MATHEMATICS OF COMPUTATION, VOLUME 33, NUMBER 148
OCTOBER 1979, PAGES 1307–1316

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

By Harvey Cohn*

Abstract. Numerical experiments result in the construction of cyclic-sixteen class fields for $\mathbf{Q}(-p)^{1/2}$, 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 $\mathbf{Z}$) exactly when a certain equation over $\mathbf{Q}$ 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

$$(1.1)\qquad \begin{aligned}\Lambda_0 &= (-5 + 2(-257)^{1/2})(1 + (1 + 16i)^{1/2})\\ &\cdot \left(\frac{-9 + (-257)^{1/2}}{1 - i}(16 + 257^{1/2})^{1/2}\right)^{1/2},\end{aligned}$$

so that the radicals in Λ_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:

$$(1.2)\qquad \begin{cases} x_1^2 \equiv -257, \quad x_2^2 \equiv -1, \quad x_3^2 \equiv 16 - x_1x_2, \\ x_4^2 \equiv (-9 + x_1)x_3/(1 - x_2), & \pmod q. \\ x_5^2 \equiv (-5 + 2x_1)\left(1 + \dfrac{x_3 - x_2/x_3}{1 - x_2}\right)x_4, \end{cases}$$

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 $k_2 = \mathbf{Q}(-p)^{1/2}$ 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 Λ_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.

AMS (MOS) subject classifications (1970). Primary 12A65, 12A25; Secondary 12A50, 12A45.

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

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 Cl, the ideal class group of order h for the field

(2.1) $$k_2 = Q(-p)^{1/2} \quad \text{(prime) } p \equiv 1 \pmod 8.$$

The 2-Sylow subgroup Cl_2 is known to be cyclic $C(2^T)$, for some $T \geq 2$. We call the *2^m-class group* $(0 < m \leq T)$ the subgroup Cl^{2^m} of Cl consisting of those classes of Cl which are 2^m-powers; then the even part of the 2^m-class group is $C(2^{T-m})$.

The *2^m-class field* k_{2m+1} is defined uniquely as that normal extension of k_2 for which a prime ideal $\mathfrak{q}$ in k_2 (of prime norm q) splits completely in k_{2m+1} precisely when $\mathfrak{q}$ belongs to a class in Cl^{2^m}. Then Gal $k_{2m+1}/k_2 = \mathrm{Cl}/\mathrm{Cl}^{2^m}$ 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., $(2) = \mathfrak{2}_1^2$, $(e) = \mathfrak{e}_1\mathfrak{e}_2$, etc. We summarize an earlier paper which goes as far as k_{16}, (see [2]). For Cl^2 we have genus theory, and

