \Gamma \rightarrow \Gamma/e, \\
\Omega \rightarrow \sigma\Omega, & \Lambda \rightarrow \Lambda\sigma\Omega/\Omega e^{1/2}, 
\end{cases}
\]

\[
(4.2b) \quad \tau: \begin{cases} 
p^{1/2} \rightarrow p^{1/2}, & (-p)^{1/2} \rightarrow -(-p)^{1/2}, & i \rightarrow -i, \\
e^{1/2} \rightarrow e^{1/2}, & e'^{1/2} \rightarrow -e'^{1/2}, & \Gamma \rightarrow ee^2/\Gamma, \\
\Omega \rightarrow \tau\Omega, & \Lambda \rightarrow e^2w^2e^{1/2}\tau\Omega/\Lambda.
\end{cases}
\]

For the operations on \(\Omega\), write \(\alpha\) and \(\beta\) as elements of \(Q(i)\), using \(\alpha'\) and \(\beta'\) to denote conjugates over \(Q\).
\[ \Omega = \alpha + \beta (e^{1/2} - e'^{1/2}), \]
\[ \tau \Omega = \sigma \Omega = \alpha' + \beta' (e^{1/2} + e'^{1/2}), \]
\[ \sigma^2 \Omega = \alpha - \beta (e^{1/2} - e'^{1/2}) = \pm i/\Omega, \]
\[ \sigma^{-1} \Omega = \sigma^3 \Omega = \alpha' - \beta' (e^{1/2} + e'^{1/2}) = \pm i/\sigma^3 \Omega. \]

To verify the Galois group (4.1) requires, first of all, normality:

**Conjecture 4.3.** \((k_{16} = k_8(\Gamma^{1/2}) \supseteq k_8(\Sigma^{1/2}) \supseteq k_8), where\)

\[ \Sigma = \Omega \sigma \Omega e^{1/2}. \]

From this result \(k_{16}(\Lambda^{1/2})\) is normal over \(Q\). We see this by listing the conjugates of \(\Sigma\) generated by \(\sigma\) and \(\tau\) (all differing by square factors). Since all conjugates of \(k_{32}\) over \(k_2\) must be generated by \(\sigma\) and since \(\Lambda^{1/2} \notin k_{16}\) (as implied by Conjecture 3.8), then \(\text{Gal } k_{32}/k_2 = C(16)\). Similarly, \(k_8(\Sigma^{1/2})/k_2\) is cyclic independently of Conjecture 4.3. The more tempting conjecture, \(k_{16} = k_8(\Sigma^{1/2}) \supseteq k_8\), seems valid but is not needed for now, (compare Section 7 below).

We shall produce a computer output to simultaneously verify Conjectures 3.8 and 4.3.

5. The Conductor-Discriminant Theorem. The radicand \(\Lambda\) was set up as a perfect (ideal) square as the first step in finding an unramified \(k_{32}\) over \(k_{16}\) (hence over \(k_2\)). The worst possible case now is that \(k_{32}\) is ramified over even primes (i.e., \(2_1\)) in \(k_2\). This would mean, in effect, that for an ideal \(f\) (the conductor) in \(k_2\), all odd primes in \(k_2\) congruent to one another \(\mod 4\) split completely if one such prime does from \(k_2\) to \(k_{32}\). This reduces the testing to a finite set; see [4].

**Lemma 5.1.** Let \(K \supset K_1 \supset k\), where \(\text{Gal } K/k = C(2^m)\), \(\text{Gal } K_1/k = C(2^{m-1})\); and let \(K_1/k\) be unramified, while \(K = K_1(\Lambda^{1/2})\), where \(\Lambda\) is an ideal square in \(K_1\). Then the conductor of \(K/k\) is a divisor of \(4\). Thus, if \(\mathfrak{p}_1\) and \(\mathfrak{p}_2\) are two odd prime ideals in \(k\), they will factor alike in \(K/k\) when they belong to the same class \(\mod 4\) in \(k\).

