MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 137–144

Computation of the Ideal Class Group of Certain Complex Quartic Fields. II

By Richard B. Lakein

Abstract. For quartic fields $K = F_3(\sqrt{\pi})$, where $F_3 = Q(\rho)$ and $\pi \equiv 1 \mod 4$ is a prime of F_3, the ideal class group is calculated by the same method used previously for quadratic extensions of $F_1 = Q(i)$, but using Hurwitz' complex continued fraction over $Q(\rho)$. The class number was found for 10000 such fields, and the previous computation over F_1 was extended to 10000 cases. The distribution of class numbers is the same for 10000 fields of each type: real quadratic, quadratic over F_1, quadratic over F_3. Many fields were found with noncyclic class group, including the first known real quadratics with groups 5×5 and 7×7. Further properties of the continued fractions are also discussed.

1. Introduction. The quartic fields $K = F(\sqrt{\mu})$, where $\mu \in F = \mathbf{Q}(\sqrt{-m})$, $m = 1, 2, 3, 7$, or 11, have many algebraic properties of integers, ideals, and units which are closely analogous to those of real quadratic fields. Furthermore, since the integers of F form a euclidean ring, one can, by means of a suitable generalization of continued fractions, actually calculate the objects of interest in K.

In addition to the detailed algebraic properties, there is a "gross" phenomenon in real quadratic fields with a counterpart in these quartic fields. The fields $\mathbf{Q}(\sqrt{p})$, for prime $p = 4k + 1$, appear to have a regular distribution of class numbers. Of the first 5000 such fields (cf. [6]), about 80% have class number $h = 1$, about 10% have $h = 3$, etc. An unpublished table of S. Kuroda [2] gives class numbers of the first 100811 such fields, up to $p = 2776817$. The distribution is:

h	1	3	5	7	9
%	77.65	11.19	3.80	1.82	1.36

Now the quartic fields $K = F(\sqrt{\pi})$, where $\pi = 4\alpha + 1$ is a prime of F, also have odd class numbers. In a recent paper [4] I used a modified version of the classical method for quadratic fields to calculate the class number and ideal class group for 5000 such quartic fields over $F = \mathbf{Q}(i)$. The distribution of class numbers was very close to that of the quadratic case.

In the present paper we extend the method to the analogous quartic fields over $F = \mathbf{Q}(\rho)$. We have calculated class number and class group for 10000 of these fields, and extended the calculations over $\mathbf{Q}(i)$ to a round 10000 fields. As predicted in

Received July 13, 1974.
AMS (MOS) subject classifications (1970). Primary 12A30, 12A50; Secondary 10F20, 12A05.

[4], the distribution is the same for all three types of fields. We present the results of the computations below. In the last section we discuss some interesting properties of three continued fractions over $\mathbf{Q}(\rho)$.

2. **The Fields over** $\mathbf{Q}(\rho)$. Let $F = \mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\rho)$, the "Eisenstein field," where $\rho = \frac{1}{2}(-1 + \sqrt{-3})$, and let $E = \mathbf{Z}[\rho]$, the Eisenstein integers. Let P be a rational prime $\equiv 1 \mod 12$, so $P = N\pi = a^2 - ab + b^2$, where the Eisenstein prime $\pi = a + b\rho$ is normalized so $a \equiv 1 \mod 4, b \equiv 0 \mod 4, b > 0$. Then let $K = F(\sqrt{\pi})$. The integers $\mathbf{I}$ of K have a basis $1, \Omega = \frac{1}{2}(1 + \sqrt{\pi})$ over E.

We are concerned with primitive ideals of $\mathbf{I}$, $\mathfrak{a} = [\alpha, \beta + \Omega]$. By [3], any ideal class of K has an ideal $\mathfrak{a}$ with norm $N\mathfrak{a} = N\alpha$ less than the "Gauss bound" $B = D^{1/2}/8 = 3P^{1/2}/8$. In particular, the splitting *prime* ideals with norm less than B generate the ideal class group. Just as in [4], our method is to count the ideal classes generated by these ideals, and the means of classifying ideals is a continued fraction expansion of the corresponding quadratic irrational over F. That is, $\mathfrak{a} = [\alpha, \beta + \Omega] \leftrightarrow A = (\beta + \Omega)/\alpha \in K$. All calculations are done in terms of the basis $1, \rho$ of E.

