ON THE IDEAL CLASS GROUP OF CERTAIN QUADRATIC FIELDS

YASUHIRO KISHI
Department of Mathematics, Fukuoka University of Education,
1-1 Bunkyoumachi Akama, Munakata-shi, Fukuoka 811-4192, Japan
e-mail: ykishi@fukuoka-edu.ac.jp

(Received 8 June 2009; revised 6 May 2010; accepted 28 June 2010)

Abstract. Let \( n (\geq 3) \) be an odd integer. Let \( k := \mathbb{Q}(\sqrt{4 - 3^n}) \) be the imaginary quadratic field and \( k' := \mathbb{Q}(\sqrt{-3(4 - 3^n)}) \) the real quadratic field. In this paper, we prove that the class number of \( k \) is divisible by 3 unconditionally, and the class number of \( k' \) is divisible by 3 if \( n (\geq 9) \) is divisible by 3. Moreover, we prove that the 3-rank of the ideal class group of \( k \) is at least 2 if \( n (\geq 9) \) is divisible by 3.

2010 Mathematics Subject Classification. 11R11, 11R29.

1. Introduction. The ideal class group is one of the most basic and mysterious objects in algebraic number theory. According to the result of Y. Yamamoto [9], there exist infinitely many quadratic fields whose \( p \)-ranks of the ideal class groups at least two for arbitrary given prime \( p \). However, it is difficult to characterize quadratic fields whose Sylow \( p \)-subgroups of the ideal class groups are not cyclic. In [1], C. Erickson et al. gave a simple parametric family of quadratic fields, whose 3-ranks of the ideal class groups at least two. In this paper, we give another family of such quadratic fields.

For an odd integer \( n (\geq 3) \), we consider two quadratic fields

\[ k := \mathbb{Q}(\sqrt{4 - 3^n}) \quad \text{and} \quad k' := \mathbb{Q}(\sqrt{-3(4 - 3^n)}). \]

In the case, where \( 4 - 3^n \) is square-free, we can easily see that the class number of \( k \) is divisible by 3. Indeed, the splitting field of

\[ f(X) = X^3 - X + 3^{(n-3)/2} \]

over \( \mathbb{Q} \) is an unramified cyclic cubic extension of \( k \) because the discriminant of \( f \) is equal to \( 4 - 3^n \). The first aim of this paper is to remove the condition ‘square-free’ in the above statement; that is, we will prove

**Theorem 1.** For an odd integer \( n \geq 3 \), the class number of \( k \) is divisible by 3.

Next we will prove the following result concerning the divisibility of the class number of \( k' \).

**Theorem 2.** For an integer \( n \geq 9 \) such that \( n \equiv 3 \pmod{6} \), the class number of \( k' \) is divisible by 3.

For a square-free negative integer \( d \) in general, denote the 3-rank of the ideal class group of the imaginary quadratic field \( \mathbb{Q}(\sqrt{d}) \) and the real quadratic field \( \mathbb{Q}(\sqrt{-3d}) \) by \( r \) and \( s \), respectively. It is well known that the inequalities \( s \leq r \leq s + 1 \) hold (see e.g. [8]). As in our previous paper [4, Theorem 7.1], it follows immediately that
**Proposition 1.1.** Let $d$ be a square-free negative integer with $3 \nmid d$. Then $r = s$ if and only if there are no cubic fields $K$ with $D_K = -3^3d$, where $D_K$ is the discriminant of $K$.

By using this proposition and Theorem 2, we will prove

**Theorem 3.** For an integer $n \geq 9$ such that $n \equiv 3 \pmod{6}$, the 3-rank of the ideal class group of $k$ is at least 2.

Recently, the author proved in his paper [5] that for any integer $n \geq 2$, the ideal class group of $k$ has a subgroup isomorphic to $C_n$, where $C_n$ is the cyclic group of order $n$. From this, together with Theorem 1 and Theorem 3, we immediately have

**Corollary 1.** For an odd integer $n \geq 5$, the ideal class group of $k$ has a subgroup isomorphic to $C_n \times C_3$. In particular, therefore, the class number of $k$ is divisible by $3n$.

