ACTA ARITHMETICA
130.2 (2007)

Parameterized families of quadratic number fields with 3-rank at least 2

by

CARL ERICKSON (Stanford, CA), NATHAN KAPLAN (Princeton, NJ),
NEIL MENDOZA (Williamstown, MA),
ALLISON M. PACELLI (Williamstown, MA)
and TODD SHAYLER (Williamstown, MA)

1. Introduction. It is well known that there are infinitely many quadratic number fields with class number divisible by a given integer n (see Nagell [8] (1922) for imaginary fields and Yamamoto [11] (1970) and Weinberger [10] (1973) for real fields). A related question concerns the n-rank of the field, that is, the greatest integer r for which the class group contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$. In [11], Yamamoto showed that infinitely many imaginary quadratic number fields have n-rank ≥ 2 for any positive integer $n \geq 2$. In 1978, Diaz y Diaz [2] developed an algorithm for generating imaginary quadratic fields with 3-rank at least 2, and Craig [1] showed in 1973 that there are infinitely many real quadratic number fields with 3-rank at least 2 and infinitely many imaginary quadratic number fields with 3-rank at least 3. A few examples of higher 3-rank have also been found (see for instance Llorente and Quer [6, 9] who found in 1987/1988 three imaginary quadratic number fields with 3-rank 6). In this paper, we give infinite, simply parameterized families of real and imaginary quadratic fields with 3-rank 2. Although the existence of such fields has been known, the fields here are much easier to describe, and the parameterization yields a new lower bound on the number of fields with discriminant $< x$ and 3-rank ≥ 2 (see [7]).

The main result is as follows:

THEOREM 1.1. *Let* $w \equiv \pm 1 \pmod 6$, *and let* c *be any integer with* $c \equiv w \pmod 6$. *Then*

$$\mathbb{Q}(\sqrt{c(w^2 + 18cw + 108c^2)(4w^3 - 27cw^2 - 486c^2w - 2916c^3)})$$

has 3-*rank at least* 2.

2000 *Mathematics Subject Classification*: Primary 11R11.
Key words and phrases: 3-rank, class number, class group, quadratic number field.

Notice that if c and w are relatively prime, and p is an odd prime with $p^{2a+1} \parallel c$ for some non-negative integer a, then p is ramified. The parameterization therefore yields infinitely many real and infinitely many imaginary quadratic fields since only finitely many primes are ramified in a given field.

As a special case of the theorem where $c = 1$ and $w = 6a + 1$, we have the following:

COROLLARY 1.2. *For any integer a, $\mathbb{Q}(\sqrt{f(a)})$ has 3-rank at least 2, where*

$$\begin{aligned} f(a) &= 31104a^5 + 84240a^4 - 69120a^3 - 572040a^2 - 813336a - 434975 \\ &= (36a^2 + 120a + 127)(864a^3 - 540a^2 - 3168a - 3425). \end{aligned}$$

It is not hard to show that this special case itself yields infinitely many real quadratic fields and infinitely many imaginary fields.

The idea of the proof is to construct, for each d of the prescribed form, two distinct unramified, cyclic, cubic extensions of $\mathbb{Q}(\sqrt{d})$. By class field theory, then, the field has 3-rank at least 2. We use Kishi and Miyake's [4] characterization of quadratic number fields with class number divisible by 3 to construct two such extensions of the same quadratic field $\mathbb{Q}(\sqrt{d})$; we guarantee that the fields are distinct by showing that the prime 3 decomposes differently in each.

2. Proof. Recall that the *Hilbert class field* of a number field K is the maximal unramified abelian extension of K, and that $\mathrm{Gal}(H/K) \cong \mathrm{Cl}_K$, where Cl_K denotes the ideal class group of K. It follows that the class number of K is divisible by 3 if and only if there is a cyclic, cubic, unramified extension of K. In fact, Hasse's theorem [3] states that if K is a quadratic field, then K has 3-rank n if and only if there are exactly $(3^n - 1)/2$ cyclic, cubic, unramified extensions of K. To prove that a quadratic field K has 3-rank at least 2, therefore, it suffices to show that K has two distinct cyclic, cubic, unramified extensions.

First, notice that we may assume that c and w are relatively prime, because the quadratic field parameterized by c and w is the same as the field parameterized by $c/(c, w)$ and $w/(c, w)$.

In [4], Kishi and Miyake give the following characterization of all quadratic fields with class number divisible by 3.