(2.2) $$k_4 = k_2(i).$$

For Cl^4 we have

(2.3) $$k_8 = k_4(\epsilon^{1/2}),$$

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

(2.4a) $$\epsilon = s + tp^{1/2}, \qquad \epsilon' = s - tp^{1/2},$$

(2.4b) $$s^2 - t^2p = -1, \qquad s > 0, t > 0.$$

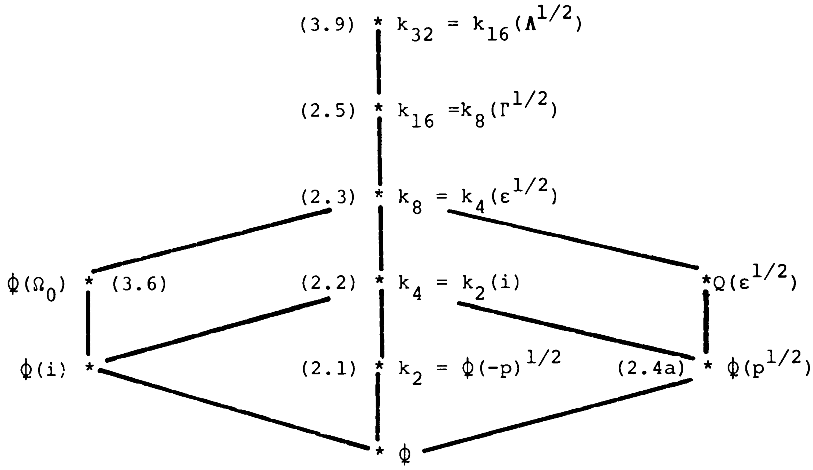

FIGURE 1
Tower of class fields over k_2

For Cl^8 (when $8 \mid h$) we have

$$k_{16} = k_8(\Gamma^{1/2}), \tag{2.5}$$

where Γ is defined by the relations

$$-p = f^2 - 2e^2, \quad f \equiv -1 \pmod 4),\ e > 0, \tag{2.6}$$

$$\Gamma = (f + (-p)^{1/2})\epsilon^{1/2}/(1 - i). \tag{2.7}$$

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

$$ew^2 = u^2 + pv^2, \quad v > 0,\ w > 0,\ u \equiv fv \pmod e). \tag{3.1}$$

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) $e = N\mathfrak{e}_1$, where $\mathfrak{e}_1$ is in a class of order 4. Similarly, $w = N\mathfrak{w}_1$ so $\mathfrak{w}_1$ is in a class of order 8. The congruence conditions of u and v guarantee that $\mathfrak{e}_1^2 \mid f + (-p)^{1/2}$, while $\mathfrak{e}_1 \mid u + v(-p)^{1/2}$ (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 $v \leqslant 5$.

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

$$(-p)^{1/2},\ i,\ \epsilon^{1/2},\ \Gamma^{1/2}, \tag{3.2}$$

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

$$\epsilon'^{1/2} = i/\epsilon^{1/2}. \tag{3.3}$$

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

$$(1 + si)^{1/2} = (\epsilon^{1/2} - \epsilon'^{1/2})/(1 - i). \tag{3.4}$$

Furthermore, if we decompose

$$p = a^2 + b^2, \quad \text{(odd) } a > 0, \text{ (even) } b, \tag{3.5a}$$

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

$$(1 + si) = (a + bi)(z_1 + z_2 i)^2, \quad z_1 > 0,\ z_2 > 0 \tag{3.5b}$$

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

$$(a + bi)^{1/2} = (\epsilon^{1/2} - \epsilon'^{1/2})/(1 - i)(z_1 + z_2 i). \tag{3.5c}$$

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

$$\Omega_0 = \frac{t_1 + it_2 + (u_1 + iu_2)(a + bi)^{1/2}}{2}, \tag{3.6}$$

TABLE I. *Input*

	$\Phi(-p)^{1/2}$						$Q(i)$		$\Phi(p^{1/2})$		$\mathfrak{Q}(a+bi)^{1/2}$					
p	h	e	f	u	v	w	a	b	s	t	z_1	z_2	t_1	t_2	u_1	u_2
257	16	13	-9	-5	2	9	1	16	16	1	1	0	-43	75	5	21
353	16	17	15	32	1	9	17	-8	71264	3793	33	52	-5	-3	-1	-1
409	16	17	-13	4	1	5	3	20	11, 19217,96968	55341,76685	74186	5533	-73	133	7	33
521	32	21	19	-2	1	5	11	-20	1283,77240	56,24309	590	2297	-2489	-1309	-309	-501
569	32	17	3	-39	4	25	13	-20	28948,63832	1213,59005	3131	1562	-219	-209	-19	-59
809	32	25	-21	404	1	81	5	28	43, 38520,26040	1, 52534,24933	1, 23023	1898	29477	-6753	3425	-4519
857	32	21	-5	11	2	13	29	4	81,18568	2,77325	397	346	-7123	-4551	-1371	-749
953	32	29	27	-33	2	13	13	28	27468,64744	889,79677	9211	2034	23	-5	3	-3
1129	16	25	11	-564	1	113	27	20	168	5	2	1	-3901	-2551	-777	-207
1153	16	29	23	17	2	13	33	-8	102,47504, 00230,72656	3,01789, 02568,75073	339, 62297	431, 79308	-12533	49579	-3145	8193
1201	16	25	7	596	3	121	25	-24	2490, 13832,32746 50571,44832	71, 85416,85609 44230,77385	3, 32361, 77461	7, 79793, 13692	-6089	527	-993	-303
1217	32	33	31	91	4	29	31	16	276,28256	7,91969	760	463	7663	39551	2841	6201
1249	32	25	-1	624	1	125	15	32	3292, 35587,03432, 90296,88240	2, 61326,40028, 30963,92593	1, 57788, 89768	35146, 88887	-3, 53389	12, 10171	59037	2, 03685
1657	16	29	-5	82	1	17	19	36	10725,88716, 86860,36632	263,49475, 20206,35645	4982, 59718	1234, 18011	6, 65485	3, 26329	1, 15735	-10057