### 2. Proofs of theorems

For a number field $K$, denote the discriminant, the norm map and the trace map of $K/\mathbb{Q}$ by $D_K$, $N_K$ and by $\text{Tr}_K$, respectively.

For an integer $m$ and a prime $p$, $v_p(m)$ denotes the greatest exponent $\mu$ of $p$ such that $p^\mu | m$.

For an element $\alpha$ of a quadratic field $k$ such that $N_k(\alpha) = m^3$ for some $m \in \mathbb{Z}$, define the cubic polynomial $f_\alpha$ by

$$f_\alpha(X) = X^3 - 3mX - \text{Tr}_k(\alpha).$$

The following proposition, which combined [3, Lemma 1] and [4, Proposition 6.5], is one of the main ingredients in the proofs of our theorems.

**Proposition 2.1.** Let $d$ be an integer with $d \not\equiv \mathbb{Z}^2 \cup (-3\mathbb{Z}^2)$ and put $k := \mathbb{Q}(\sqrt{d})$ and $k' := \mathbb{Q}(\sqrt{-3d})$. Let $\alpha$ be an integer in $k'$ whose norm is a cube in $\mathbb{Z}$: $N_{k'}(\alpha) = m^3$ ($m \in \mathbb{Z}$). Then the polynomial $f_\alpha$ is reducible over $\mathbb{Q}$ if and only if $\alpha$ is a cube in $k'$. Moreover, if $f_\alpha$ is irreducible over $\mathbb{Q}$, then the splitting field of $f_\alpha$ over $\mathbb{Q}$ is a cyclic cubic extension of $k$ unramified outside 3 and $v_3(D_K) \neq 5$ for some cubic subfield $K$.

**Remark 2.2.** It is well known that we have $v_3(D_K) = 0$, 1, 3, 4 or 5 for a cubic field $K$ (see e.g. [2, Satz 6]). The prime 3 is totally ramified in $K$ if and only if $v_3(D_K) = 3$, 4 or 5.

Next, we extract some results from P. Llorente and E. Nart [7, Theorem 1].

**Proposition 2.3.** Suppose that the cubic polynomial

$$F(X) = X^3 - aX - b, \quad a, b \in \mathbb{Z}$$

is irreducible over $\mathbb{Q}$, and that either $v_3(a) < 2$ or $v_3(b) < 3$ holds. Let $\theta$ be a root of $F(X) = 0$, and put $K = \mathbb{Q}(\theta)$. Then the prime 3 is totally ramified in $K/\mathbb{Q}$ if and only if one of the following conditions holds:

1. (LN-i) $1 \leq v_3(b) \leq v_3(a)$;
2. (LN-ii) $3 | a, a \not\equiv 3 \pmod{9}$, $3 \nmid b$ and $b^2 \not\equiv a + 1 \pmod{9}$;
3. (LN-iii) $a \equiv 3 \pmod{9}$, $3 \nmid b$ and $b^2 \not\equiv a + 1 \pmod{27}$.
Proof of Theorem 1. By the assumption, we can express \( n = 2m + 1, m (\geq 1) \in \mathbb{Z} \).
Define the element \( \alpha \in k' = \mathbb{Q}(\sqrt{3^{2m+1} - 12}) \) by
\[
\alpha := \frac{3^{2m+1} - 2 + 3^m \sqrt{3^{2m+1} - 12}}{2}.
\]
Then we have
\[
N_{k'}(\alpha) = 1^3 \quad \text{and} \quad \text{Tr}_{k'}(\alpha) = 3^{2m+1} - 2.
\]
The polynomial
\[
f_\alpha(X) = X^3 - 3X - (3^{2m+1} - 2)
\]
is irreducible over \( \mathbb{Q} \) because
\[
f_\alpha(X) \equiv X^3 - X - 1 \pmod{2}
\]
is irreducible over \( \mathbb{F}_2 \). Then by Proposition 2.1, the splitting field of \( f_\alpha \) over \( \mathbb{Q} \) is a cyclic cubic extension of \( k \) unramified outside 3. Moreover, \( f_\alpha \) does not satisfy the conditions (LN-i), (LN-ii) and (LN-iii) in Proposition 2.3. Therefore, the splitting field of \( f_\alpha \) over \( \mathbb{Q} \) is an unramified cyclic cubic extension of \( k \), and hence the class number of \( k \) is divisible by 3. \( \square \)