It remains to describe the continued fraction (CF). The CF used in [4] for calculations over $\mathbf{Q}(i)$ was the "nearest Gaussian integer" CF. For calculations over $\mathbf{Q}(\rho)$ we use the "nearest Eisenstein integer" CF. Both were defined by Hurwitz [1]. The complex plane is partitioned into congruent regular hexagons $H(a)$ centered at points $a \in \mathbf{Z}[\rho]$; then "the nearest Eisenstein integer to z" means the integer a for which $z \in H(a)$. Now $H(a) = a + H(0)$, and, in terms of $1, \rho$,

$$H(0) = \{x + y\rho \mid -1 \leqslant 2x - y < 1, -1 \leqslant x - 2y < 1, -1 \leqslant x + y < 1\}.$$

Thus given $z = x + y\rho$, let a and b be the nearest rational integer to x and y, respectively, and set $z_1 = (x - a) + (y - b)\rho$, thus translating z to the parallelogram

$$P(0) = \{x + y\rho \mid -\tfrac{1}{2} \leqslant x < \tfrac{1}{2}, -\tfrac{1}{2} \leqslant y < \tfrac{1}{2}\}.$$

Then if $z_1 \notin H(0)$ adjust $a + b\rho$ to obtain the nearest Eisenstein integer to z.

Except for the definition of the CF, the fact that the arithmetic is in the form $a + b\rho$, and the corresponding difference in testing which primes of F split in K, the method is essentially the same as in [4].

3. **Results of the Computation.** We computed the ideal class group (and so the class number) for 10000 fields $K = \mathbf{Q}(\rho, \sqrt{\pi})$ with prime discriminant $\pi = a + b\rho \equiv 1 \mod 4$, $13 \leqslant N\pi \leqslant 481909$. (The case where π is a rational prime $q \equiv 5 \mod 12$ was excluded, since it is known that $h = \frac{1}{2}h(q)h(-3q)$, where the latter are quadratic class numbers.) As conjectured in [4], the distribution of class numbers is the same as for real quadratic fields and for extensions of $\mathbf{Q}(i)$.

In Table 1 we list the distribution of class numbers for 10000 cases of each of the three types of fields. The quadratic fields, tabulated from [2], are $\mathbf{Q}(\sqrt{p})$, $5 \leqslant p \leqslant 225217$. The computation over $F_1 = \mathbf{Q}(i)$ in [4] was extended to 10000

TABLE 1. 10000 *fields of each type*

h	*Quadratic*	*over* $Q(i)$	*over* $Q(\rho)$
1	7954	7928	7982
3	1028	1073	1000
5	368	383	383
7	184	170	200
9	133	126	140
11	62	65	66
13	56	47	58
15	56	45	38
17	26	39	23
19	19	20	20
21	22	15	23
23	8	12	11
25	17	11	12
27	9	11	14
29	8	4	4
31	1	11	5
33	7	6	2
35	8	7	3
37	3	2	3
39	4	7	–
>40	27	18	13

cases, $F_1(\sqrt{\pi})$, $17 \leqslant N\pi \leqslant 482441$. Tables 2, 3, 4 give the distribution for 1000 fields at a time for each of the three types.

It now seems reasonable to expect the same distribution for fields quadratic over $Q(\sqrt{-m})$, $m = 2, 7$ or 11.

The results on class groups are quite interesting. Of the 10000 quadratic fields, only 7 have a noncyclic class group, namely $C(3) \times C(3)$. Of the fields over $Q(\rho)$, there are 22 with noncyclic group, all having two factors divisible by 3. For 19 fields the group is $C(3) \times C(3)$; for 2 fields it is $C(3) \times C(9)$; and one field has $C(3) \times C(15)$. There is as yet no explanation for this large number of noncyclic cases. Of course the base field $F_3 = Q(\rho)$ contains the cube roots of 1, but this relates to *cubic* extensions of F_3.

Of the fields over $Q(i)$, 4 have group $C(3) \times C(3)$; and one, $P = N\pi = 369913$, $\pi = 363 + 488i$, has group $C(5) \times C(5)$. The ideal classes containing prime divisors of $1 + 2i$ and of $3 - 2i$ are independent and each of order 5. There are six subgroups of order 5, each containing prime divisors of several Gaussian primes below the "Gauss bound."