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)),

$$N_{\mathbf{Q}(i)}\Omega_0 = ((t_1 + it_2)^2 - (u_1 + iu_2)^2(a + bi))/4 = \pm i. \tag{3.7}$$

(Often there is a more convenient Ω_1 in $\mathbf{Q}(a + bi)^{1/2}$ of norm $i\xi^2$, $\xi \in \mathbf{Q}(i)$, which differs from Ω_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*

$$k_{32} = k_{16}(\Lambda^{1/2}) \tag{3.9}$$

may be taken as

$$\Lambda = (u + v(-p)^{1/2})\Omega\Gamma^{1/2}, \tag{3.10}$$

where Ω is either Ω_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 $q = N\mathfrak{q}$ and $\mathfrak{q} \in \mathrm{Cl}^{16}$, we can write

$$f_0 q = x^2 + py^2, \qquad 16f_0 \mid h. \tag{3.11}$$

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 Ω $(=\Omega_0$ or $i\Omega_0)$.

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

$$\mathrm{Gal}\, k_{32}/\mathbf{Q} = \langle \sigma, \tau \mid \sigma^{16} = \tau^2 = (\sigma\tau)^2 = 1 \rangle, \tag{4.1}$$

where σ and τ may be chosen as follows:

$$\sigma: \begin{cases} (-p)^{1/2} \longrightarrow (-p)^{1/2}, & p^{1/2} \longrightarrow -p^{1/2}, \quad i \longrightarrow -i, \\ \epsilon^{1/2} \longrightarrow \epsilon'^{1/2}, & \epsilon'^{1/2} \longrightarrow -\epsilon^{1/2}, \quad \Gamma \longrightarrow \Gamma/\epsilon, \\ \Omega \longrightarrow \sigma\Omega, & \Lambda \longrightarrow \Lambda\sigma\Omega/\Omega\epsilon^{1/2}, \end{cases} \tag{4.2a}$$

$$\tau: \begin{cases} p^{1/2} \longrightarrow p^{1/2}, & (-p)^{1/2} \longrightarrow -(-p)^{1/2}, \quad i \longrightarrow -i, \\ \epsilon^{1/2} \longrightarrow \epsilon^{1/2}, & \epsilon'^{1/2} \longrightarrow -\epsilon'^{1/2}, \quad \Gamma \longrightarrow \epsilon e^2/\Gamma, \\ \Omega \longrightarrow \tau\Omega, & \Lambda \longrightarrow e^2 w^2 \epsilon^{1/2}\tau\Omega\Omega/\Lambda. \end{cases} \tag{4.2b}$$

For the operations on Ω, write α and β as elements of $\mathbf{Q}(i)$, using α' and β' to denote conjugates over $\mathbf{Q}$,

$$
\begin{aligned}
\Omega &= \alpha + \beta(\epsilon^{1/2} - \epsilon'^{1/2}),\\
\tau\Omega = \sigma\Omega &= \alpha' + \beta'(\epsilon^{1/2} + \epsilon'^{1/2}),\\
\sigma^2\Omega &= \alpha - \beta(\epsilon^{1/2} - \epsilon'^{1/2}) = \pm i/\Omega,\\
\sigma^{-1}\Omega = \sigma^3\Omega &= \alpha' - \beta'(\epsilon^{1/2} + \epsilon'^{1/2}) = \pm i/\sigma^3\Omega.
\end{aligned} \tag{4.2c}
$$