The proof follows from the fact that the different of \(K_1/k\) is 1 (unramified), while that of \(K/K_1\) divides 2 (since \(\Lambda\) is an ideal square). Thus, the discriminant of \(K/k\) divides \(2^{2m}\). But by the conductor-discriminant theorem (see Hasse [4]), this discriminant = \(\prod_{\chi} f_{\chi}\), where \(\chi\) are the characters of \(H_0 = \text{Gal } K/k\) and \(f_{\chi}\) is the conductor over \(k\) of the field fixed by that subgroup of \(H_0\) for which \(\chi = 1\). In effect, \(f_{\chi} = 1\) for all proper subfields and \(f_{\chi}\) is the conductor for \(K\) occurring as often in the product as \(\chi\) is primitive, i.e., \(\phi(2^m) = 2^{m-1}\) times. But \(2^{2m} = 4^{\phi(2^m)}\).

We, therefore, need a refinement of \(\text{Cl}^{2m} \mod \text{Cl}^{2m} (\mod 4)\). Here we consider only odd ideals \(a\) and \(b\); they are equivalent exactly when for odd integers in \(k_2\), namely \(\alpha\) and \(\beta\)

\[ \alpha a = \beta b, \quad \alpha \equiv \beta \mod 4. \]
The even part of $\text{Cl}^{2m}(\text{mod} \times 4)$ is $C(2^{T-m}) \times C(2) \times C(2)$. The cycles $C(2) \times C(2)$ come from the four-group of odd principal ideals $(\alpha)$ modulo 4, i.e., $\pm \alpha$, where

\begin{equation}
\alpha \equiv 1, \quad 1 + 2(-p)^{1/2}, \quad (-p)^{1/2}, \quad (-p)^{1/2} + 2 \quad (\text{mod} \ 4).
\end{equation}

Once we verify the splitting properties in $\text{Cl}^{16}(\text{mod} \times 4)$ in $k_{32}/k_2$ it will follow (from the equivalent definitions of class field in Section 2) that $k_{32}/k_2$ is unramified and the conductor $\mathfrak{f}$ was actually the unit ideal.

Preliminary Computational Procedure 5.2. For any $p$ (with $16 \mid h$) we can verify Conjecture 4.3 by testing to see that primes generating $\text{Cl}^8(\text{mod} \times 4)$ split completely in $k_8(\Sigma^{1/2})$. To verify Conjecture 3.8 we need only have to assume Conjecture 4.3 and make tests to show that primes generating $\text{Cl}^8(\text{mod} \times 4)$ split completely in $k_{16}(\Lambda^{1/2})$ while one prime which splits in $k_{16}$ (i.e., an eighth-power class) does not, (so $\Lambda^{1/2} \notin k_{16}$).

We begin with $\text{Cl}^8$. For given $p$, let $x$ and $y$ vary so as to generate primes $q$ such that

\begin{equation}
f_0q = x^2 + py^2, \quad x > 0, y > 0,
\end{equation}

where $f_0 = 1$ and 2 when $h = 16$ and $f_0 = 1$, 2, and $e$ when $h = 32$. When $f_0 = e$, we further require

\begin{equation}
f_0y \equiv \pm x \quad (\text{mod} \ e),
\end{equation}

so for some choice of sign $q \sim e^{-1}$ (compare (3.1)). In all cases the class of $q$ is an eighth power, and together they generate $\text{Cl}^8$.

Final Computational Procedure 5.5. Select three primes $q$ for each $p$ as follows: Two of them are principal ($f_0 = 1$) and correspond to two of the three nontrivial classes in (5.1b). The third corresponds to a nonprincipal class, namely a generator of $\text{Cl}^8(\text{mod} \times 4)$, (so $f_0 = 2$ when $h = 16$ and $f_0 = e$ when $h = 32$). Procedure 5.2 can be restricted to just these $q$.

The slight improvement from Procedures 5.2 to 5.5 is due to the fact that we really use a multiplicative symbol "$((K/k)/C)$" to test the splitting character of the ideal $q$ in class $C$ from $k$ to $K$. Thus, it is trivial that the square of a class will split.

6. Verification of Conjectures by Output. The test primes $q$ are chosen by a machine search according to (5.3) (with the a priori guess that $q < 9999$ would suffice) Actually, the machine accepted for output one representative $q$ per class in $\text{Cl}^8(\text{mod} \times 4)$ when available, so Table II was selected from a much longer list.