While the group $C(5) \times C(5)$ was known to occur for *complex* quadratic fields—see [5, p. 162]—there was no real quadratic field of prime discriminant known to have a noncyclic class group involving anything but the 3-primary part of the group. This

TABLE 2. *Quadratic fields by thousands*

h	1	2	3	4	5	6	7	8	9	10	total	h
1	816	806	798	777	787	776	817	794	788	795	7954	1
3	101	112	93	116	101	109	101	89	101	105	1028	3
5	35	35	41	34	38	39	31	48	35	32	368	5
7	22	14	22	22	20	15	11	15	29	14	184	7
9	9	10	15	16	16	18	12	13	13	11	133	9
11	6	4	3	6	10	6	3	9	7	8	62	11
13	5	3	6	6	8	8	2	12	2	4	56	13
15	2	5	6	3	4	8	10	9	3	6	56	15
17	1	1	5	2	2	4	2	1	4	4	26	17
19	–	2	3	3	3	1	–	1	2	4	19	19
21	1	–	1	3	2	4	3	2	2	4	22	21
23	–	2	–	1	1	–	2	–	–	2	8	23
25	–	1	3	3	3	1	3	–	2	1	17	25
27	1	2	–	1	–	2	–	1	–	2	9	27
29	–	–	1	1	2	1	–	–	1	2	8	29
31	–	–	–	–	–	–	1	–	–	–	1	31
33	–	–	–	2	–	1	–	–	2	2	7	33
35	–	1	–	–	1	3	–	2	1	–	8	35
37	–	1	–	–	1	–	–	1	–	–	3	37
39	–	–	1	–	–	1	–	1	–	1	4	39
43	1	–	–	–	–	–	–	–	1	–	2	43
45		1	–	1	–	2	1	–	1	2	8	45
47			–	1	–	–	–	–	–	–	1	47
49			–	1	–	–	–	–	–	–	1	49
51			–	1	–	–	–	–	1	–	2	51
55			–		–	1	–	–	–	–	1	55
57			1		–		–	–	–	–	1	57
59			–		–		–	1	–	–	1	59
61			–		–		–	–	1	1	2	61
63			1		–		–	–	1		2	63
65					–		–	–	1		1	65
77					–		–	1	–		1	77
85					–		–		1		1	85
87					1		1		–		2	87
153									1		1	153

led us to check the quadratic fields in Kuroda's table [2] with class number divisible by a square greater than 9. In the range $p \leqslant 2776817$ we found 9 fields with group $C(3) \times C(9)$; 2 fields with $C(3) \times C(27)$, and 4 more interesting cases:

p	class group of $Q(\sqrt{p})$
1129841	$C(5) \times C(5)$
1510889	$C(5) \times C(5)$
1777441	$C(5) \times C(15)$
2068117	$C(7) \times C(7)$

TABLE 3. *Quadratic over* $Q(i)$ *by thousands*

h	1	2	3	4	5	6	7	8	9	10	total	h
1	830	805	792	798	769	780	782	800	781	791	7928	1
3	100	108	102	100	115	108	110	107	112	111	1073	3
5	35	30	48	42	43	34	34	33	40	44	383	5
7	14	17	16	22	16	19	18	16	19	13	170	7
9	5	8	12	12	19	13	17	10	17	13	126	9
11	6	8	5	3	6	13	7	8	4	5	65	11
13	3	8	8	3	8	6	3	2	3	3	47	13
15	2	6	5	2	6	6	6	5	3	4	45	15
17	3	3	4	5	4	5	6	3	2	4	39	17
19	–	–	2	3	1	7	4	1	1	1	20	19
21	–	1	–	2	3	–	1	2	3	3	15	21
23	1	–	2	1	1	2	–	1	2	2	12	23
25	1	–	–	1	1	1	1	1	5	–	11	25
27		3	–	1	1	–	3	1	2	–	11	27
29		1	1	–	1	–	1	–	–	–	4	29
31		–	1	1	1	2	3	2	1	–	11	31
33		2	–	–	1	1	–	1	–	1	6	33
35			–	1	3	–	–	1	–	2	7	35
37			–	–	–	–	1	–	–	1	2	37
39			–	2	1	–	2	2	–	–	7	39
41			–	–		–	–	–	1	–	1	41
43			1	–		–	–	–	–	1	2	43
45			–	–		1	–	1	1	–	3	45
49			–	–		–	–	–	1	–	1	49
53			–	–		–	–	2	–	–	2	53
57			1	1		–	–	1	–	–	3	57
59						–	1		–	–	1	59
61						1			–	–	1	61
63						–			–	1	1	63
65						1			–		1	65
69									1		1	69
85									1		1	85

Just as the first field with $C(3) \times C(3)$ is $p = 32009 = 179^2 - 32$, the first occurrence of $C(5) \times C(5)$ is for $p = 1129841 = 1063^2 - 128$. (See [5, pp. 157, 161].)

