MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 164
OCTOBER 1983, PAGES 711–730

On the Existence of Fields Governing the 2-Invariants of the Classgroup of $\mathbf{Q}(\sqrt{dp})$ as p Varies

By H. Cohn* and J. C. Lagarias

Abstract. This paper formulates general conjectures relating the structure of the 2-classgroup $C_2(dp)$ associated to $\mathbf{Q}(\sqrt{dp})$ to the splitting of the ideal (p) in certain algebraic number fields. Here $d \not\equiv 2 \pmod 4$ is a fixed integer and p varies over primes. The conjectures assert that there exists an algebraic number field $\Omega_j(d)$ such that the Artin symbol $[(\Omega_j(d)/\mathbf{Q})/(p)]$ determines the first j 2-invariants of the group $C_2(dp)$, i.e. it determines $C_2(dp)/C_2(dp)^{2^j}$. These conjectures imply that the set of primes p for which $C_2(dp)$ has a given set of 2-invariants has a natural density which is a rational number. Existing results prove the conjectures whenever $j = 1$ or 2 and also for an infinite set of d with $j = 3$. The smallest open case is $j = 3$, $d = -21$. This paper presents evidence concerning these conjectures for $d = -4$, 8 and -21. Numerical evidence is given that $\Omega_3(-21)$ exists, and that natural densities which are rational numbers exist for the sets of primes with $2^j \mid h(dp)$ for $d = -4$ and 8, for $1 \leq j \leq 7$. A search for the hypothetical field $\Omega_4(-4)$ ruled out the simplest candidate fields: $\Omega_4(-4)$ is not a normal extension of Q of degree 16 ramifying only at (2).

1. Introduction. Gauss initiated the study of the group $C(D)$ of equivalence classes of integral binary quadratic forms of discriminant D. He calculated the 2-rank e_1 of the 2-classgroup $C_2(D)$ (that is, the Sylow 2-subgroup of $C(D)$) in terms of the prime factorization of D using his theory of genera. On the other hand he noted that the subgroup of classes of odd order $C_{\text{odd}}(D)$ behaved irregularly and exhibited no obvious patterns as a function of D.

Gauss' theory of binary quadratic forms was later reworked by Dedekind in terms of the arithmetic of quadratic fields; Dedekind's formulation is most often used today. In this formulation the group $C(D)$ is interpreted as the ideal classgroup of the quadratic field $\mathbf{Q}(\sqrt{D})$, taken in the narrow or strict sense, when D is a fundamental discriminant,** and as a narrow ring classgroup of $\mathbf{Q}(\sqrt{D})$ if D is a nonfundamental discriminant. The *class number* $h(D)$ is the order of the classgroup $C(D)$. Note that $\mathbf{Q}(\sqrt{-p})$ has discriminant $-4p$ when $p \equiv 1 \pmod 4$, so the corresponding form classgroup is $C(-4p)$. The correspondence between form classgroups and ring classgroups is described in Cohn [4] and Stark [35].

This paper is concerned with the 2-classgroup $C_2(D)$. Many results have been proved about the structure of $C_2(D)$ as a function of D. The structure of such an abelian 2-group G is specified by its complete set of 2^j-invariants e_j. These invariants are defined inductively by

$$\left|G/G^{2^j}\right| = 2^{e_1+e_2+\cdots+e_j}.$$

Received November 22, 1982.
1980 *Mathematics Subject Classification.* Primary 12A50; Secondary 12A25.
* Research partially supported by N.S.F. grant MCS-7903060.
** D is *fundamental* if $D \equiv 1 \pmod 4$ is squarefree or if $D \equiv 0 \pmod 4$ and $D/4 \equiv 2$ or $3 \pmod 4$ is squarefree.

0025-5718/83 $1.00 + $.25 per page

Using methods that in principle go back to Gauss and Dirichlet, Redei and Reichardt [30] (see also [26]) determined the 4-invariant e_2 of $C_2(D)$ in terms of quadratic residue criteria among the prime factors of D. Redei [27] later determined in special cases the 8-invariant e_3 of $C_2(D)$ in terms of quartic residue criteria involving these prime factors. Redei [28], [29] went on to develop a general theory analyzing the structure of the 2-classgroup, and related it to equations of the form $D_1x^2 - D_2y^2 = z^{2^n}$, where $D_1D_2 = D$, and to the anti-Pellian equation $x^2 - DY^2 = -1$. He gave a general determination of the 2^j-invariants of $C_2(D)$ in terms of the ranks of certain matrices calculated using class field theory. Morton [19] gave an elementary version of Redei's theory and showed that Redei's matrices could be calculated using the solutions of certain auxiliary equations of the form $x_1^2 - a_1x_2^2 - a_2x_3^2 = 0$. Waterhouse [36] had earlier showed the 8-invariant e_3 could be calculated in this way. These results all have the feature that for $j \geqslant 3$ the 2-invariants e_j are no longer connected in a direct way with the prime factorization of D.

This paper proposes conjectures that relate the 2^j-invariants of $C_2(D)$ to the prime factors of D in an explicit way, and presents evidence supporting these conjectures.

These conjectures were motivated by the special case $C_2(-4p)$, where p is a prime. In that case $C_2(-4p)$ is a cyclic group, by genus theory, and we know that

$$2 \mid h(-4p) \Leftrightarrow p \equiv 1 \pmod 4, \tag{1.1}$$

$$4 \mid h(-4p) \Leftrightarrow p \equiv 1 \pmod 8, \tag{1.2}$$

$$8 \mid h(-4p) \Leftrightarrow p = x^2 + 32y^2. \tag{1.3}$$

Here (1.1) follows from genus theory, (1.2) from the Redei-Reichardt theorem, and (1.3) is a result of Barrucand and Cohn [1]. We observed that the right sides of (1.1)–(1.3) can be interpreted in terms of the splitting of prime ideals (p) in certain normal extensions of $\mathbf{Q}$, as follows.

$$p \equiv 1 \pmod 4 \Leftrightarrow (p) \text{ splits completely in } \mathbf{Q}(i), \tag{1.4}$$

$$p \equiv 1 \pmod 8 \Leftrightarrow (p) \text{ splits completely in } \mathbf{Q}(\zeta_8), \tag{1.5}$$

$$p = x^2 + 32y^2 \Leftrightarrow (p) \text{ splits completely in } \mathbf{Q}\left(\zeta_8, \sqrt{1 + \sqrt{2}}\right). \tag{1.6}$$

Here $\zeta_8 = \exp(2\pi i/8)$ is an 8th root of unity. The equivalences (1.4), (1.5) are consequences of class field theory over $\mathbf{Q}$, and (1.6) is a consequence of class field theory over $\mathbf{Q}(\sqrt{-2})$. ($\mathbf{Q}(\zeta_8, \sqrt{1 + \sqrt{2}})$ is the ring class field (mod(4)) over $\mathbf{Q}(\sqrt{-2})$. See [2] for a discussion of ring class fields.)

A consequence of conditions (1.4)–(1.6) is that the sets of primes they determine have a natural density. Let Σ_j denote the set of all primes p for which $2^j \mid h(-4p)$. The right sides of (1.4)–(1.6) imply that the sets Σ_1, Σ_2, and Σ_3 have natural densities $1/2$, $1/4$, and $1/8$, respectively, by an application of the Chebotarev density theorem [4], [17].

CHEBOTAREV DENSITY THEOREM. *Let K be a finite Galois extension of $\mathbf{Q}$, and C a conjugacy class of the Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Then the set of primes*

$$\Sigma(C) = \left\{(p): \left[\frac{K/\mathbf{Q}}{(p)}\right] = C\right\},$$

has a natural density which is equal to $|C|/|G|$.

Recall here that the *Artin symbol* $[(K/\mathbf{Q})/(p)]$ is a conjugacy class of the Galois group $\mathrm{Gal}(K/\mathbf{Q})$ defined for all primes $p \nmid d_K$, where d_K is the discriminant of K. It consists of those elements $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ for which there is a prime ideal P of K lying over (p) for which $x^\sigma \equiv x^p \pmod{P}$, for all algebraic integers x in K. The Chebotarev density theorem applies to the sets defined by the right side of (1.4)–(1.6) because the condition that (p) split completely in a normal extension K over $\mathbf{Q}$ is exactly that the Artin symbol $[(K/\mathbf{Q})/(p)]$ be the identity element in the Galois group $\mathrm{Gal}(K/\mathbf{Q})$.