THEOREM 2.1. *Choose $u, w \in \mathbb{Z}$ and let $g(Z) = Z^3 - uwZ - u^2$. If*

(i) *$d = 4uw^3 - 27u^2$ is not a square in $\mathbb{Z}$,*
(ii) *u and w are relatively prime,*
(iii) *$g(Z)$ is irreducible,*
(iv) *one of the following conditions holds:*

(I) $3\nmid w$,
(II) $3\,|\,w$, $uw \not\equiv 3 \pmod 9$, $u \equiv w \pm 1 \pmod 9$,
(III) $3\,|\,w$, $uw \equiv 3 \pmod 9$, $u \equiv w \pm 1 \pmod{27}$,

then the normal closure of $\mathbb{Q}(\theta)$, *where* θ *is a root of* $g(Z)$, *is a cyclic, cubic, unramified extension of* $\mathbb{Q}(\sqrt{d})$; *in particular, then,* $K = \mathbb{Q}(\sqrt{d})$ *has class number divisible by* 3. *Conversely, every quadratic number field* K *with class number divisible by* 3 *and every unramified, cyclic, cubic extension of* K *is given by a suitable choice of integers* u *and* w.

Given integers c and w with $c \equiv w \equiv \pm 1 \pmod 6$, we define integers u, x, and y so that the two pairs of integers u, w and x, y each satisfy the conditions of Theorem 2.1. In addition, if θ_1 is a root of $g_1(Z) = Z^3 - uwZ - u^2$ and θ_2 is a root of $g_2(Z) = Z^3 - xyZ - x^2$, then the cubic fields $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$ have discriminants with the same square free part as

$$d = c(w^2 + 18cw + 108c^2)(4w^3 - 27cw^2 - 486c^2w - 2916c^3).$$

By Theorem 2.1, then, $\mathbb{Q}(\sqrt{d})$ has two cyclic, cubic, unramified extensions L_1 and L_2 (we also show that L_1 and L_2 are distinct by showing that the prime 3 splits differently in each). It then follows from Hasse's theorem that $\mathbb{Q}(\sqrt{d})$ has 3-rank at least 2. Here L_1 and L_2 are the normal closures of $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$; since d is not a square, each has Galois group S_3 over $\mathbb{Q}$.

LEMMA 2.2. *Let* c *and* w *be integers with* $c \equiv w \equiv \pm 1 \pmod 6$. *If*

$$u = c(w^2 + 18cw + 108c^2), \qquad x = 9u, \qquad y = w + 18c,$$

then the pairs u, w *and* x, y *each satisfy the hypotheses of Theorem* 2.1, *that is,* $\mathbb{Q}(\sqrt{4uw^3 - 27u^2})$ *and* $\mathbb{Q}(\sqrt{4xy^3 - 27x^2})$ *each admit cyclic, cubic, unramified extensions.*

Proof. First note that since $c \equiv w \equiv \pm 1 \pmod 6$ and $(c, w) = 1$, we have $(6c, w) = 1$. It follows that $(u, w) = 1$ since $u \equiv 108c^3 \pmod w$. Also, since

$$x = 9c(w^2 + 18cw + 108c^2) = 9cw(w + 18c) + 972c^3 \equiv 972c^3 \pmod y,$$

and $y \equiv w \pmod{6c}$, we see that any prime factor of x and y would divide $6c$ and therefore w. Since $(6c, w) = 1$, this implies that $(x, y) = 1$ as well. Thus condition (ii) in Theorem 2.1 is satisfied.

For condition (iii), observe that c and w are odd, so u, x, and y are odd as well. Then

$$\begin{aligned} g_1(Z) &= Z^3 - uwZ - u^2 \equiv Z^3 + Z + 1 \\ &\equiv Z^3 - xyZ - x^2 = g_2(Z) \pmod 2, \end{aligned}$$

so g_1 and g_2 are both irreducible over $\mathbb{Z}$.

Condition (iv) is clearly satisfied since w and therefore y are not divisible by 3.

Finally, we show that condition (i) is also satisfied, namely, that $4uw^3 - 27u^2$ and $4xy^3 - 27x^2$ are not squares in $\mathbb{Z}$. This follows, in fact, from the other conditions. Let θ_1 and θ_2 be roots of $g_1(Z)$ and $g_2(Z)$, respectively, and let L_1 and L_2 be the normal closures of $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$, respectively. It suffices to show that the Galois groups of L_1 and L_2 over $\mathbb{Q}$ are S_3 since cubic fields with square discriminants are normal. So let $i = 1, 2$ and suppose, for contradiction, that the Galois group of L_i over $\mathbb{Q}$ is $\mathbb{Z}/3\mathbb{Z}$. Let p be a prime in $\mathbb{Z}$ that is totally ramified in L_i. If $v_p(a)$ denotes the exact power of p dividing a, then Llorente and Nart's characterization of prime decomposition in cubic fields [5] implies that either

(1) $1 \le v_p(b_i) \le v_p(a_i)$, where $g_i^*(Z) = Z^3 + a_i Z + b_i$ is obtained from $g_i(Z)$ by substituting Z/t for Z with appropriate $t \in \mathbb{Z}$ so that $v_q(a_i) \le 1$ or $v_q(b_i) \le 2$ for all primes q,

or

(2) $p = 3$, $3 \mid a_i$.

