MATHEMATICS OF COMPUTATION
VOLUME 59, NUMBER 200
OCTOBER 1992, PAGES 633-638

QUADRATIC FIELDS WITH SPECIAL CLASS GROUPS

JAMES J. SOLDERITSCH

ABSTRACT. For every prime number $p \geq 5$ it is shown that, under certain hypotheses on $x \in \mathbf{Q}$, the imaginary quadratic fields $\mathbf{Q}(\sqrt{x^{2p} - 6x^p + 1})$ have ideal class groups with noncyclic p-parts. Several numerical examples with $p = 5$ and 7 are presented. These include the field

$$\mathbf{Q}(\sqrt{-4805446123032518648268510536}).$$

The 7-part of its class group is isomorphic to $C(7) \times C(7) \times C(7)$, where $C(n)$ denotes a cyclic group of order n.

1. INTRODUCTION

The ideal class groups of the rings of integers of imaginary quadratic number fields have been studied intensively. Quite a number of things can be said about the 2-part of these finite abelian groups. For instance, by Gauß's genus theory, the number of independent generators of the 2-part of the class groups is easily expressed in terms of the number of primes dividing the discriminant of the field. The "rest" of the class group, the so-called *odd* part, is not so well understood. It seems that this part is almost always cyclic [1]. In other words, for odd primes p, the number of independent generators of the p-part, or the *p-rank*, of the class group does usually not exceed one. It appears to be difficult to find imaginary quadratic number fields whose class groups have a high p-rank for some odd prime p.

In [10], Yamamoto exhibited for each integer $n \geq 1$ an infinite number of imaginary quadratic fields with a copy of $C(n) \times C(n)$ in their class groups. Here, $C(n)$ denotes a cyclic group of order n. Shanks [7] was the first to exhibit examples where one needs at least *three* independent generators to generate the odd part of the class group. More precisely, in 1971 he exhibited imaginary quadratic fields whose class groups have 3-rank at least three. Craig [2] subsequently was able to show that there exist infinitely many quadratic fields with 3-rank at least three. Later, examples of class groups with 3-rank at least 4, 5, and even 6 have been found by Diaz y Diaz, Shanks and Williams [3], Quer and Llorente [4, 5], and others.

In this paper several examples of imaginary quadratic number fields are presented whose class groups have p-rank at least 3 for $p = 5$ or 7. These examples were originally documented in the author's 1977 Lehigh University thesis [9]. Since then, other examples with 5-rank at least 3 or even 4, and with 7-rank at

Received by the editor October 3, 1991.
1991 *Mathematics Subject Classification*. Primary 11R29; Secondary 11Y40, 11-04.

least 3, have been found [4, 6]. No examples with p-rank at least 3 seem to be known for any prime $p > 7$. However, the author believes that the method used successfully to find the examples shown in this paper has the potential to produce examples of p-rank at least three for primes $p > 7$.

In the next section it will be shown that, for each odd prime $p \geq 5$ and under suitable hypotheses on $x \in \mathbf{Q}$, the class group of the number field

$$\mathbf{Q}(\sqrt{x^{2p} - 6x^p + 1})$$

has a subgroup isomorphic to $C(p) \times C(p)$. In the final section several numerical examples are presented. These include six examples where the 5-rank is at least 3 and one example where the 7-rank is at least 3. The class groups have all been calculated by means of Shanks's algorithm [8].

2. Two independent generators

In this section we will, for each prime number $p \geq 5$, exhibit a large family of imaginary quadratic fields whose class groups admit $C(p) \times C(p)$ as a subgroup of their ideal class groups. It can, in fact, be shown that the family is infinite [9].

In the proposition below two ideals are exhibited whose pth powers are principal. In the theorem sufficient conditions are given for these ideals to be independent and of order p in the class group.