The equivalences (1.1)–(1.6) lead us to ask the question: Under what circumstances can the set of primes p for which $C_2(dp)$ has a given structure G be described in terms of Artin symbol conditions in some algebraic number field? Here d is held fixed and p is allowed to vary. We must suppose that $d \not\equiv 2 \pmod 4$ in order that there be an infinite number of primes p for which $D = dp$ is a discriminant.

We conjecture this is always the case. In order to relate the conjectures to known results, we phrase them in terms of the quotient group $C_2(dp)/C_2(dp)^{2^j}$, i.e., in terms of the 2^k-invariants of $C_2(dp)$ for $1 \leqslant k \leqslant j$.

CONJECTURE $C_j(d)$. *Given the integer* $d \not\equiv 2 \pmod 4$, *there exists a normal extension* $K = K_j(d)$ *of* $\mathbf{Q}$ *having the following property* $P_j(d)$.

Property $P_j(d)$. *If* p_1 *and* p_2 *are primes such that* $[(K/\mathbf{Q})/(p_1)] = [(K/\mathbf{Q})/(p_2)]$, *then* $C_2(dp_1)$ *and* $C_2(dp_2)$ *have the same* 2^k*-invariants for* $1 \leqslant k \leqslant j$.

Using elementary group-theoretic and Galois-theoretic considerations, we prove the following result in Appendix A.

THEOREM 1.1. *If there exists some extension* K *with Property* $P_j(d)$, *then there exists a unique field* $\Omega_j(d)$ *of smallest degree with this property. Furthermore* $\Omega_j(d)$ *is a subfield of every field* K *having Property* $P_j(d)$.

We call such a field $\Omega_j(d)$ a *governing field*, since the Artin symbols $[(\Omega_j(d)/\mathbf{Q})/(p)]$ govern the structure of the group $C_2(dp)/C_2(dp)^{2^j}$.

If Conjecture $C_j(d)$ is true, then an application of the Chebotarev density theorem implies the truth of the following conjecture.

DENSITY CONJECTURE $D_j(d)$. *Given the integer* $d \not\equiv 2 \pmod 4$, *and an abelian 2-group* G *of exponent* $\leqslant j - 1$, *the set*

$$\Sigma_j(d, G) = \{(p) : C_2(dp) \cong G\}.$$

has a natural density which is equal to a rational number.

What evidence is there for these conjectures? First, Conjecture $C_1(d)$ is true for all $d \not\equiv 2 \pmod 4$. This follows from genus theory using class field theory over $\mathbf{Q}$; one can take $K_1(d) = \mathbf{Q}(\sqrt{-1})$. Second, Conjecture $C_2(d)$ is true for all $d \not\equiv 2 \pmod 4$. This follows from the Redei-Reichardt theorem and more class field theory over $\mathbf{Q}$; one can take for $K_2(d)$ the field $\mathbf{Q}(\sqrt{-1}, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_r})$, where the p_i are the distinct primes dividing $2d$. Third, Conjecture $C_3(d)$ is known to be true for some particular d. For $d = -4$, the equivalences (1.3) and (1.6) imply that $\Omega_3(-4) = \mathbf{Q}(\zeta_8, \sqrt{1 + \sqrt{2}})$. Conjecture $C_3(d)$ is also true for all those discriminants d to which the results of Redei [27] apply; his quartic residue symbol criteria can be used to find an appropriate field $K_3(d)$ using class field theory. More recently Morton [20]–[23]

has proved Conjecture $C_3(d)$ for an infinite set of squarefree d. Kaplan [10]–[12] has also derived criteria which we believe (but have not checked) can be used to prove Conjecture $C_3(d)$ for certain infinite classes of d, using class field theory.

The available methods of proof all break down for $j \geq 4$. They give no indication whether or not Conjecture C_4 is true for *any* d.

This paper describes the results of a search for numerical evidence supporting these conjectures. First, we tested the Density Conjecture $D_j(d)$ for $d = -4$ and 8, where $C_2(dp)$ is always a cyclic group, by examining large tables of class numbers. We accumulated data for $d = -4$ and empirically observed that the densities of the sets Σ_j on an initial segment of primes were close to $1/2^j$ for $4 \leq j \leq 7$, in particular, close to $1/16$ for $16 \mid h(-4p)$. In addition there exist fast algorithms for computing $C_2(D)$ without computing $C(D)$. (The basic algorithm of this type is due to Shanks [33]. See [14] for additional references and a computational complexity analysis of one such algorithm.***) We give data for $d = 8$ extracted from a table of Kaplan and Sanchez [13] computed using such an algorithm. Here the densities of the sets $\Sigma_j(8)$ of primes with $2^j \mid h(8p)$ on an initial segment of primes were close to $1/4^j$ for $4 \leq j \leq 7$. (The densities $1/4^j$ for $1 \leq j \leq 3$ are known to exist.)

Second, we examined Conjecture $C_3(d)$ for the simplest case $d = -21$ which is not yet known to be true. Section 3 describes our search for $\Omega_3(-21)$. Guided by analogy with existing results, we located a field K for which there is overwhelming numerical evidence that $\Omega_3(-21) \subseteq K$. This example convinces us that Conjecture C_3 is true for all $d \not\equiv 2 \pmod 4$.

Third, we examined Conjecture $C_4(-4)$. Section 4 describes our search for a field $\Omega_4(-4)$ extending the equivalences (1.1)–(1.6). We obtained negative results, ruling out all candidate fields of degree 16 ramifying only at (2), and certain fields of degree 32. Section 5 suggests new directions to pursue in a search for $\Omega_4(-4)$. At present we do not have any direct evidence for the truth of Conjecture $C_4(-4)$.

P. Morton has observed that the available evidence supports conjectures somewhat stronger than Conjecture $C_j(d)$. First, in all known cases the splitting behavior of (p) in $\Omega_j(d)$ and its subfields determines the 2^k-invariants of $C_2(dp)$ for $1 \leq k \leq j$. This assertion can be formulated in Galois-theoretic terms, as follows. We say that elements σ_1, σ_2 of a group G are in the same *division* if there is an element $\tau \in G$ and an integer m relatively prime to $\operatorname{ord}(\sigma_2)$ such that $\sigma_1 = \tau(\sigma_2)^m\tau^{-1}$. (This term is a translation of the name *Abteilung* used by Frobenius for the same concept.) The divisors of a group G are disjoint unions of conjugacy classes. It can be shown that the division that $[(K/\mathbf{Q})/(p)]$ is in determines how (p) splits in all the subfields of K, and conversely. (See [16, Theorem 1.2].) We let $\{(K/\mathbf{Q})/(p)\}$ denote the division of $\operatorname{Gal}(K/\mathbf{Q})$ containing $[(K/\mathbf{Q})/(p)]$.

Second, Morton observed that in the case of positive discriminants D with $D \equiv 0 \pmod 4$, the conjecture can be extended to include the solvability of the anti-Pellian equation $X_1^2 - DX_2^2/4 = -1$. More generally, if we define for a positive nonsquare

*** The second author takes this opportunity to remark that a footnote on p. 374 of Morton [19] unfortunately suggests that the use of Gauss' ternary form algorithm in an algorithm to calculate $C_2(d)$ was first proposed in [14]. This idea is due to D. Shanks [33].

discriminant the identity form $Q_D(x_1, x_2)$ by

$$Q_D(x_1, x_2) = \begin{cases} x_1^2 - \dfrac{D}{4}x_2^2 & \text{if } D \equiv 0 \pmod 4, \\ x_1^2 + x_1x_2 - \dfrac{D-1}{4}x_2^2 & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

then it is known that the equation

$$Q_D(x_1, x_2) = D^*, \qquad (x_1, x_2) = 1,$$

is solvable for exactly two values of D^* with $D^* \neq 1$, D and D^* dividing D. Furthermore the product of these two values is D. Consequently, if $D = dp$ with $(p, d) = 1$, there is a unique such D^* with $D^* \mid d$. In this case we denote this value by $d^*(d, p)$. For example, $d^*(d, p) = -1$ if and only if the anti-Pellian equation for dp is solvable. Morton conjectures there is a field where prime-splitting conditions determine $d^*(d, p)$ for each fixed 2-classgroup.

We may formulate Morton's observations as follows.