If $p \nmid uw$, then clearly the first condition does not hold. If $p \mid w$, then $v_p(b_i) = 0$ since u and w are relatively prime, so the first condition cannot hold for $i = 1$ or 2. Neither can it hold if $p \mid u$, for then as in [4, Lemma 2] we see that $v_p(a_i) = \beta$ and $v_p(b_i) = n + 2\beta$ for some integers n and β, with $\beta = 0$ or 1, where $v_p(u) = 2n + \beta$ (resp. $v_p(x) = 2n + \beta$). The second condition is impossible for $i = 1$, because $3 \nmid cw$ and therefore $3 \nmid a_1$. If $i = 2$, after substitution (with $t = 3$), $v_3(a_1) = v_3(u(w + 18c)) = 0$, so the second condition does not hold. Thus, no prime is totally ramified in L_1, contradicting the assumption that the splitting field of $g_1(Z)$ is a $\mathbb{Z}_3$-extension of $\mathbb{Q}$. The argument for L_2 is similar. The pairs u, w and x, y must therefore each generate cubic, cyclic, unramified extensions of the quadratic fields $\mathbb{Q}(\sqrt{4uw^3 - 27u^2})$ and $\mathbb{Q}(\sqrt{4xy^3 - 27x^2})$, respectively. ■

The following lemma follows from Theorem 1 in Llorente and Nart [5].

LEMMA 2.3. *For $u, w \in \mathbb{Z}$, set $g(Z) = Z^3 - uwZ - u^2$, and let θ be a root of g.*

(i) *If $uw \equiv 1 \pmod 3$, then 3 is inert in $\mathbb{Q}(\theta)$.*
(ii) *If $v_3(x) = 2n$ for some $n > 0$ with $xy/3^{2n} \equiv 1 \pmod 3$, then 3 splits completely in $\mathbb{Q}(\theta)$.*

We are now ready to prove the main theorem.

Proof of Theorem 1.1. Given $c \equiv w \equiv \pm 1 \pmod 6$, set

$$u = c(w^2 + 18cw + 108c^2), \qquad x = 9u, \qquad y = w + 18c.$$

Let θ_1 be a root of $g_1(Z) = Z^3 - uwZ - u^2$ and θ_2 a root of $g_2(Z) = Z^3 - xyZ - x^2$. Let L_1 and L_2 denote the normal closures of $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$, respectively. By Lemma 2.2, the pairs u, w and x, y satisfy the hypotheses of Theorem 2.1, so that L_1 and L_2 are unramified, cyclic, cubic extensions of $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$, respectively. Notice, however, that the cubic fields $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$ have discriminants which differ by a square factor:

$$\begin{aligned} 4xy^3 - 27x^2 &= 4(9u)(w+18c)^3 - 27(9u)^2 \\ &= 9[4u(w^3 + 54c(w^2 + 18wc + 108c^2)) - 243u^2] \\ &= 9[4u(w^3 + 54u) - 243u^2] = 9(4uw^3 - 27u^2). \end{aligned}$$

Thus L_1 and L_2 are both S_3-extensions of $\mathbb{Q}$ with the same quadratic subfield $\mathbb{Q}(\sqrt{d})$, where

$$\begin{aligned} d &= \sqrt{4uw^3 - 27u^2} \\ &= \sqrt{c(w^2 + 18cw + 108c^2)(w^3 - 27cw^2 - 486c^2w - 2916c^3)}. \end{aligned}$$

Finally, we claim that L_1 and L_2 are not isomorphic. We will show that the prime 3 splits differently in the two fields. Since $v_3(x) = 2$, and $xy/9 = u(w+18c) \equiv uw \equiv 1 \pmod 3$, Lemma 2.3 shows that 3 splits completely in $\mathbb{Q}(\theta_2)$. It follows that 3 must also split completely in its normal closure L_2. Since $uw \equiv 1 \pmod 3$, Lemma 2.3 implies that 3 is inert in $\mathbb{Q}(\theta_1)$. Thus 3 does not split completely in L_1 (in fact, 3 must factor as the product of two distinct primes in L_1), and so L_1 and L_2 are not isomorphic. Thus $\mathbb{Q}(\sqrt{d})$ has two distinct cubic, cyclic, unramified extensions, and therefore has 3-rank at least 2. ∎