Proposition. *Let $p \geq 5$ be a prime number and let $a, b, f \in \mathbf{Z}$ with $a > 0$, with $\gcd(a, 2b) = 1$, and with $b^2 + a^p = f^2$. Suppose that $d = b^2 - a^p$ is not a square. Let I and J be the two ideals in the ring of integers O_F of $F = \mathbf{Q}(\sqrt{d})$ given by $I = (a, b + \sqrt{d})$ and $J = (a^2, b^2 + f\sqrt{d})$. Then*

(i) *$N(I) = a$ and $N(J) = a^2$.*

(ii) *$I^p = (b + \sqrt{d})$ and $J^p = (b^2 + f\sqrt{d})$.*

(iii) *All powers of I and J are primitive O-ideals.*

Proof. (i) Since d is not a square, the field F is a quadratic extension of $\mathbf{Q}$. The conjugate of $x \in F$ is denoted by $\overline{x}$. We have

$$I \cdot \overline{I} = (a^2, a(b + \sqrt{d}), a(b - \sqrt{d}), b^2 - d) = a \cdot I',$$

where I' is an ideal of O_F containing a, $b + \sqrt{d}$, and $b - \sqrt{d}$. This implies that $2b \in I'$ and, since $\gcd(a, 2b) = 1$, that I' is the unit ideal O_F. By the multiplicativity of the norm we have that $N(I)N(\overline{I}) = a^2$ and therefore that $N(I) = a$. The proof for J is similar: just replace a, b, and d by a^2, b^2, and $f^2 d$, respectively. This proves (i).

(ii) Since $(b + \sqrt{d})(b - \sqrt{d}) = a^p$, we have that

$$I^p \subset (a^p, b + \sqrt{d}) \subset (b + \sqrt{d}).$$

Since $a^p = b^2 - d$, the norms of these ideals are equal. This shows that $I^p = (b + \sqrt{d})$. The proof for J is similar. It follows from the fact that $a^{2p} = b^4 - f^2 d$. This proves (ii).

(iii) We recall that an ideal is called *primitive* if it is not divisible by any integer $n > 1$. Suppose l is a prime number dividing a power of I and let $\mathfrak{p}$ be a prime ideal of F dividing l. Then $\mathfrak{p}$ divides I and hence a. Since a is odd and coprime with d, we conclude that $\mathfrak{p}$ is unramified in $F = \mathbf{Q}(\sqrt{d})$.

Therefore, l divides $I = (a, b+\sqrt{d})$. This implies that l divides both a and b, which is impossible, since $\gcd(a, b) = 1$. The proof for J is similar. This completes the proof of the proposition. □

Lemma. *Let F be an imaginary quadratic number field with ring of integers O_F and discriminant Δ_F. Let I_1 and I_2 be two primitive O_F-ideals of norm less than $\sqrt{|\Delta_F|/2}$. If $I_1 \equiv I_2$ in the class group of F, then I_1 and I_2 are equal.*

Proof. It is well known and easily established that for every nonzero ideal I of O_F, its inverse in the ideal class group is given by the class of $\overline{I}$. Therefore, if $I_1 \equiv I_2$, we have that $I_1\overline{I}_2 = (\alpha)$ for some $\alpha \in O_F$. It follows that $N(\alpha) < |\Delta_F|/4$. Since F is an *imaginary* quadratic number field, this implies that $\alpha \in \mathbf{Z}$. On the other hand, $I_2\overline{I}_2 = (\beta)$ with $\beta \in \mathbf{Z}$. Combining this with $I_1\overline{I}_2 = (\alpha)$, we find

$$(\beta)I_1 = (\alpha)I_2.$$

Since the ideals I_1 and I_2 are not divisible by integers $n > 1$, we see that $\alpha = \pm\beta$ and hence that $I_1 = I_2$, as required. □

The following is the main result of this section.

Theorem. *Let $p \geq 5$ be a prime and let $a, b, f \in \mathbf{Z}$ with $\gcd(a, 2b) = 1$ and with $b^2 + a^p = f^2$. Suppose that $d = b^2 - a^p < 0$. Let F be the imaginary quadratic field $\mathbf{Q}(\sqrt{d})$ with ring of integers O_F and discriminant Δ_F. Let I and J be the two O_F-ideals given by $I = (a, b+\sqrt{d})$ and $J = (a^2, b^2+f\sqrt{d})$. If $1 < a^{p-1} < |\Delta_F|/4$, then the group generated by the classes of I and J generate a subgroup isomorphic to $C(p) \times C(p)$ in the class group of F.*

Proof. By Proposition (i) and the fact that $1 < a^{p-1} < |\Delta_F|/4$, we have that $1 < a = N(I) < \sqrt{|\Delta_F|/2}$. We see that I is not the trivial ideal and, by the lemma applied to I and O_F, that it is not principal. Therefore, by Proposition (ii) the class of I generates a cyclic subgroup of order p inside the class group of F.