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*

$$\Sigma = \Omega\sigma\Omega\epsilon^{1/2}. \tag{4.4}$$

From this result $k_{16}(\Lambda^{1/2})$ is normal over $\mathbf{Q}$. We see this by listing the conjugates of Σ generated by σ and τ (all differing by square factors). Since all conjugates of k_{32} over k_2 must be generated by σ and since $\Lambda^{1/2} \notin k_{16}$ (as implied by Conjecture 3.8), then 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, $k_{16} = k_8(\Sigma^{1/2})(\supset k_8)$, 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 Λ 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 $\mathfrak{f}$ (the *conductor*) in k_2, all odd primes in k_2 congruent to one another $\text{mod}^\times \mathfrak{f}$ (see (5.1a) below) 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* Gal $K/k = C(2^m)$, Gal $K_1/k = C(2^{m-1})$; *and let* K_1/k *be unramified, while* $K = K_1(\Lambda^{1/2})$, *where* Λ *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* $(\text{mod}^\times 4)$ *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 Λ is an ideal square). Thus, the discriminant of K/k divides 2^{2^m}. But by the conductor-discriminant theorem (see Hasse [4]), this discriminant $= \Pi_\chi \mathfrak{f}_\chi$, where χ are the characters of H_0 = Gal K/k and $\mathfrak{f}_\chi$ is the conductor over k of the field fixed by that subgroup of H_0 for which $\chi = 1$. In effect, $\mathfrak{f}_\chi = 1$ for all proper subfields and $\mathfrak{f}_\chi$ is the conductor for K occurring as often in the product as χ is primitive, i.e., $\phi(2^m) = 2^{m-1}$ times. But $2^{2^m} = 4^{\phi(2^m)}$. □

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

$$\alpha\mathfrak{a} = \beta\mathfrak{b}, \quad \alpha \equiv \beta \pmod 4. \tag{5.1a}$$

The even part of $\mathrm{Cl}^{2^m}(\mathrm{mod}^\times 4)$ 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 (α) modulo 4, i.e., $\pm\alpha$, where

$$\alpha \equiv 1, \quad 1 + 2(-p)^{1/2}, \quad (-p)^{1/2}, \quad (-p)^{1/2} + 2 \pmod 4. \tag{5.1b}$$

Once we verify the splitting properties in $\mathrm{Cl}^{16}(\mathrm{mod}^\times 4)$ 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* Cl^8 $(\mathrm{mod}^\times 4)$ *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* Cl^8 $(\mathrm{mod}^\times 4)$ *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 Cl^8. For given p, let x and y vary so as to generate primes q such that

$$f_0 q = x^2 + py^2, \quad x > 0, y > 0, \tag{5.3}$$

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

$$f_0 y \equiv \pm x \pmod e, \tag{5.4}$$

so for some choice of sign $\mathfrak{q} \sim \mathfrak{e}_1^{-1}$ (compare (3.1)). In all cases the class of $\mathfrak{q}$ is an eighth power, and together they generate 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* Cl^8 $(\mathrm{mod}^\times 4)$, *(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 $\mathfrak{q}$ 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 Cl^8 $(\mathrm{mod}^\times 4)$ 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})

$$\begin{cases} x_1^2 \equiv -p, \quad x_2^2 \equiv -1, \quad x_3^2 \equiv s - tx_1x_2, \\ x_4^2 \equiv (f + x_1)x_3/(1 - x_2), \\ x_5^2 \equiv (u + vx_1)x_2^U y_4 x_4 \quad (\equiv w_5), \end{cases} \pmod q. \tag{6.1}$$

TABLE II. *Output*

$qf_0 = x^2 + py^2$								index (base r) of					
p	h	Ω	q	f_0	x	y	r	x_1	x_2	x_3	x_4	w_5	w_6
257	16	$i\Omega_0$	293	1	6	1	2	12	73	120	97	0	112
			1109	1	9	2	2	437	277	493	257	1052	68
			241	2	15	1	7	80	60	161	54	145	216
353	16	Ω_0	389	1	6	1	2	78	97	128	165	252	50
			1493	1	9	2	2	245	373	675	64	558	12
			181	2	3	1	2	56	45	103	29	109	134
409	16	Ω_0	509	1	10	1	2	91	127	150	238	238	156
			1637	1	1	2	2	817	409	948	328	1534	174
			229	2	7	1	6	107	57	150	24	227	10
521	32	$i\Omega_0$	557	1	6	1	2	158	139	332	148	474	362
			2309	1	15	2	2	1052	577	1510	1119	1992	1602
			101	21	40	1	2	27	25	67	4	33	68
569	32	$i\Omega_0$	2333	1	42	1	2	278	583	658	589	2232	494
			2357	1	9	2	2	661	589	1227	17	382	590
			641	17	76	3	3	66	160	445	256	355	176
809	32	Ω_0	1709	1	30	1	3	724	427	849	18	52	294
			3461	1	15	2	2	840	865	2510	702	26	3152
			149	25	54	1	2	40	37	83	13	89	44
857	32	Ω_0	1181	1	18	1	7	9	295	479	18	742	884
			4157	1	27	2	2	1182	1039	1907	282	2616	1766
			53	21	16	1	2	4	13	22	4	5	36
953	32	$i\Omega_0$	1277	1	18	1	2	63	319	422	333	850	998
			3821	1	3	2	3	586	955	1957	1805	1236	1076
			157	29	60	1	5	53	39	64	73	41	98
1129	16	Ω_0	1229	1	10	1	2	183	307	782	525	670	1194
			4517	1	1	2	2	2257	1129	2156	1667	2934	2592
			569	2	3	1	3	1	142	258	261	465	380
1153	16	$i\Omega_0$	1637	1	22	1	2	255	409	848	526	696	842
			4621	1	3	2	2	1617	1155	1464	171	3556	2566
			577	2	1	1	5	288	144	170	209	109	280
1201	16	Ω_0	1237	1	6	1	2	395	309	580	58	474	190
			4813	1	3	2	2	327	1203	2571	1642	1180	1580
			601	2	1	1	7	300	150	325	10	279	86
1217	32	$i\Omega_0$	4133	1	54	1	2	872	1033	2042	77	920	370
			4877	1	3	2	2	1306	1219	3407	545	1270	734
			37	33	2	1	2	1	9	20	4	7	0
1249	32	Ω_0	1733	1	22	1	2	856	433	1171	755	1094	942
			5021	1	5	2	3	1791	1255	1397	1425	4018	4212
			269	25	74	1	2	57	67	125	32	203	126
1657	16	$i\Omega_0$	1693	1	6	1	2	225	423	1260	380	1672	1402
			6637	1	3	2	2	1397	1659	3690	624	1040	4214
			829	2	1	1	2	414	207	254	160	797	130