CONJECTURE $C_j^*(d)$. *Given the integer $d \not\equiv 2 \pmod 4$, there is a finite Galois extension $K_* = K_j^*(d)$ of $\mathbf{Q}$ with the following properties $P_j^*(d)$ and $U_j^*(d)$.*

Property $P_j^*(d)$. If two primes p_1, p_2 have Artin symbols lying in the same division of $\mathrm{Gal}(K^*/\mathbf{Q})$, *i.e.* $\{(K^*/\mathbf{Q})/(p_1)\} = \{(K^*/\mathbf{Q})/(p_2)\}$, *then $C_2(dp_1)$ and $C_2(dp_2)$ have the same 2^k-invariants, for $1 \leq k \leq j$.*

Property $U_j^*(d)$. If $d > 0$, and $\{(K^*/\mathbf{Q})/(p_1)\} = \{(K^*/\mathbf{Q})/(p_2)\}$, and $C_2(dp_1)$ and $C_2(dp_2)$ have 2^j-invariant zero, then $d^*(d, p_1) = d^*(d, p_2)$.

As with Conjecture $C_j(d)$, it can be shown that if a field $K_j^*(d)$ exists, then there is a unique field $\Omega_j^*(d)$ with the same properties which is a subfield of all such fields $K_j^*(d)$. (See Appendix A.)

It is conceivable that further insight into these conjectures may be gained by more explicit knowledge about the Hilbert 2-class fields of $\mathbf{Q}(\sqrt{dp})$; cf. [5], [6], [7].

Finally we remark that it is possible to formulate analogues of Conjecture $C_j(D)$ concerning the structure of the l-classgroup of cyclic l-extensions of $\mathbf{Q}$, where l is an odd prime.

We formulated the conjectures of this paper (in a less precise form) in early 1978, and proved Theorem 4.2 at that time. We described our results to P. Morton in 1979 and suggested that Conjecture $C_3(d)$ could be proved for all $d \not\equiv 2 \pmod 4$. This led to his work [20]–[23]. The precise form of the conjectures stated in this paper would not have been made without Pat Morton's contributions; we are grateful to him for helpful conversations. Some of the results of this paper were announced in [8].

2. Numerical Data on Densities. We examined the Density Conjecture for $d = -4$ using a table of class numbers $h(-d)$ for $d < 150{,}000$. In this case $C_2(-4p)$ is cyclic, so one needs only to find the value of j such that $2^j \| h(-4p)$. Since the Density Conjecture $D_3(-4)$ is known to be true in this case, we only tabulated primes p for which $8 \mid h(-4p)$. Table 1 presents the observed counts of primes with $2^j \| h(-4p)$, where the counts were done in blocks of 100. At the bottom of the table we give the expected values of the counts, assuming conjectural densities of $1/2^j$ for $4 \leq j \leq 7$,

and we compare this with the observed average value of the counts. The agreement of the data with these conjectured densities is good. The density fluctuations in the blocks of 100 are well within the ranges one would expect if there exist governing fields $\Omega_j(-4)$ for $4 \leqslant j \leqslant 7$.

TABLE 1

Primes p for which $2^j \| h(-4p)$, *counted in blocks of* 100 *primes for which* $8 \mid h(-4p)$.

Block	8	16	32	64	128	≥ 256
100	62	20	16	2	0	0
200	52	28	14	5	1	0
300	47	26	15	9	2	1
400	50	25	17	4	2	2
500	45	32	13	7	3	0
600	55	23	13	3	5	1
700	39	26	20	9	6	0
800	44	29	16	7	4	0
900	48	23	13	8	3	5
1000	46	30	13	5	5	1
1100	56	20	12	5	4	3
1200	47	23	20	6	4	0
1300	50	26	12	5	4	3
1400	48	27	14	7	3	1
1500	46	27	12	7	5	3
1600	52	30	7	6	2	3
1700	48	29	10	2	4	7
Expected Value	50.0	25.0	12.5	6.25	3.13	3.13
Observed	49.1	26.1	13.9	5.71	3.35	1.77

We examined the Density Conjecture for $d = 8$ using the table of Kaplan and Sanchez [13]. They computed the 2-class number of $\mathbf{Q}(\sqrt{2p})$ for $p < 2{,}000{,}000$ for which $8 \mid h(8p)$, using a special purpose algorithm; see [33], [13]. In this case again $C_2(8p)$ is cyclic; the densities are known to exist and to be $1/4^j$ for the sets of primes with $2^j \mid h(8p)$ for $k = 1$, 2 and 3. Table 2 presents counts for such primes done in blocks of 1000. At the bottom of the table we give the expected values of the counts, assuming conjectured densities of $3/4^j$ for $2^j \| h(8p)$ for $4 \leqslant j \leqslant 7$. Kaplan and Sanchez [13] have conjectured that the three sets of primes p with $2^j \| h(8p)$ and $x_1^2 - 2px_2^2 = -1$, 2 and -2, respectively, each have density $1/4^j$. The data agree well with these conjectured densities.

Table 3 gives the least primes p for which $2^j \| h(-4p)$, for $1 \leqslant j \leqslant 9$. Table 4 lists the least primes p for which $2^j \| h(8p)$ and for which a particular equation $x_1^2 - 2px_2^2 = D^*$ is solvable, where $D^* = -1$, 2 or -2.

TABLE 2

Primes p for which $2^j \| h(8p)$, *counted in blocks of* 1000 *primes such that* $8 \mid h(8p)$.

Block	8	16	32	64	128	≥ 256
1000	768	199	42	11	0	0
2000	764	186	43	5	2	0
3000	763	182	47	6	2	0
4000	777	167	41	12	3	0
5000	758	174	57	10	1	0
6000	748	193	50	7	2	0
7000	742	192	51	13	0	2
8000	746	199	45	7	2	1
9000	777	179	34	8	2	0
Expected Value	750	187.5	46.88	11.72	2.93	0.98
Observed	760.3	185.7	45.56	8.78	1.56	0.55

TABLE 3

The smallest prime p for which $2^j \| h(-4p)$.

2^j	D
2	5
4	17
8	41
16	257
32	521
64	4481
128	9521
256	21929
512	72089

TABLE 4

The smallest primes p for which $2^j \| h(8p)$ *and* $X^2 - 2pY^2 = -1, 2$ *or* -2 *is solvable*.

2^j	-1	2	-2
2	5	7	3
4	41	17	73
8	113	337	257
16	3089	3361	1217
32	12641	25409	23041
64	50753	120977	27953
128	675569	206081	243137
256	1410977	1566449	1408961

3. The Governing Field $\Omega_3(-21)$. Conjecture $C_3(d)$ has been proved for all d in which the 2-classgroup is cyclic; see [23]. In addition Morton [20] has proved Conjecture $C_3(d)$ for $d = -p_1 p_2 \cdots p_k$, where all $p_i \equiv 1 \pmod 4$ and all $(p_i/p_j) = 1$. The simplest case left open is $d = -21$.

We searched for a field $\Omega_3(\sqrt{-21})$ governing the structure C/C^8 of the fields $\mathbf{Q}(\sqrt{-21p})$, where p runs over primes $p \equiv 3 \pmod 4$. In this case the 2-classgroup of $\mathbf{Q}(\sqrt{-21p})$ has the structure $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2^j\mathbf{Z}$ for some $j \geq 1$. To analyze the structure of this group further, we use the language of quadratic forms. Table 5 gives (ambiguous) forms Q_3, Q_7 and Q_{21} which are representative of the three nontrivial form classes of order 2 of discriminant $-21p$. There are two genus characters χ_{-3}, χ_{-7} given by the Kronecker symbols $(-3/\cdot)$ and $(-7/\cdot)$. Table 5 also gives the values of these characters on these forms calculated using the quadratic reciprocity law. From Table 5 one sees that the class $[Q_3]$ is never the square of an ideal class, the class $[Q_{21}]$ is a square if and only if $(-3/p) = (-7/p) = 1$, i.e. (p) splits completely in $\mathbf{Q}(\sqrt{-3}, \sqrt{-7})$, and the class $[Q_7]$ is a square if and only if $(7/p) = 1$, i.e. (p) splits completely in $\mathbf{Q}(\sqrt{7})$.

TABLE 5

Ambiguous forms and genus characters for discriminants $D = -21p, p \equiv 3 \pmod 4$.

			χ_{-3}	χ_{-7}
Q_3	=	$3x^2 + 3xy + \frac{7p+3}{4}y^2$	$\left(\frac{p}{3}\right)$	-1
Q_7	=	$7x^2 + 7xy + \frac{3p+7}{4}y^2$	1	$-\left(\frac{p}{7}\right)$
Q_{21}	=	$21x^2 + 21xy + \frac{p+21}{4}y^2$	$\left(\frac{p}{3}\right)$	$\left(\frac{p}{7}\right)$

From Table 5 we infer that $\Omega_2(-21) = \mathbf{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{7})$. Here $\sqrt{-1}$ is present to guarantee the Artin symbols of $\Omega_2(-21)$ separate primes $p \equiv 1 \pmod 4$ from primes $p \equiv 3 \pmod 4$.