If the class of J were in this subgroup, then $J \equiv I^k$ in the class group for some $k \in \mathbf{Z}$. Therefore,

$$J \equiv I^k \quad \text{or} \quad J \equiv \overline{I}^k \quad \text{for some } 0 \leq k < p/2.$$

Since $a^{p-1} < |\Delta|/4$, the norms of the ideals I^k and $\overline{I}^k$, for $0 \leq k < p/2$, do not exceed $\sqrt{|\Delta_F|/2}$. By Proposition (iii) the ideals I^k, $\overline{I}^k$, and J are all primitive. Since $p \geq 5$, the norm of J does not exceed $\sqrt{|\Delta_F|/2}$, and it follows from the lemma that actually

$$J = I^k \quad \text{or} \quad J = \overline{I}^k \quad \text{for some } 0 \leq k < p/2.$$

Taking norms, we can easily see that this implies $J = I^2$ or $J = \overline{I}^2$. Taking pth powers and using Proposition (ii) gives the following equality of principal ideals:

$$(b^2 + f\sqrt{d}) = (b \pm \sqrt{d})^2.$$

Since $2 < a^{p-1} < |\Delta_F|/4$, we see that $\Delta_F \neq -3$ or -4 and hence that $O_F^* = \{\pm 1\}$. Therefore, taking real parts, we get $\pm b^2 = b^2 + d$. Since $\Delta_F \neq -8$ or, equivalently, $F \neq \mathbf{Q}(\sqrt{-2})$, this equation has no solutions. This shows that the class of J is not in the group generated by the class of I. By Proposition (ii) the class of J has order p and the result follows. $\square$

Solving the equations satisfied by a, b, and f, we obtain a family of fields F:

Corollary. *Let $p \geq 5$ be a prime. The class groups of*

$$F = \mathbf{Q}(\sqrt{x^{2p} - 6x^p + 1})$$

contain a subgroup isomorphic to $C(p) \times C(p)$ whenever $x = s/t \in \mathbf{Q}$ satisfies $3 - \sqrt{8} < x^p < 3 + \sqrt{8}$, $s, t \in \mathbf{Z}$ both odd, and $1 < (st)^{p-1} < |\Delta_F|/4$.

Proof. We solve the equation

$$f^2 - b^2 = (f - b)(f + b) = a^p$$

of the theorem with $a > 1$ an odd integer and $\gcd(a, 2b) = 1$: we must have that f is odd and b is even, and hence that $\gcd(f+b, f-b) = 1$ as well. We conclude that $f - b = s^p$, $f + b = t^p$, and $a = st$ for $s, t \in \mathbf{Z}$ odd integers with $st > 1$. This implies that

$$a = st, \quad b = (t^p - s^p)/2, \quad 4d = t^{2p} - 6t^p s^p + s^{2p}.$$

Here, $d = b^2 - a^p$ as in the theorem. We have that

$$F = \mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{x^{2p} - 6x^p + 1})$$

with $x = s/t$. The corollary is now clear: the first condition ensures that $d < 0$ and hence that F is an imaginary quadratic number field. The second ensures that $a = st$ is odd, and the last one is just the condition $1 < a^{p-1} < |\Delta_F|/4$. Finally, it is clear that $\gcd(a, 2b) = 1$ whenever $\gcd(s, t) = 1$. $\square$

We note in passing that an analogous result can be established for $p = 3$ and that, although all of the class groups so constructed are guaranteed to have 3-rank at least 2, many of them turn out to have 3-rank three or more [9].

3. Numerical examples

In this section we present the results of some of the calculations done for [9]. We have calculated the class groups of the fields that occur in the corollary with $p = 5$ or 7. Only $x = s/t \in \mathbf{Q}$ were considered with

$$|t^{2p} - 6s^p t^p + s^{2p}|$$

less than a certain bound. After dividing out any square factors, the resulting discriminants $\Delta(s, t)$ were, in order of magnitude, fed to the computer program CLASNO, which calculated the structure of the class group of $F = \mathbf{Q}(\sqrt{t^{2p} - 6s^p t^p + s^{2p}})$. Since CLASNO is based on Shanks's algorithm [8], it is possible that we only find a *proper subgroup* of the ideal class group. This is, however, very unlikely to happen and, most probably, we have each time calculated the entire class group.