Proof of Corollary 1.2. The given example results from letting $c = 1$ and writing $w = 6a + 1$ for some integer a. Then $u = w^2 + 18w + 108 = 36a^2 + 120a + 127$ and $4w^3 - 27u = 864a^3 - 540a^2 - 3168a - 3425$. We will show that the family above gives infinitely many imaginary quadratic number fields with 3-rank at least 2 and infinitely many real quadratic number fields with 3-rank at least 2. To see that this is the case, let p be any prime with $p \equiv 1 \pmod 3$. We claim that there exists some integer a such that $f(a)$ is positive and p divides $f(a)$ an odd number of times. Thus p divides the discriminant of $\mathbb{Q}(\sqrt{f(a)})$. Since there are infinitely many primes $p \equiv 1 \pmod 3$, and only finitely many primes can divide a given discriminant, it follows that there are infinitely many real quadratic fields of the form $\mathbb{Q}(\sqrt{f(a)})$ with 3-rank at least 2. The same is true for negative $f(a)$, giving the same result for imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{f(a)})$ with 3-rank at least 2.

Let p be any prime with $p \equiv 1 \pmod 3$. Then -3 is a square mod p, so there exists some $z \in \mathbb{Z}$ such that $z^2 \equiv -27 \pmod p$. Choose $a' \in \mathbb{Z}$ with

$$6a' \equiv z - 10 \pmod p.$$

Choose an integer b with $(72a' + 120)b \equiv 1 \pmod{p}$. This is possible since

$$72a' + 120 \equiv 12z \pmod{p},$$

which implies that $(p, 72a' + 120) = 1$. Define a as follows:

$$a = \begin{cases} a' & \text{if } (6a' + 10)^2 \not\equiv -27 \pmod{p^2}, \\ a' + bp & \text{if } (6a' + 10)^2 \equiv -27 \pmod{p^2}. \end{cases}$$

In either case, then, $(6a + 10)^2 \not\equiv -27 \pmod{p^2}$. It follows that $v_p(u) = 1$, since $u = 36a^2 + 120a + 127 \equiv (6a + 10)^2 + 27 \not\equiv 0 \pmod{p^2}$, but

$$\begin{aligned} u = 36a^2 + 120a + 127 &\equiv (6a + 10)^2 + 27 \equiv 6a(6a + 20) + 127 \\ &\equiv (z - 10)(z + 10) + 127 \equiv z^2 + 27 \equiv 0 \pmod{p}. \end{aligned}$$

Since u is odd for any a, and $(u, w) = 1$, we see that u and $4w^3 - 27u$ are relatively prime for any a. So p exactly divides $f(a) = u(4w^3 - 27u)$. This implies that p divides the discriminant of $\mathbb{Q}(\sqrt{f(a)})$ exactly once, and so, p is ramified in $\mathbb{Q}(\sqrt{f(a)})$, as claimed.

Note that we can always choose a' and b above so that $a \le 2$; this yields infinitely many imaginary quadratic fields with 3-rank at least 2. Similarly, we can choose a' and b so that $a \ge 3$, so there are also infinitely many real quadratic fields with 3-rank at least 2. ∎

References

[1] M. Craig, *A type of class group for imaginary quadratic fields*, Acta Arith. 22 (1973), 449–459.

[2] F. Diaz y Diaz, *On some families of imaginary quadratic fields*, Math. Comp. 32 (1978), 637–650.

[3] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Z. 31 (1930), 565–582.

[4] Y. Kishi and K. Miyake, *Parametrization of the quadratic fields whose class numbers are divisible by three*, J. Number Theory 80 (2000), 209–217.

[5] P. Llorente and E. Nart, *Effective determination of the decomposition of rational primes in a cubic field*, Proc. Amer. Math. Soc. 87 (1983), 579–585.

[6] P. Llorente and J. Quer, *On the 3-Sylow subgroup of the class group of quadratic fields*, Math. Comp. 50 (1988), 321–333.

[7] F. Luca and A. M. Pacelli, *Class groups of quadratic fields of 3-rank at least 2: Effective bounds*, J. Number Theory, to appear.

[8] T. Nagel, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 1 (1922), 140–150.

[9] J. Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12*, C. R. Acad. Sci. Paris Sér. I Math. 305 (1987), 215–218.

[10] P. J. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory 5 (1973), 237–241.

[11] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970), 57–76.

Department of Mathematics
Stanford University
Stanford, CA 94305, U.S.A.
E-mail: cerickson@stanford.edu

Department of Mathematics
Princeton University
Princeton, NJ 08544, U.S.A.
E-mail: nathank@princeton.edu

Department of Mathematics
Williams College
Williamstown, MA 01267, U.S.A.
E-mail: Neil.Mendoza@williams.edu
Allison.Pacelli@williams.edu
Todd.B.Shayler@williams.edu

Received on 5.7.2006
and in revised form on 16.11.2006 (5234)