Table 5 lists the fields among each 10000 cases with noncyclic class group.

4. Remarks on the Continued Fractions. Let the CF for the basis number Ω begin $\Omega = a_0 + 1/x_1$. In all 20000 cases computed, the CF of x_1 is purely periodic with a complete quotient $x_m = (b + \Omega)/\zeta$, where ζ is a unit (root of 1) of F, and $x_{m+1} = \zeta x_1$. Then calculating the denominators q_n of the convergents of the CF for x_1, we obtain a unit $E_1 = q_m x_{m+1} + q_{m-1}$. This unit is the fundamental unit E_0 in all cases computed, except only three cases. It appears

TABLE 4. *Quadratic over $Q(\rho)$ by thousands*

h	1	2	3	4	5	6	7	8	9	10	total	h
1	833	799	798	810	814	785	785	788	785	785	7982	1
3	92	94	111	96	87	114	89	90	114	113	1000	3
5	43	45	32	37	34	39	43	41	36	33	383	5
7	16	20	21	15	19	17	23	23	23	23	200	7
9	6	14	11	15	14	13	16	17	13	21	140	9
11	5	7	8	4	8	5	14	10	2	3	66	11
13	2	9	9	6	8	5	4	6	3	6	58	13
15	1	5	3	2	2	4	6	4	6	5	38	15
17	1	3	1	3	2	4	3	3	2	1	23	17
19	–	1	3	2	1	1	7	3	1	1	20	19
21	1	2	1	3	2	4	3	2	4	1	23	21
23		–	–	3	1	–	1	3	2	1	11	23
25		1	–	1	4	1	2	1	–	2	12	25
27			–	–	2	4	2	4	–	2	14	27
29			–	1	–	1	–	1	–	1	4	29
31			1	1	1	1	–	–	1	–	5	31
33			1	–	–	–	–	–	1	–	2	33
35				–	1	–	–	2	–	–	3	35
37				–		1	–	–	1	1	3	37
41				–		1	–	–	2	–	3	41
43				–			–	–	1	–	1	43
45				–			1	–	–	–	1	45
49				–			–	–	–	1	1	49
51				–			–	–	1		1	51
53				1			–	1	–		2	53
57							–	–	1		1	57
59							–	1	–		1	59
63							1		1		2	63

that the "nearest integer" CF for *real* numbers, and its two complex generalizations, yield $E_1 = E_0$ in all but the following exceptional cases:

	π	Ω	E_0	E_1
over **Q**:	5	$\frac{1}{2}(1+\sqrt{5})$	Ω	E_0^2
over F_1:	$1+4i$	$\frac{1}{2}(1+\sqrt{\pi})$	Ω	E_0^2
	$5+4i$	$\frac{1}{2}(1+\sqrt{\pi})$	$i+(1+i)\Omega$	E_0^2
	$1+2i$	$(1+\sqrt{\pi})/(1+i)$	Ω	$-iE_0^3$
over F_3:	$1+4\rho$	$\frac{1}{2}(1+\sqrt{\pi})$	Ω	$-\rho E_0^3$
	$5+4\rho$	$\frac{1}{2}(1+\sqrt{\pi})$	Ω	E_0^2

There seems to be no reason for these exceptions, other than the fact that they are the smallest cases.