TABLE I

Group	Freq
$C(5) \times C(5)$	259
$C(5^2) \times C(5)$	55
$C(5^3) \times C(5)$	20
$C(5^4) \times C(5)$	4
$C(5^5) \times C(5)$	1
$C(5) \times C(5) \times C(5)$	4
$C(5^2) \times C(5) \times C(5)$	2

TABLE II

(s, t)	$\Delta(s, t)$	h_F	class group
(19, 15)	−4574009420324	1088000	$C(5) \times C(5) \times C(5)$ $\times C(2) \times C(4) \times C(1088)$
(39, 29)	−51887726858696	4492500	$C(5) \times C(5) \times C(25)$ $\times C(7188)$
(57, 53)	−19853645645824292	53813000	$C(5) \times C(5) \times C(5)$ $\times C(2) \times C(215252)$
(61, 49)	−638330124616229092	177136000	$C(5) \times C(5) \times C(5) \times C(2)$ $\times C(2) \times C(2) \times C(177136)$
(95, 69)	−10293170626023930824	1927395500	$C(5) \times C(5) \times C(5)$ $\times C(15419164)$
(99, 95)	−29120288199415792912 4	13632240000	$C(5) \times C(5) \times C(25) \times C(2)$ $\times C(2) \times C(5452896)$

For $p = 5$ we have calculated, in this way, 345 class groups. The frequencies of the isomorphism types of the 5-parts that we encountered are given in Table I.

We found six cases where the 5-rank is at least 3. These are described in more detail in Table II. By h_F we denote the class number, i.e., the cardinality of the class group of $F = \mathbf{Q}(\sqrt{t^{2p} - 6s^p t^p + s^{2p}})$. In the cases $(s, t) = (39, 29)$ and $(57, 53)$, the discriminant $\Delta(s, t)$ is equal to $t^{2p} - 6s^p t^p + s^{2p}$ divided by 7^2. In all other cases, $\Delta(s, t) = t^{2p} - 6s^p t^p + s^{2p}$.

For $p = 7$ we have calculated 200 class groups. The frequencies of the isomorphism types of the 7-parts that we encountered are given in Table III.

TABLE III

Group	Freq
$C(7) \times C(7)$	161
$C(7^2) \times C(7)$	32
$C(7^3) \times C(7)$	5
$C(7^2) \times C(7^2)$	1
$C(7) \times C(7) \times C(7)$	1

Only the 200th case was an example with 7-rank of the class group at least 3. It occurred for $(s, t) = (87, 85)$. We have

$$\Delta(87, 85) = -4805446123032518648268510536.$$

The class number of $F = \mathbf{Q}(\sqrt{\Delta(87, 85)})$ is 37212446915840, and the class group is isomorphic to

$$C(7) \times C(7) \times C(7) \times C(2) \times C(2) \times C(27122774720).$$

ACKNOWLEDGMENTS

It has been quite some time since the research discussed in this note was performed. Nonetheless, I would like to acknowledge the support given to me at the time by my dissertation advisor Clifford Queen, and by Dan Shanks, who provided a stimulating correspondence and interest in this investigation. I would also like to thank René Schoof, who originally became aware of my unpublished results and took an interest in them. His recent encouragement to me to review my work and provide this note is very much appreciated and has led to a renewal of my computational work in this area.

BIBLIOGRAPHY

1. D. A. Buell, *Class groups of quadratic fields*, Math. Comp. **30** (1976), 610–623.
2. M. Craig, *A type of class groups for imaginary fields*, Acta Arith. **22** (1973), 449–459.
3. F. Diaz y Diaz, D. Shanks, and H. C. Williams, *Quadratic fields with 3-rank equal to 4*, Math. Comp. **33** (1979), 836–840.
4. P. Llorente and J. Quer, unpublished tables.
5. J. Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12*, C. R. Acad. Sci. Paris **305** (1987), 215–218.
6. R. Schoof, *Class groups of complex quadratic fields*, Math. Comp. **41** (1983), 295–302.
7. D. Shanks, *A quadratic field of prime discriminant requiring three generators for its class group, and related theory*, Acta Arith. **21** (1972), 71–87.
8. ——, *Class number, a theory of factorization and genera*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, RI, 1971, pp. 415–440.
9. J. J. Solderitsch, *Quadratic fields with special class groups*, thesis, Lehigh University, 1977.
10. Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

9 HAWTHORNE LANE, ROSEMONT, PENNSYLVANIA 19010-1015
E-mail address: jjs@prc.unisys.com