Table 6 presents numerical data on the 2-class number of $\mathbf{Q}(\sqrt{-21p})$ for $21p < 250{,}000$. The primes are grouped in four columns according to the signs of the genus characters χ_{-3}, χ_{-7}. Table 6 also specifies the fields in which primes $p \equiv 3 \pmod 4$ having the given genus character values split completely. (The 2-class number of $\mathbf{Q}(\sqrt{-21p})$ for those p in the third column is always 4.) We hoped that the hypothetical field $\Omega_3(-21)$ would be a compositum of certain ring class fields, i.e. that the splitting of primes in $\Omega_3(-21)$ could be described in terms of representation by quadratic forms, whose discriminants divide some power of 4.21. (This is suggested by analogy with the result of Barrucand and Cohn [1] and Morton's results.) This is indeed so, in the sense that the numerical data is consistent with:

$$16 \mid h(-21p) \Leftrightarrow \text{(A) or (B) or (C) below holds,}$$

TABLE 6

2-class numbers of $\mathbf{Q}(\sqrt{-21\,p})$, $p \equiv 3 \pmod 4$.

χ_{-3}	1		1		-1		-1	
χ_{-7}	1		-1		1		-1	
Splitting Field	$Q(\sqrt{-3},\sqrt{-7})$		$Q(\sqrt{-3},\sqrt{7})$		$Q(\sqrt{3},\sqrt{-7})$		$Q(\sqrt{3},\sqrt{7})$	
	p	$\lvert C_2\rvert$	p	$\lvert C_2\rvert$	p	$\lvert C_2\rvert$	p	$\lvert C_2\rvert$
	43	16	19	16	11	4	47	8
	67	8	31	8	23	4	59	32
	79	8	103	8	71	4	83	8
	127	8	139	8	107	4	131	8
	151	16	199	16	179	4	167	8
	163	8	223	16	191	4	227	32
	211	16	271	8	239	4	251	64
	331	16	283	32	263	4	311	8
	379	16	307	16	347	4	383	16
	463	8	367	16	359	4	419	16
	487	16	439	16	431	4	467	64
	499	32	523	8	443	4	479	8
	547	8	607	16	491	4	503	16
	571	8	619	8	599	4	563	16
	631	8	643	64	659	4	587	16
	739	8	691	8	683	4	647	8
	751	32	727	8	743	4	719	32
	823	8	787	8	827	4	839	8
	883	16	811	8	863	4	887	8
	907	64	859	128	911	4	971	8
	919	32	1039	16	947	4	983	32
	967	8	1063	8	1019	4	1091	8
	991	32	1123	8	1031	4	1151	16
	1051	8	1231	32	1103	4	1223	8
	1087	8			1163	4		
	1171	128			1187	4		

where

$$\text{(A)}\quad \left(\frac{-3}{p}\right) = \left(\frac{-7}{p}\right) = 1 \quad \text{and} \quad p = 7x^2 + 36y^2,$$

$$\text{(B)}\quad \left(\frac{-3}{p}\right) = 1, \left(\frac{-7}{p}\right) = -1 \quad \text{and} \quad p = 7x^2 + 12y^2,$$

$$\text{(C)}\quad \left(\frac{-3}{p}\right) = \left(\frac{-7}{p}\right) = -1 \quad \text{and} \quad p = 84x^2 - y^2.$$

It is well known that there exist fields called *ring class fields* whose Artin symbols separate primes represented by classes of quadratic forms of a fixed discriminant;

see [2], [16]. In this case there are fields K_A, K_B, K_C such that the primes $p \equiv 3 \pmod 4$ that split completely in these fields are exactly the primes specified by (A), (B), (C), respectively. They are:

$$K_A = \mathbf{Q}\left(\sqrt{-3}, \sqrt{-7}, \sqrt{-2\left(3+\sqrt{21}\right)}\right),$$

$$K_B = \mathbf{Q}\left(\sqrt{-3}, \sqrt{7}, \sqrt{1+2\sqrt{7}}\right),$$

$$K_C = \mathbf{Q}\left(\sqrt{3}, \sqrt{7}, \sqrt{2\left(7+\sqrt{21}\right)}\right).$$

(These fields also contain primes $p \equiv 1 \pmod 4$ that split completely.) These three fields are subfields of the ring class fields of discriminants -12.84, -4.84, 4.84, respectively.

This evidence leads us to the following conjecture.

CONJECTURE. *The governing field* $\Omega_3(-21)$ *exists and is a subfield of*

$$\mathbf{Q}\left(\sqrt{-1}, \sqrt{3}, \sqrt{7}, \sqrt{-2\left(3+\sqrt{21}\right)}, \sqrt{1+2\sqrt{7}}, \sqrt{2\left(7+\sqrt{21}\right)}\right).$$

4. The Governing Field $\Omega_4(-4)$. Conjecture $C_3(d)$ has been proved for an infinite set of $d \not\equiv 2 \pmod 4$. By contrast Conjecture $C_4(d)$ has not been proved for even a single $d \not\equiv 2 \pmod 4$.

In order to produce numerical support for Conjecture $C_4(-4)$, we searched for the hypothetical governing field $\Omega_4(-4)$. We were guided by analogy with the known governing fields $\Omega_j(d)$ with $j \leq 3$. These suggest the following two working hypotheses concerning $K = \Omega_4(-4)$.

(H1) K is normal over $\mathbf{Q}$ and $[K:\mathbf{Q}] = 16$.

(H2) The discriminant of K is 2^k, for some k, i.e. K ramifies only over the ideal (2).

Evidence favoring (H1) is given by the pattern of fields (1.4)–(1.6) and by the fact that those p with $16 \mid h(-p)$ appear to have natural density $1/16$, as described in Table 3. Evidence favoring (H2) is that all known governing fields $\Omega_j(d)$ ramify only at primes dividing $2d$.

There are only a finite number of fields K satisfying (H1), (H2). This is a consequence of the following fact, which has been known in principle since the 1920's. We indicate a proof for the reader's convenience.

THEOREM 4.1. *For any positive integer N and any finite set of primes $S = \{p_1, \ldots, p_k\}$ there are only a finite number of algebraic number fields K such that*:

(i) $[K:\mathbf{Q}] = N$.

(ii) *All primes p dividing the discriminant d_K are in S.*

Proof. Using the theory of the different and higher ramification groups, one can obtain a bound $B(N, p)$ such that if $p^j \| d_K$, then $j \leq B(N, p)$ for all fields K of degree N over $\mathbf{Q}$. Ore [25] showed that if $N = b_0 + b_1 p + b_2 p^2 + \cdots + b_m p^m$ with $0 \leq b_m \leq p-1$ and if A denotes the number of nonzero b_i, then one can take $B(N, p) = b_0 + 2b_1 p + \cdots + (m+1)b_m p^m - A$, and that this bound is sharp. We conclude that condition (ii) implies

$$d_K \mid D = \prod_{p \in S} p^{B(N,p)}.$$

Hence $d_K \leqslant D$. Theorem 4.1 then follows from the well-known fact that only a finite number of algebraic number fields can have the same discriminant (cf. Narkiewicz [24, Theorem 2.11]). □

Since there are only a finite number of fields K satisfying (H1), (H2), it is possible to test for each K whether or not $K = \Omega_4(-4)$. We obtained the following result.

THEOREM 4.2. *Let K be a field such that*
(i) *K is a normal extension of $\mathbf{Q}$ of degree* 16.
(ii) *K ramifies only over* (2).
Then $K \neq \Omega_4(-4)$.

We give two proofs of this theorem.

First Proof. In order that $K = \Omega_4(-4)$ we must have $\Omega_3(-4) = \mathbf{Q}(\zeta_8, \sqrt{1+\sqrt{2}})$ be a subfield of K; we assume that in the remainder of the proof. Then K is Galois over $\mathbf{Q}(\zeta_8)$ with Galois group G of order 4. Then G is abelian, and so all possible K are specified by class field theory over $\mathbf{Q}(\zeta_8)$.

Class field theory asserts that for an abelian extension K/k the prime ideals that split completely from k to K are those belonging to a certain subgroup of a ray classgroup modulo a certain conductor $\mathrm{cond}(K/k)$. In our case assumption (ii) implies that the conductor involves only prime ideals lying over (2) in $\mathbf{Q}(\zeta_8)$. Now $\mathbf{Q}(\zeta_8)$ has unique factorization and in it $(2) = (\pi_2)^4$ totally ramifies, and we can take $\pi_2 = 1 + \zeta_8$. Hence $\mathrm{cond}(K/k) = (\pi_2)^m$ for some integer m.