Remark 2.4. We will give another proof of Theorem 1 by using [6, Theorem]. Put \( u = 3^{2(m-1)} \) and \( w = 1 \) in [6, Theorem]; we have
\[
g(Z) = Z^3 - 3^{2(m-1)}Z - 3^{4(m-1)}
\]
and
\[
d = 4 \cdot 3^{2(m-1)} - 27 \cdot (3^{2(m-1)})^2 = 3^{2(m-1)}(4 - 3^{2m+1}).
\]
We easily see that the condition (i) in [6, Theorem] holds. Furthermore,
\[
g(Z) = Z^3 - 3^{2(m-1)}Z - 3^{4(m-1)} \equiv Z^3 - Z - 1 \pmod{2}
\]
is irreducible over \( \mathbb{F}_2 \), so \( g(Z) \) is irreducible over \( \mathbb{Q} \). Then the class number of \( \mathbb{Q}(\sqrt{d}) = k \) is divisible by 3.

Proof of Theorem 2. By the assumption, we can express \( n = 6u + 3, u (\geq 1) \in \mathbb{Z} \).
Define the element \( \alpha \in k = \mathbb{Q}(\sqrt{4 - 3^{6u+3}}) \) by
\[
\alpha := \frac{3^{u+1}(3^{2u+1} - 2) + \sqrt{4 - 3^{6u+3}}}{2}.
\]
Then we have
\[
N_k(\alpha) = (3^{2u+1} - 1)^3 \quad \text{and} \quad \text{Tr}_k(\alpha) = 3^{u+1}(3^{2u+1} - 2).
\]
Let us show that
\[
f_\alpha(X) = X^3 - 3(3^{2u+1} - 1)X - 3^{u+1}(3^{2u+1} - 2)
\]
is irreducible over $\mathbb{Q}$. In the case $u = 1$, we can verify that

$$f_{\alpha}(X) = X^3 - 3(3^{2u+1} - 1)X - 3^{1+1}(3^{2u+1} - 2) = X^3 - 78X - 225$$

is irreducible over $\mathbb{Q}$. Assume now that $u \geq 2$ and that $\alpha \in k^3$. Then we can express

$$\alpha = \left(\frac{s + t\sqrt{D}}{2}\right)^3$$

for some $s, t \in \mathbb{Z}$, where $D$ is the square-free part of $4 - 3^{6u+3}$. Since

$$\left(\frac{s + t\sqrt{D}}{2}\right)^3 = \frac{s(s^2 + 3t^2D)/4 + t(3s^2 + t^2D)/4 \cdot \sqrt{D}}{2},$$

we have

$$4 \cdot 3^{u+1}(3^{2u+1} - 2) = s(s^2 + 3t^2D), \quad (2.1)$$

and hence $s$ is divisible by 3. On the other hand, since the norm of $(s + t\sqrt{D})/2$ is equal to $3^{2u+1} - 1$, we have

$$t^2D = s^2 - 4(3^{2u+1} - 1), \quad (2.2)$$

and hence $t^2D$ is not divisible by 3. Therefore we get

$$v_3(s^2 + 3t^2D) = 1. \quad (2.3)$$

From (2.1) and (2.3), we have $3^u | s$, and hence we can express

$$s = 3^u a \quad (2.4)$$

for some $a \in \mathbb{Z}$. Substituting (2.2) and (2.4) into (2.1), it follows that

$$4 \cdot 3^{u+1}(3^{2u+1} - 2) = s(s^2 + 3(s^2 - 4(3^{2u+1} - 1)))$$
$$= 4s(s^2 - 3^{2u+2} + 3)$$
$$= 4 \cdot 3^{u+1}a(3^{2u-1}(a^2 - 9) + 1),$$

and so

$$3^{2u+1} - 2 = a(3^{2u-1}(a^2 - 9) + 1). \quad (2.5)$$

If $a \leq -3$, then

$$a(3^{2u-1}(a^2 - 9) + 1) \leq 0 < 3^{2u+1} - 2.$$  

This is a contradiction. If $a \geq 4$, then

$$a(3^{2u-1}(a^2 - 9) + 1) \geq 4(3^{2u-1} \cdot 7 + 1) = 28 \cdot 3^{2u-1} + 4 > 3^{2u+1} - 2.$$  