Here Ω is represented by y_4, where

(6.2) $$y_4 \equiv f(x_2, x_3) \equiv \frac{1}{2}\left(t_1 + t_2x_2 + \frac{(u_1 + u_2x_2)(x_3 - x_2/x_3)}{(1 - x_2)(z_1 + x_2z_2)}\right) \pmod q;$$

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 Σ (see (4.4)) by

(6.3) $$x_6^2 \equiv y_4y_4'x_3 \quad (\equiv w_6) \quad \pmod q,$$

where y'_4 represents $\sigma\Omega$. Thus by (4.2a),

$$y'_4 \equiv f(-x_2, x_2/x_3) \pmod q. \tag{6.4}$$

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 $q \mid 2ewtp$, 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 $f_0 q^{\text{odd}} = x^2 + py^2$). 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 Cl^8, e.g., if $128 \nmid h$, 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

$$i,\ \Omega,\ \sigma\Omega,\ \epsilon^{1/2} \tag{7.1}$$

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

$$\Lambda^* = (u^* + v^*(-p)^{1/2})\Omega^*\Lambda^{1/2}\Gamma^{-1/2}. \tag{7.2}$$

Here $u^{*2} + v^{*2}p = ww^{*2}$, as in (3.1), with a similar sign condition to ensure the ideal-square property of Λ^*. Likewise, Ω^* 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 Ω^* 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 $p = a_0^2 + 32b_0^2$; 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.

City College of New York
138 Street and Convent Avenue
New York, New York 10031

1. P. BARRUCAND & H. COHN, "Note on primes of type $x^2 + 32y^2$, class number, and residuacity," *J. Reine Angew. Math.*, v. 238, 1969, pp. 67–70. MR **40** #2641.

1a. H. BAUER, "Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern," *J. Reine Angew. Math.*, v. 248, 1971, pp. 42–46. MR **44** #6643.

2. H. COHN & G. COOKE, "Parametric form of an eight class field," *Acta Arith.*, v. 30, 1976, pp. 367–377. MR **54** #10201.

3. P. G. L. DIRICHLET, "Untersuchungen über die Theorie der complexen Zahlen," *J. Reine Angew. Math.*, v. 22, 1841, pp. 375–378.

4. H. HASSE, "Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper," *J. Reine Angew. Math.*, v. 162, 1930, pp. 169–184.

5. E. L. INCE, *Cycles of Reduced Ideals in Quadratic Fields*, British Assoc. Adv. Sci. Math. Tables, vol. IV, London, 1934.

6. R. LAKEIN, *Class Number and Fundamental Unit of Dirichlet Fields With Prime Relative Discriminant.* (Unpublished table.)

7. K. S. WILLIAMS, "On the divisibility of the class number of $Q(-p)^{1/2}$ by 16." (Manuscript.)