FACT 1. *All fields K containing $\mathbf{Q}(\zeta_8, \sqrt{1+\sqrt{2}})$ and satisfying* (i), (ii) *have conductor $(\pi_2)^m$ for some $m \leqslant 12$ over $\mathbf{Q}(\zeta_8)$.*

We defer the proof of Fact 1. Assuming it is true, we may conclude that any two prime ideals $\mathbf{Q}(\zeta_8)$ in the same ray class $(\mathrm{mod}^*(\pi_2)^{12})$ must have the same Artin symbol in *each* field K satisfying (i), (ii). We can show that no such K is $\Omega_4(-4)$ by exhibiting two such ideals (π_{p_1}) and (π_{p_2}) of norms p_1 and p_2, respectively, such that $8 \| h(-p_1)$ and $16 \mid h(-p_2)$. Indeed we have

$$\pi_{593} = -11 + 12\zeta_8^2 + 16\zeta_8^3, \qquad N(\pi_{593}) = 593,$$
$$\pi_{8273} = -11 - 8\zeta_8 - 4\zeta_8^2 + 8\zeta_8^3, \qquad N(\pi_{8273}) = 8273,$$

with $h(-593) = 24$, $h(-8273) = 64$. It is immediate that

$$\pi_{593} \equiv \pi_{8273} \pmod{(8)}$$

are in the same ray class with conductor $(\pi_2)^{12}$. The theorem follows.

It remains to prove Fact 1. To do this we explicitly determine all such extensions K. Then for each K we bound its conductor, using the conductor-discriminant formula of Hasse [9] and relative different calculations.

To determine all such fields, we use the fact that they are all Kummer extensions, since $\mathbf{Q}(\zeta_8)$ contains the 4th roots of unity. We use the already mentioned fact that $\mathbf{Q}(\zeta_8)$ has class number one (proved using the Minkowski discriminant bound), and the known factorization $(2) = (\pi_2)^4$. We also need generators for the unit group $\mathbf{U}$ of $\mathbf{Q}(\zeta_8)$.

FACT 2. $\mathbf{U} = \langle \varepsilon, \zeta_8 \rangle$, *where* $\varepsilon = 1 + \sqrt{2}$.

It is a well-known fact that unit groups of cyclotomic fields are generated by the real units and the roots of unity. In this case the real subfield of $\mathbf{Q}(\zeta_8)$ is $\mathbf{Q}(\sqrt{2})$, and Fact 2 follows.

Let $k_0 = \mathbf{Q}(\zeta_8)$. The information above implies that all such K have either the form $k_0(\sqrt[4]{\mu})$, where μ has norm 1, 2, 2^2 or 2^3, or the form $k_0(\sqrt{\mu_1}, \sqrt{\mu_2})$, where $\mu_1 = 1 + \sqrt{2}$ and μ_2 has norm 1 or 2. Recalling that $\pi_2 = 1 + \zeta_8$, the complete list is:

Cyclic 4-extensions. $K = k_0(\sqrt[4]{\mu})$, where $\mu = (1 + \sqrt{2})\theta^2$ and $\theta = 1, \zeta_8, \pi_2, \zeta_8\pi_2$.

Noncyclic 4-extensions. $K = k_0(\sqrt{1 + \sqrt{2}}, \sqrt{\mu})$, where $\mu = \zeta_8, \pi_2, \zeta_8\pi_2$.

We now bound the conductors of these fields, making use of Hasse's conductor-discriminant relation [9]. We need here three special cases of his formula.

(a) If K/k is a quadratic extension, then

$$\operatorname{cond}(K/k) = D_{K/k}.$$

(b) If K/k is cyclic of degree 4 with an intermediate quadratic extension k_1, then

$$D_{K/k} = (\operatorname{cond}(K/k))^2 D_{k_1/k}.$$

(c) If K/k is a noncyclic abelian extension of degree 4 with intermediate quadratic extensions k_1, k_2, k_3, then

$$\operatorname{cond}(K/k) = \text{l.c.m.}\,(\operatorname{cond}(k_i/k)).$$

We will also compute relative differents ($\delta_{K/k}$) of quadratic extensions and make use of the relation

$$D_{K/k} = N_{K/k}(\delta_{K/k}). \tag{4.1}$$

valid in such a case. The relative different $\delta_{K/k}$ of a quadratic extension $K = k(\sqrt{\mu})$ is bounded by

$$\delta_{K/k} \mid \left(2\sqrt{\mu}\right), \tag{4.2}$$

using the polynomial $f(x) = x^2 - \mu$ and $f'(\sqrt{\mu}) = 2\sqrt{\mu}$; cf. Lang [18, p. 62].

For $k_1 = k_0(\sqrt{1 + \sqrt{2}})$ we obtain the sharper bound

$$\delta_{k_1/k_0} \mid (\pi_2)^3. \tag{4.3}$$

Take $\theta = (1 + \sqrt{1 + \sqrt{2}})/(1 - \zeta_8)$, an integer in k_1 satisfying $x^2 - (2/(1 - \zeta_8))x - \theta\theta' = 0$, where θ' is the conjugate of θ. Then

$$(f'(\theta)) = \left(\frac{2}{1 - \zeta_8}\sqrt{1 + \sqrt{2}}\right) = (\pi_2)^3,$$

as an ideal in k_1. This proves (4.3). (In fact $\delta_{k_1/k_0} = (\pi_2)^3$ in this case.) From fact (a) we get

$$\operatorname{cond}(k_1/k_0) = D_{k_1/k_0} \mid (\pi_2)^6. \tag{4.4}$$

Next let $k_2 = k_0(\sqrt{\zeta_8})$, $k_3 = k_0(\sqrt{\pi})$, $k_4 = k_0(\sqrt{\zeta_8\pi})$. Using (4.2), we have $\operatorname{cond}(k_i/k_0) \mid (\pi_2)^9$, in all three cases. Then, using (c), we obtain $\operatorname{cond}(K/k_0) \mid (\pi_2)^9$, if $\operatorname{Gal}(K/k_0)$ is a noncyclic group of order 4.

The cyclic 4-extension case remains. We first bound D_{K/k_1} by bounding the different δ_{K/k_1} via (4.2) for all four possible fields K and then using (4.1). We obtain

$$D_{K/k_1} \mid (4\pi_2). \tag{4.5}$$

Next we use the relation (cf. Ribenboim [32, p. 213]),

$$D_{K/k_0} = \left(D_{k_1/k_0}\right)^2 N_{k_1/k_0}\left[D_{K/k_1}\right].$$

Letting $D_{k_1/k_0} = (\pi_2)^a$, where $a \leqslant 6$ by (4.4), we obtain

$$D_{K/k_0} \mid (\pi_2)^{2a}\left(16\pi_2^2\right) = (\pi_2)^{18+2a}.$$

Then, using Hasse's formula (b), we obtain

$$\operatorname{cond}(K/k_0) \mid (\pi_2)^{(18+a)/2}.$$

Since $\operatorname{cond}(K/k_0) = (\pi_2)^b$ for an integer b and $a \leqslant 6$, this implies $b \leqslant 12$, finishing the proof. □

We remark that with slightly more work the bound on the conductor $(\pi_2)^m$ in Fact 1 can be sharpened to $m \leqslant 11$. We use the fact that in k_1 the ideal $(2) = (\Lambda)^8$, where

$$\Lambda = \frac{1}{\sqrt{1+i}} - \frac{\zeta_8}{1+\zeta_8}.$$

Thus in k_1 we have $\pi_2 = \eta\Lambda^2$ for some unit η in k_1. Consequently the cyclic 4-extensions of k_0 are given by $K = k_1(\sqrt{\mu})$, where $\mu = (\sqrt{1+\sqrt{2}})\alpha$, where $\alpha = 1$, $\zeta_8, \eta, \eta\zeta_8$. Using (4.2) with these μ, we may replace (4.5) by

$$D_{K/k_1} \mid (4).$$

Using this improved bound in the proof above leads to $m \leqslant 11$.

This first proof depended on finding suitable prime elements π_{593} and π_{8273}. Once they were found, it was straightforward to verify that they have the required properties. We found π_{593} using Reuschle's tables [31] and located π_{8273} by a computer search.

The second proof is more direct, but involves more computation than the first proof.

Second Proof. (Sketch) We determine all possible fields K with $\mathbf{Q}(\zeta_8, \sqrt{1+\sqrt{2}})$ as a subfield, normal over $\mathbf{Q}(\zeta_8)$, which ramify only over (2), as in the first proof.