TABLE 5. *Noncyclic class groups*

Real quadratic fields $Q(\sqrt{p})$ with group 3×3:

p = 32009, 62501, 114889, 142097, 151141, 153949, 220217

Quartic fields $F_1(\sqrt{\pi})$:

$P = N\pi$	π	group
54713	$107 + 208i$	3×3
201881	$91 + 440i$	3×3
369913	$363 + 488i$	5×5
466553	$683 + 8i$	3×3
467497	$251 + 636i$	3×3

Quartic fields $F_3(\sqrt{\pi})$ with group 3×3:

$P = N\pi$	π	P	π	P	π	P	π
41617	$-59 + 168\rho$	175333	$37 + 436\rho$	287233	$-59 + 504\rho$	394489	$-527 + 168\rho$
73849	$185 + 312\rho$	190669	$477 + 380\rho$	299317	$553 + 12\rho$	434221	$581 + 716\rho$
83269	$285 + 292\rho$	198109	$353 + 500\rho$	360973	$-399 + 292\rho$	449077	$773 + 356\rho$
120397	$37 + 364\rho$	278149	$105 + 572\rho$	361561	$525 + 656\rho$	452989	$-275 + 492\rho$
160201	$-71 + 360\rho$	283909	$-323 + 292\rho$	362473	$661 + 144\rho$		

Quartic fields $F_3(\sqrt{\pi})$ with other groups:

$P = N\pi$	π	group
298621	$-315 + 316\rho$	3×15
363157	$693 + 292\rho$	3×9
452629	$-255 + 508\rho$	3×9

In [4] there were two fields over F_1 where the CF did not identify two equivalent ideals as being in the same ideal class. We now have 6 examples of this shortcoming of the CF's. There are 4 fields $F_1(\sqrt{\pi})$, with $P = N\pi$ = 2633, 210209, 316073, 343393; and 2 fields $F_3(\sqrt{\pi})$, with $P = N\pi$ = 35521, 371281. In each case there is an ideal class containing two (equivalent) ideals whose CF periods are distinct; and likewise two distinct periods representing the conjugate (inverse) class.

For comparison we reran the first 1000 fields over F_3, using two other CF's. Let's call the original CF H, based on the hexagons $H(a) = a + H(0)$. Corresponding to the parallelograms $P(a) = a + P(0)$ is the CF P, and finally the CF R, based on rectangles $R(a) = a + R(0)$, where

$$R(0) = \{x + y\rho \mid -\tfrac{1}{2} \leqslant y < \tfrac{1}{2}, -1 \leqslant 2x - y < 1\}.$$

The fundamental polygons for the three CF's have the same area, only the diameters of H, R, then P are successively larger.

Both R and P settled the 833 cases with $h = 1$. However, of the 167 cases with $h > 1$, there were many cases for which the CF's gave distinct periods for equivalent ideals. In fact, R failed in this way for 49 fields, and P failed for 55 fields—out of 167 cases! In contrast, $\mathcal{H}$ failed only twice in 2018 cases with $h > 1$.

As a final comparison we tabulated the length m of the primitive partial period of Ω, using the three CF's. Denote p_1, p_2, p_3 the period length using algorithm $\mathcal{H}$, $\mathcal{R}$, or $\mathcal{P}$, respectively. In 812 cases $p_1 = p_2 = p_3$; in 188 cases either p_2 or $p_3 > p_1$. More precisely, $p_1 = p_2 < p_3$ in 175 cases, $p_1 < p_2 = p_3$ in 3 cases, $p_1 < p_2 < p_3$ in 7 cases, and $p_1 = p_3 < p_2$ in 3 cases. The p_i's ranged between 1 and 62, and $\max p_i - p_1 \leqslant 3$.

The computations were done from January to March 1974 on the CDC 6400 at SUNY at Buffalo.

Department of Mathematics
State University of New York at Buffalo
Amherst, New York 14226

1. A. HURWITZ, "Über die Entwicklung komplexer Grössen in Kettenbrüche," *Acta Math.*, v. 11, 1887–1888, pp. 187–200. (Werke II, pp. 72–83).

2. S. KURODA, "Table of class numbers $h(p) > 1$ for quadratic fields $Q(\sqrt{p})$, $p \leqslant 2776817$," *Math. Comp.*, v. 29, 1975, UMT, pp. 335–336 (this issue).

3. R. B. LAKEIN, "A Gauss bound for a class of biquadratic fields," *J. Number Theory*, v. 1, 1969, pp. 108–112. MR 39 #1427.

4. R. B. LAKEIN, "Computation of the ideal class group of certain complex quartic fields," *Math. Comp.*, v. 28, 1974, pp. 839–846.

5. D. SHANKS, "On Gauss's class number problems," *Math. Comp.*, v. 23, 1969, pp. 151–163. MR 41 #6814.

6. D. SHANKS, "Review of Table: Class numbers of primes of the form $4n + 1$," *Math. Comp.*, v. 23, 1969, pp. 213–214.