This is also a contradiction. Therefore $a$ must be in the range

$$-2 \leq a \leq 3. \quad (2.6)$$
It follows from (2.5) that

\[-2 \equiv a \pmod{3^{2u-1}}.\]

From this together with (2.6) and \(u \geq 2\), we have \(a = -2\). This contradicts that the left-hand side of (2.5) is odd. Hence \(\alpha\) is not a cube in \(k\). Therefore, by Proposition 2.1, \(f_\alpha\) is irreducible over \(\mathbb{Q}\). Since \(f_\alpha\) does not satisfy the conditions (LN-i), (LN-ii) and (LN-iii), the splitting field of \(f_\alpha\) over \(\mathbb{Q}\) is an unramified cyclic cubic extension of \(k'\). The proof is completed.

**Proof of Theorem 3.** We keep the notation and situation from the proof of Theorem 2. Then the 3-rank of the ideal class group of \(k'\) is at least 1. By Proposition 1.1, therefore, it is sufficient to show that there is a cubic field \(K\) with \(\text{disc}(K) = -3^3 D\).

Now define the element \(\alpha \in k\) by

\[\alpha := 2 + \sqrt{4 - 3^{6u+3}}.\]

It follows from

\[N_k(\alpha) = (3^{2u+1})^3 \text{ and } \text{Tr}_k(\alpha) = 4\]

that we have

\[f_\alpha(X) = X^3 - 3^{2u+2}X - 4.\]

Let \(\theta\) be a root of \(f_\alpha(X) = 0\), and put \(K = \mathbb{Q}(\theta)\). Since

\[f_\alpha(X + 1) = X^3 + 3X^2 - 3(3^{2u+1} - 1)X - 3(3^{2u+1} + 1),\]

we see by Eisenstein’s criterion for the prime 3 that \(f_\alpha\) is irreducible over \(\mathbb{Q}\). Then by the last half of Proposition 2.1, the splitting field of \(f_\alpha\) over \(\mathbb{Q}\) is a cyclic cubic extension of \(k'\) unramified outside 3. We can easily check that the condition (LN-ii) holds. Then 3 is totally ramified in \(K\) and so \(v_3(D_K) = 3\) by Proposition 2.1. Hence we have \(D_K = -3^3 D\). By Proposition 1.1 and Theorem 2, therefore, the 3-rank of the ideal class group of \(k\) is at least 2. The proof is completed.

**Remark 3.1.** We use computer manipulations with GP/PARI (Version 2.1.7). From these tables, we can see that for an integer \(n\) in the range \(9 \leq n \leq 100\) with \(n \equiv 3 \pmod{6}\), the ideal class group of \(k\) has a subgroup isomorphic to \(C_3 \times C_3\) (thus, in particular, \(C_9 \times C_3\)). However, the author has not yet proved this.