For each such field we determined on a computer which primes $p < 2500$ split completely. These are given in Table 7. Primes that split completely are exactly the primes whose Artin symbol is the identity element. To show $K \neq \Omega_4(-4)$, it suffices to locate two primes p_1 and p_2 that split completely, such that $8 \| h(-p_1)$, and $16 \mid h(-p_2)$. This can be done for each field K using Table 7. (Note that (593) splits completely in all seven candidate fields; this provides a consistency check on the first proof.)

The data in Table 7 was calculated using the fact that conditions for a prime (p) to split completely in a field K can be expressed in terms of the factorization (mod p) of a monic polynomial $f(x) = 0$ whose root generates the field (Lang [18, p. 27]).† In this case the fields are generated by a series of square-root adjunctions, and we can convert the condition that (p) split completely into the solvability of a series

† More precisely, this is true except for a finite set of exceptional primes, which are the primes $p \mid \operatorname{Disc}(f(x))$. The only exceptional prime for the seven candidate fields we tested was (2).

of square root extractions (mod p). For example, for $K = \mathbf{Q}(\zeta_8, \sqrt[4]{1+\sqrt{2}})$, if $p \neq 2$, then the ideal (p) splits completely in K if and only if the following system of congruences can be solved (mod p):

$$
\begin{aligned}
x_1^2 &\equiv -1 && (\text{mod } p),\\
x_2^2 &\equiv x_1 && (\text{mod } p),\\
x_3^2 &\equiv 1 + x_2 + (x_2)^{-1} && (\text{mod } p),\\
x_4^2 &\equiv x_3 && (\text{mod } p).
\end{aligned} \tag{4.6}
$$

(Here x_1, x_2, x_3, x_4 play the role of $\sqrt{-1}$, ζ_8, $\sqrt{1+\sqrt{2}}$ and $\sqrt[4]{1+\sqrt{2}}$, respectively, in $\mathbf{Z}/p\mathbf{Z}$.) We derived a system of successive square-root extractions (mod p) like (4.6) for each of the seven candidate fields K and used a well-known fast algorithm for extracting square roots (mod p) (see [34]) to compute the data given in Table 7. □

TABLE 7

Primes $p < 2500$ that split completely in fields of degree 16 which are Galois over $k_0 = \mathbf{Q}(\zeta_8)$.

Test Primes	Noncyclic $K = k_0(\sqrt{1+\sqrt{2}}, \sqrt{\mu})$			Cyclic $K = k_0(\sqrt[4]{(1+\sqrt{2})\mu^2})$			
	(μ)			(μ)			
$16\|h(-p)$	π_2	ζ_8	$\zeta_8\pi_2$	1	π_2	ζ_8	$\zeta_8\pi_2$
257	337	113	41	41	113	137	41
409	457	257	137	313	137	353	113
521	521	337	313	353	257	521	257
569	569	353	337	409	457	569	313
809	577	577	409	457	593	593	409
857	593	593	577	593	761	857	521
953	761	881	593	761	809	953	569
1129	809	1153	881	809	1129	1153	593
1153	857	1201	1201	1129	1201	1201	857
1201	881	1217	1217	1153	1217	1217	953
1217	953	1249	1321	1201	1249	1321	1201
1249	1129	1553	1553	1217	1321	1601	1217
1657	1201	1601	1657	1601	1993	1777	1249
2113	1217	1777	1889	1657	2113	1993	1657
2137	1553	1889	1993	1777	2129	2113	2113
2153	1889	2113	2113	2113	2137	2129	2129
2273	2113	2129	2129	2129		2153	2153
2377	2129	2273	2297	2137		2273	2297
	2137			2273		2377	2377
	2153			2297			
	2377						

Theorem 4.2 shows we must abandon at least one of the hypotheses (H1), (H2). We considered replacing hypothesis (H1) by:

(H1*) K is normal over $\mathbf{Q}$ and $[K:\mathbf{Q}] = 2^j$ for some $j \geq 5$.

We retained hypothesis (H2); Section 5 presents some further evidence suggesting (H2) is true.

Theorem 4.1 shows that there are only a finite number of fields satisfying (H1*), (H2) that have $j \leq N$, for a fixed N. Their number grows rapidly with increasing N. It is a difficult matter to obtain a complete list of such fields for any $N \geq 6$.

We examined certain fields of degree 32 satisfying (H1*), (H2) suggested by the following theorem of K. S. Williams [37].

TABLE 8

Primes $p < 2500$ that split completely in certain fields of degree 32 that are cyclic extensions of $\mathbf{Q}(\zeta_{16})$, given by $K = \mathbf{Q}\left(\zeta_{16}, \sqrt[4]{2\mu^2}\right)$.

Test Primes	1	Ω_2	Ω_3	$\Omega_2\Omega_3$	π_2	$\pi_2\Omega_2$	$\pi_2\Omega_3$	$\pi_2\Omega_2\Omega_3$
257	257	113	353	113	257	113	337	113
1153	337	337	593	257	353	881	577	257
1201	881	353	1153	577	577	1553	881	337
1217	1217	577	1201	881	593	1777	1153	353
1249	1249	593	1217	1153	1201	1889	1217	593
2113	1553	1201	1601	2129	1217		1249	1153
2273	1777	1249	1777	2273	1553		1889	1201
	2113	1553	2113		1601		2113	1249
		1601	2129		1889		2129	1601
			2273		2113		2273	1777
								1889
								2129
								2273

ζ_{16}	$\zeta_{16}\Omega_2$	$\zeta_{16}\Omega_3$	$\zeta_{16}\Omega_2\Omega_3$	$\zeta_{16}\pi_2$	$\zeta_{16}\pi_2\Omega_2$	$\zeta_{16}\pi_2\Omega_3$	$\zeta_{16}\pi_2\Omega_2\Omega_3$
113	353	113	257	113	337	113	257
257	577	337	337	257	593	577	353
593	881	353	577	337	1201	593	881
1201	1249	881	593	353	1889	1153	1153
1217	1601	1153	1153	579	2129	1201	1249
1249	1777	1217	1201	881		1217	1553
2113	2129	1553	1553	1217		1249	1601
2129		1601	1777	1601		1553	1889
		2113	2273	1777		1777	2273
		2273		1889		1889	
				2113		2113	
				2129		2273	

THEOREM. *If* $p \equiv 1 \pmod 8$, *then* $h(-p) \equiv t + p - 1 \pmod{16}$, *where* $\varepsilon_p = t + u\sqrt{p}$ *is the fundamental unit of norm* -1 *in* $\mathbf{Q}(\sqrt{p})$.

This theorem suggests that the congruence class (mod 16) of p may be a relevant variable in determining when $16 \mid h(-p)$, i.e. that $\mathbf{Q}(\zeta_{16}) \subseteq \Omega_4(-4)$. We obtained the following negative result.

TABLE 9

Primes $p < 2500$ *that split completely in certain fields of degree* 32 *that are noncyclic Galois extensions of* $\mathbf{Q}(\zeta_{16})$, *given by* $K = \mathbf{Q}\left(\zeta_{16}, \sqrt[4]{2}, \sqrt{\mu}\right)$.

Test Primes	Ω_2	Ω_3	$\Omega_2\Omega_3$	π_2	$\pi_2\Omega_2$	$\pi_2\Omega_3$	$\pi_2\Omega_2\Omega_3$
257	337	113	257	113	353	113	257
1153	1153	577	353	257	577	337	337
1201	1249	1217	593	1153	593	353	577
1217	1553	1777	881	1217	881	593	1249
1249	1889	1889	1201	1553	1153	881	1777
2113	2129	2113	1601	2113	1201	1201	
2273	2273		1889	2129	1553	1217	
				2273	1601	1249	
					1777	1601	
					2129	2113	
					2273		

ζ_{16}	$\zeta_{16}\Omega_2$	$\zeta_{16}\Omega_3$	$\zeta_{16}\Omega_2\Omega_3$	$\zeta_{16}\pi_2$	$\zeta_{16}\pi_2\Omega_2$	$\zeta_{16}\pi_2\Omega_3$	$\zeta_{16}\pi_2\Omega_2\Omega_3$
257	113	337	113	257	113	353	113
353	593	577	257	337	337	1217	257
577	881	593	337	593	353	1249	577
1153	1153	881	353	881	577	1553	593
1217	1201	1201	1553	1153	1153	1601	881
1249	1249	1217	1601	1201	1601	1777	1201
1601	1777	1553	1777	1217	2273	2113	1249
1889	1889	1889	1889	1777		2129	1553
2113	2273	2113	2129	2113			2129
2273		2129		2273			

THEOREM 4.3. *Let* K *be a field such that*

(i) K *is a normal extension of* $\mathbf{Q}(\zeta_{16})$ *of degree* 32 *over* $\mathbf{Q}$.