The arithmetic modulo $q$ was performed with the help of a table of indices generated internally for each $q$. Thus, the machine tried to solve for $x_1, x_2, x_3, x_4, x_5$ representing $(-p)^{1/2}, i, \epsilon^{1/2}, \Gamma^{1/2}, \Lambda^{1/2}$ (as residues modulo a prime divisor of $q$ in $k_{32}$)

\begin{equation}
\begin{cases}
x_1^2 \equiv - p, \quad x_2^2 \equiv - 1, \quad x_3^2 \equiv s - tx_1x_2, \\
x_4^2 \equiv (f + x_1)x_3(1 - x_2), \quad (\text{mod} \ q), \\
x_5^2 \equiv (u + wx_1)x_2y_4x_4 \quad (\equiv w_5),
\end{cases}
\end{equation}

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Here $\Omega$ is represented by $y_4$, where

$$(6.2) \quad y_4 = f(x_2, x_3) \equiv \frac{1}{2} \left( t_1 + t_2 x_2 + \frac{u_1 + u_2 x_2 (x_3 - x_2/x_3)}{1 - x_2(z_1 + x_2 z_2)} \right) \pmod{q};$$

and, of course, we let $U = 0$ if $\Omega = \Omega_0$ and $U = 1$ if $\Omega = i\Omega_0$.

To check Conjecture 4.3, test $\Sigma$ (see (4.4)) by

$$(6.3) \quad x_6^2 \equiv y_4 y'_4 x_3 \pmod{w_6}.$$
where \( y'_4 \) represents \( \sigma \Omega \). Thus by (4.2a),

\[
y'_4 \equiv f(-x_2, x_2/x_3) \pmod{q}.
\]

The output is given by the indices of \( x_1, x_2, x_3, x_4, w_5, w_6 \) with primitive root \( r \pmod{q-1} \) as shown in Table II. We now have the sign choices of (3.2) in the \( x_1, \ldots, x_4 \) and the residuacity of \( w_5, w_6 \). Thus, Procedure 5.5 requires that \( w_6 \) has an even index, while \( w_5 \) has an odd index just when \( f_0 > 1 \).

We use “large” \( q \) to avoid \( q \mid 2ewp \), so 0 is never a factor in (6.1). If \( h = 16 \cdot \text{odd} \) or \( 32 \cdot \text{odd} \), no modification is required (since our search at worst misses eligible primes \( q \) where \( f_0 q^{0 \text{dd}} = x^2 + py^2 \)). If, however, \( 64 \mid h \), we should have to use a different value of \( f_0 \) in (5.3) to catch the nonprincipal generator of \( \text{Cl}^8 \), e.g., if \( 128 \mid h \), we could take \( f_0 = w \).

7. Concluding Remarks. Further computations seem to indicate that when \( p \equiv 1 \pmod{4} \), \( k_8(\Gamma^{1/2}) = k_8(\Sigma^{1/2}) = k_{16} \), (even when \( 8 \nmid h \)). In fact, it would seem that \( k_8 \) has as a 2-fundamental system of units

\[
i, \Omega, \sigma \Omega, e^{1/2}
\]

of torsion-free rank 3, although this system becomes no part of a 2-fundamental set in \( k_{16} \) (because \( \Sigma^{1/2} \) occurs).

The rank of the unit system is an indication of how the current results lead to a much more chaotic state of affairs. It is an easy guess that the 32-class field \( k_{64} \) is generated by \( \Lambda^{1/2} \), where

\[
\Lambda^* = (u^* + v^*(-p)^{1/2})\Omega^*\Lambda^{1/2}\Gamma^{-1/2}.
\]

Here \( u^{*2} + v^{*2}p = \phi^{**2} \), as in (3.1), with a similar sign condition to ensure the ideal-square property of \( \Lambda^* \). Likewise, \( \Omega^* \) is a unit of \( k_{16} \) (not \( k_8 \)); and the torsion-free rank of such units is now 7 (not 3). Thus, the chances of guessing \( \Omega^* \) become increasingly remote. Nevertheless, the pattern of inductively finding the \( 2^m \)-class field seems, at least conjecturally, clear from (3.10) and (7.2).

As a parallel problem, the criterion for \( 16 \mid h \) is as yet unknown and seems to be of a much greater degree of difficulty than that of \( 8 \mid h \), which is given by the representability of \( p = a^2 + 32b^2 \); see [1]. The author is greatly indebted to Jeff Lagarias for helpful discussions and speculations as well as comments on the present paper.

The Computing Center of the City University of New York has kindly provided the service of the Wylbur-IBM 370 System.


7. K. S. WILLIAMS, “On the divisibility of the class number of $\mathbb{Q}(-p)^{\frac{1}{2}}$ by 16.” (Manuscript.)