**3. Numerical examples.** In Table 1, we list the square-free part of \(4 - 3^n\), the structure of the ideal class group of \(k = \mathbb{Q}(\sqrt{4 - 3^n})\) and the class number of \(k' = \mathbb{Q}(\sqrt{-3(4 - 3^n)})\) for \(3 \leq n \leq 49\) with \(n \equiv 1 \pmod{2}\). In Table 2, we list the structure of the ideal class group of \(k = \mathbb{Q}(\sqrt{4 - 3^n})\) for \(50 \leq n \leq 100\) with \(n \equiv 3 \pmod{6}\). Here we denote an abelian group \(C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}\) by \([n_1, n_2, \ldots, n_r]\).
Table 1.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Square-free part of $4 - 3^n$</th>
<th>The structure of the ideal class group of $\mathbb{Q}(\sqrt{4 - 3^n})$</th>
<th>The class number of $\mathbb{Q}(\sqrt{-3(4 - 3^n)})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$-23$</td>
<td>[3]</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>$-239$</td>
<td>[15]</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>$-2183$</td>
<td>[42]</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>$-19679$</td>
<td>[54, 3]</td>
<td>6</td>
</tr>
<tr>
<td>11</td>
<td>$-177143$</td>
<td>[264]</td>
<td>16</td>
</tr>
<tr>
<td>13</td>
<td>$-1594319$</td>
<td>[1872]</td>
<td>64</td>
</tr>
<tr>
<td>15</td>
<td>$-14348903$</td>
<td>[270, 15]</td>
<td>150</td>
</tr>
<tr>
<td>17</td>
<td>$-129140159$</td>
<td>[9690]</td>
<td>230</td>
</tr>
<tr>
<td>19</td>
<td>$-1162261463$</td>
<td>[31350]</td>
<td>1818</td>
</tr>
<tr>
<td>21</td>
<td>$-10460353199$</td>
<td>[12663, 3, 3]</td>
<td>1665</td>
</tr>
<tr>
<td>23</td>
<td>$-94143178823$</td>
<td>[159942]</td>
<td>7154</td>
</tr>
<tr>
<td>25</td>
<td>$-1601679791$</td>
<td>[60300]</td>
<td>804</td>
</tr>
<tr>
<td>27</td>
<td>$-7625597484983$</td>
<td>[310554, 6]</td>
<td>74892</td>
</tr>
<tr>
<td>29</td>
<td>$-68630377364879$</td>
<td>[4315722, 2]</td>
<td>82596</td>
</tr>
<tr>
<td>31</td>
<td>$-617673396283943$</td>
<td>[32074677]</td>
<td>660543</td>
</tr>
<tr>
<td>33</td>
<td>$-5559060566555519$</td>
<td>[29688714, 3]</td>
<td>1050978</td>
</tr>
<tr>
<td>35</td>
<td>$-50031545098999703$</td>
<td>[52523730, 3]</td>
<td>3287202</td>
</tr>
<tr>
<td>37</td>
<td>$-450283905890997359$</td>
<td>[1018421115]</td>
<td>12171397</td>
</tr>
<tr>
<td>39</td>
<td>$-4052555153018976263$</td>
<td>[123043050, 3, 3]</td>
<td>34215606</td>
</tr>
<tr>
<td>41</td>
<td>$-36472996377170786399$</td>
<td>[5322108033]</td>
<td>47957583</td>
</tr>
<tr>
<td>43</td>
<td>$-328256967394537077623$</td>
<td>[7736038668, 2]</td>
<td>373576936</td>
</tr>
<tr>
<td>45</td>
<td>$-2954312706550833698639$</td>
<td>[505223730, 18, 2, 2, 2]</td>
<td>533315808</td>
</tr>
<tr>
<td>47</td>
<td>$-265888143538957503287783$</td>
<td>[21629637726, 2, 2]</td>
<td>1818043912</td>
</tr>
<tr>
<td>49</td>
<td>$-239299329230617529509079$</td>
<td>[153033164592, 6]</td>
<td>5545046352</td>
</tr>
</tbody>
</table>

Table 2.

<table>
<thead>
<tr>
<th>$n$</th>
<th>The structure of the ideal class group of $\mathbb{Q}(\sqrt{4 - 3^n})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>51</td>
<td>[227163157560, 6]</td>
</tr>
<tr>
<td>57</td>
<td>[57240211680, 18, 6, 6]</td>
</tr>
<tr>
<td>63</td>
<td>[42265762274736, 18]</td>
</tr>
<tr>
<td>69</td>
<td>[920661234127056, 6, 6]</td>
</tr>
<tr>
<td>75</td>
<td>[80380027121635350, 3, 3]</td>
</tr>
<tr>
<td>81</td>
<td>[2144525716486877706, 6, 2]</td>
</tr>
<tr>
<td>87</td>
<td>[37490396487976286514, 6, 2]</td>
</tr>
<tr>
<td>93</td>
<td>[406363908197600166438, 6, 6]</td>
</tr>
<tr>
<td>99</td>
<td>[16886151827162849108592, 18]</td>
</tr>
</tbody>
</table>

**Acknowledgement.** The author is grateful to the referee for his/her careful reading and for many comments on this paper.
REFERENCES