(ii) K *contains* $\mathbf{Q}(\zeta_{16}, \sqrt{1 + \sqrt{2}})$.

(iii) K *ramifies only over* (2).

Then $K \neq \Omega_4(-4)$.

Proof. (Sketch) We find explicit generators for all such fields and proceed as in the second proof of Theorem 4.2.

We use the following facts about $\mathbf{Q}(\zeta_{16})$.

FACT 1. $\mathbf{Q}(\zeta_{16})$ *has class number one.*

FACT 2. *The ideal* $(2) = (\omega_2)^8$, *where* $\omega_2 = 1 - \zeta_{16}$.

FACT 3. *The unit group* $\mathbf{U} = \langle \zeta_{16}, \Omega_1, \Omega_2, \Omega_3 \rangle$, *where the* Ω_k *are given by*

$$\Omega_k = \sum_{j=0}^{2k} (\zeta_{16})^j, \qquad k = 1, 2, 3.$$

We again have two cases, depending on whether the candidate field K has cyclic or noncyclic Galois group over $\mathbf{Q}(\zeta_{16})$. Let $k_2 = \mathbf{Q}(\zeta_{16})$.

Cyclic 4*-extensions.* $K = k_2(\sqrt[4]{\mu})$, *where* $\mu = \sqrt{2}\,\theta^2$ *and*

$$\theta = \Omega_1^{a_1}\Omega_2^{a_2}\Omega_3^{a_3}\omega_2^{a_4}\zeta_{16}^{a_5},$$

with each $a_i = 0$ *or* 1.

Here we used the fact that $\mathbf{Q}(\zeta_{16}, \sqrt[4]{2}) = \mathbf{Q}(\zeta_{16}, \sqrt{1+\sqrt{2}})$. There are in fact only 16 distinct cyclic fields; the presence of $1 + \sqrt{2}$ in the unit group introduces redundancies in this list. The redundancies are given by $k_2(\sqrt[4]{\mu}) = k_2(\sqrt[4]{\mu'})$, where $\mu' = \sqrt{2}\,(\theta')^2$ and

$$\theta' = \Omega_1^{1-a_1}\Omega_2^{1-a_2}\Omega_3^{1-a_3}\omega_2^{a_4}\zeta_{16}^{a_5}.$$

We obtain a nonredundant list of fields by fixing $a_3 = 0$. Table 8 shows for all such fields K that $K \neq \Omega_4(-4)$.

Noncyclic 4*-extensions.* $K = k_2(\sqrt[4]{2}, \sqrt{\mu})$, *where* $\mu = \Omega_1^{a_1}\Omega_2^{a_2}\omega_2^{a_4}\zeta_{16}^{a_5}$ *and each* $a_i = 0$ *or* 1, *not all zero.*

Table 9 shows that all such noncyclic fields K have $K \neq \Omega_4(-4)$. □

5. Where might $\Omega_4(-4)$ be? Does the governing field $\Omega_4(-4)$ exist? We have ruled out the simplest candidate fields. It appears that the simple pattern of the equivalences (1.1)–(1.6) does not extend to the case where $16 \mid h(-p)$. We believe that the existence of the hypothetical field $\Omega_4(-4)$ would provide the most reasonable explanation of the observed densities in Tables 1 and 2. At this point one would like further theory which indicates where to search next for $\Omega_4(-4)$.

The following result, due to P. Morton, provides some further theory and suggests the possible truth of hypothesis (H2).

THEOREM 5.1 (MORTON). *Let* $n \geq 1$, *and let* p *be a prime for which*

$$p = 2x^{2^n} - y^{2^n} \tag{5.1}$$

is solvable with $x \equiv 1 \pmod 2$, $n \geq 1$. *Then* $2^{n+1} \mid h(-4p)$.

Proof. (Morton) The condition $x \equiv 1 \pmod 2$ guarantees $p \equiv 1 \pmod 8$, so that $(2) = \mathbf{P}^2$ in $\mathbf{Q}(\sqrt{-p})$. Also $\mathbf{P}$ is a nonprincipal prime ideal since $x^2 + py^2 = 2$ is unsolvable. In $\mathbf{Q}(\sqrt{-p})$ we may rewrite (5.1) in the form

$$\left(y^{2^{n-1}} + \sqrt{-p}\right)\left(y^{2^{n-1}} - \sqrt{-p}\right) = 2x^{2^n}. \tag{5.2}$$

Now let $\mathbf{A}$ be the greatest common ideal divisor of $(y^{2^{n-1}} + \sqrt{-p})$ and $(y^{2^{n-1}} - \sqrt{-p})$ in $\mathbf{Q}(\sqrt{-p})$. Then $\mathbf{A} \mid (y^{2^{n-1}} + \sqrt{-p}) - (y^{2^{n-1}} - \sqrt{p}) = 2\sqrt{-p}$. Since y is odd and $p \nmid y$, this gives $\mathbf{A} \mid (2)$. Since $p \equiv 1 \pmod 8$, $\frac{1}{2}(y^{2^{n-1}} + \sqrt{-p})$ is not an algebraic integer, so

$(2) \nmid y^{2^{n-1}} + \sqrt{-p}$ and consequently $\mathbf{A} = \mathbf{P}$. Then (5.2) implies the ideal factorizations

$$\left(y^{2^{n-1}} + \sqrt{-p}\right) = (\mathbf{B}_1)^{2^n}\mathbf{P}, \qquad \left(y^{2^{n-1}} - \sqrt{-p}\right) = (\mathbf{B}_2)^{2^n}\mathbf{P}.$$

Consequently $[\mathbf{B}_1]^{2^n} \sim [\mathbf{P}]$ as ideal classes, $[\mathbf{B}_1]^{2^{n+1}} \sim [\mathbf{P}]^2 \sim [(1)]$ as ideal classes, so $2^{n+1} \mid h(-4p)$. □

The hypothesis $x \equiv 1 \pmod 2$ is necessary for Theorem 5.1 to be true. Indeed, one might ask whether the weaker conditions

$$\pm p = 2x^{2^n} - y^{2^n}, \qquad p \equiv 1 \pmod{2^{n+2}},$$

imply that $2^{n+1} \mid h(-4p)$. This is true if $n = 1$ or 2 but is false for $n = 3$ as shown by the example $x = 2$, $y = 5$, $p = 390113$. Here $h(-4p) = 8.61$ and 16 does not divide $h(-4p)$.

We examine the case $n = 3$ of Theorem 5.1. It states that if

$$p = 2x^8 - y^8, \tag{5.3}$$

with $x \equiv 1 \pmod 2$, then $16 \mid h(-4p)$. The condition (5.3) implies that p is the norm of the principal prime ideal (π) in the nonnormal extension $\mathbf{Q}(\sqrt[8]{2})$, where

$$\pi = x\sqrt[8]{2} - y.$$

The condition that π be principal is a splitting condition on (p) in the Hilbert class field of $\mathbf{Q}(\sqrt[8]{2})$, and the condition that $x \equiv 1 \pmod 2$ is a splitting condition on (p) in a ray class field over $\mathbf{Q}(\sqrt[8]{2})$ whose conductor involves only ideals lying over (2). These observations are consistent with hypothesis (H2) in that they involve fields that ramify only over (2).

Morton's condition (5.3) involves the representation of p by the norm of an element in a $\mathbf{Z}$-module of rank 2 in the ring of integers O_L of the field $L = \mathbf{Q}(\sqrt[8]{2})$. If we could extend this to a condition involving a $\mathbf{Z}$-module of full rank 8 in O_L it would follow that $\Omega_4(-4)$ exists, and that it is an appropriate class field over $\mathbf{Q}(\zeta_8, \sqrt[8]{2})$. Based on these remarks, we advance the following working conjecture.

WORKING CONJECTURE. *For all large enough* j, $\Omega_4(-4) \subseteq M_j$, *where* M_j *is the ray class field* $\pmod{(2)^j}$ *over* $\mathbf{Q}(\zeta_8, \sqrt[8]{2})$.

This conjecture can be used as a basis for a more extensive computer-aided search for $\Omega_4(-4)$. We remark that the fields M_j for large j contain $\Omega_3(-4)$ and they ramify only over (2). Theorem 5.1 together with the prime 390113 mentioned earlier show that $\Omega_4(-4)$ is not contained in $\mathbf{Q}(\zeta_{32}, \sqrt[8]{2})$. Consequently if the working conjecture is true, we must have $j \geqslant 1$.

Appendix A. Governing Fields Are Unique.

Proof of Theorem 1.1. Let K_1 and K_2 be two fields having Property $P_j(d)$. The uniqueness of a minimal such field contained in all the others follows from the fact that $k = K_1 \cap K_2$ also has the Property $P_j(d)$.

To prove this fact, let K_1K_2 be the compositum of K_1 and K_2. It is Galois over $\mathbf{Q}$ since K_1 and K_2 are. Let H_1 and H_2 be the subgroups of $G = \mathrm{Gal}(K_1K_2/\mathbf{Q})$ keeping

K_1 and K_2 fixed, respectively. A well-known fact of Galois theory states that H_1H_2 is a normal subgroup of G and its fixed field is $K_1 \cap K_2$. (See Figure A-1.)

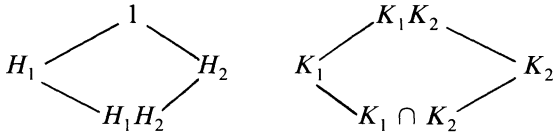

FIGURE A-1

Galois groups and their corresponding fixed fields

Now let f be any function on G with the properties:

(i) f is constant on conjugacy classes of G.

(ii) $f(ah_i) = f(a)$ for any $h_i \in H_i$, i.e. f is a function defined on G/H_i.

Then f is defined on G/H_1H_2 and is constant on conjugacy classes there. To see this, note that $f(ah_1h_2) = f(ah_1) = f(a)$ for all $a \in G$, $h_1 \in H_1$, $h_2 \in H_2$. Also if $a = cbc^{-1} \pmod{H_1H_2}$, then $f(a) = f(cbc^{-1}h_1h_2) = f(cbc^{-1}) = f(b)$. For our application, f is that function on G which satisfies (i) and assigns to an element a the appropriate 2-classgroup structure guaranteed to exist by Property $P_j(d)$ for that Artin symbol. Note that K_1K_2 has the Property $P_j(d)$ because the sets of primes determined by its Artin symbols are a refinement of the sets of primes determined by the Artin symbols of K_1. Then property (ii) above is just the assertion that K_1 and K_2 have Property $P_j(d)$, and the conclusion is that $K_1 \cap K_2$ also has Property $P_j(d)$. □

Remark. The same argument applies, mutatis mutandis, when conjugacy classes are replaced by divisions. Consequently, there are corresponding unique minimal fields $\Omega_j^*(d)$ for Conjecture $C_j^*(d)$.

City University of New York
New York, New York 10031

Bell Laboratories
Murray Hill, New Jersey 07974

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

2. G. BRÜCKNER, "Characterisierung der galoisschen Zahlkörper deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind," *Math. Nachr.*, v. 32, 1966, pp. 317–326.

3. N. CHEBOTAREV, "Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionenklasse gehören," *Math. Ann.*, v. 95, 1926, pp. 191–228.

4. H. COHN, *Advanced Number Theory*, Dover Reprint, 1980.

5. H. COHN, "Cyclic-sixteen class fields for $\mathbf{Q}(\sqrt{-p})$ by modular arithmetic," *Math. Comp.*, v. 33, 1979, pp. 1307–1316.

6. H. COHN, "The explicit Hilbert 2-cyclic class field for $\mathbf{Q}(\sqrt{-p})$," *J. Reine Angew. Math.*, v. 321, 1981, pp. 64–77.

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

8. H. COHN & J. C. LAGARIAS, "Is there a density for the set of primes p such that the class number of $\mathbf{Q}(\sqrt{-p})$ is divisible by 16?," *Colloq. Math. Soc. János Bolyai*, v. 34, Topics in Classical Number Theory, Budapest, Hungary, 1981.

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

10. P. KAPLAN, "Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et reciprocité biquadratique," *J. Math. Soc. Japan*, v. 25, 1973, pp. 596–608.

11. P. KAPLAN, "Sur le 2-groupe des classes d'ideaux des corps quadratiques," *J. Reine Angew. Math.*, v. 283/284, 1976, pp. 313–363.

12. P. KAPLAN, "Cycles d'ordre au moins 16 dans le 2-groupe des classes d'ideaux de certains corps quadratiques," Calculateurs en Math. (Conf., Limoges, 1975), *Bull. Soc. Math. France Mém.* No. 49–50, 1977, pp. 113–124.

13. P. KAPLAN & C. SANCHEZ, *Table de 2-Groupes d'Ideaux au Sens Restreint et des Facteurs Principaux des Corps Quadratiques Réels* $\mathbf{Q}(\sqrt{2p})$, $p < 2{,}000{,}000$, Université de Nancy I, U.E.R. de Mathematics, 1975.

14. J. C. LAGARIAS, "On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$," *Trans. Amer. Math. Soc.*, v. 260, 1980, pp. 485–508.

15. J. C. LAGARIAS, "Worst-case complexity bounds for algorithms in the theory of integral quadratic forms," *J. Algorithms*, v. 1, 1980, pp. 142–186.

16. J. C. LAGARIAS, "Sets of primes determined by systems of polynomial congruences," *Illinois J. Math.*, v. 27, 1983. (To appear.)

17. J. C. LAGARIAS & A. M. ODLYZKO, "Effective versions of the Chebotarev density theorem," in *Algebraic Number Fields, L-Functions and Galois Properties*, Proc. 1975 Durham Symposium (A. Fröhlich, Ed.), Academic Press, London, 1977, pp. 409–464.

18. S. LANG, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970.

19. P. MORTON, "On Redei's theory of the Pell equation," *J. Reine Angew. Math.*, v. 307/308, 1979, pp. 373–398.

20. P. MORTON, *The 2-Classgroup of a Quadratic Number Field and the Pell Equation* $x^2 - \Delta Y^2 = -1$, Thesis, University of Michigan, 1979.

21. P. MORTON, "Density results for the 2-classgroups of imaginary quadratic fields," *J. Reine Angew. Math.*, v. 332, 1982, pp. 156–187.

22. P. MORTON, "Density results for the 2-classgroups and fundamental units of real quadratic fields," *Studia. Sci. Math. Hungar.* (To appear.)

23. P. MORTON, "The quadratic number fields with cyclic 2-classgroups," *Pacific J. Math.*, v. 108, 1983, pp. 165–175.

24. W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw, 1974.

25. O. ORE, "Existenzbeweise für algebraische Körper mit Vorgeschreibenen Eigenshaften," *Math. Z.*, v. 25, 1926, pp. 474–489.

26. L. REDEI, "Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörper," *J. Reine Angew. Math.*, v. 171, 1934, pp. 55–60.

27. L. REDEI, "Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörper," *J. Reine Angew. Math.*, v. 171, 1934, pp. 131–148.

28. L. REDEI, "Bedingtes Artinsches symbol mit Anwendung der Klassenkörpertheorie," *Acta Math. Acad. Sci. Hungar.*, v. 4, 1953, pp. 1–29.

29. L. REDEI, "Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung," *Acta Math. Acad. Sci. Hungar.*, v. 4, 1953, pp. 31–87.

30. L. REDEI & H. REICHARDT, "Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers," *J. Reine Angew. Math.*, v. 170, 1933, pp. 69–74.

31. C. G. REUSCHLE, *Tafeln complexer Primzahlen welche aus Wurzeln der Einheit gebildet sein*, Belin Akad. Buchdrk., 1875, p. 443.

32. P. RIBENBOIM, *Algebraic Numbers*, Wiley, New York, 1972.

33. D. SHANKS, "Gauss' ternary form algorithm and the 2-Sylow subgroup," *Math. Comp.*, v. 25, 1971, pp. 837–853.

34. D. SHANKS, "Five number-theoretic algorithms," *Proc. 2nd Manitoba Conf. in Numer. Math.*, 1972, pp. 51–70.

35. H. M. STARK, "Values of L-functions at $s = 1$ I. L-functions for quadratic forms," *Adv. in Math.*, v. 7, 1971, pp. 301–343.

36. W. C. WATERHOUSE, "Pieces of eight in class groups of quadratic fields," *J. Number Theory*, v. 5, 1973, pp. 95–97.

37. K. S. WILLIAMS, "On the class number of $\mathbf{Q}(\sqrt{-p})$ modulo 16 for $p \equiv 1 \pmod 8$ a prime," *Acta Arith.*, v. 39, 1981, pp. 381–398.