TAIWANESE JOURNAL OF MATHEMATICS
Vol. 19, No. 5, pp. 1387-1399, October 2015
DOI: 10.11650/tjm.19.2015.5081
This paper is available online at http://journal.taiwanmathsoc.org.tw

REMARKS ON QUADRATIC FIELDS WITH NONCYCLIC IDEAL CLASS GROUPS

Kwang-Seob Kim

Abstract. Let n be an integer. Then, it is well known that there are infinitely many imaginary quadratic fields with an ideal class group having a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Less is known for real quadratic fields, other than the cases that $n = 3, 5,$ or 7, due to Craig [3] and Mestre [4, 5]. In this article, we will prove that there exist infinitely many real quadratic number fields with the ideal class group having a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ In addition, we will prove that there exist infinitely many imaginary quadratic number fields with the ideal class group having a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

1. Introduction

The divisibility properties of class numbers are very important for understanding the structure of ideal class groups of number fields. Numerous results about the divisibility of class numbers of quadratic fields have been given by many authors (for more details see [1, 2, 6, 7, 8, 9, 10, 11, 12]). Through such works, it has been shown that, for any integer n, there exist infinitely many imaginary (resp. real) quadratic number fields whose ideal class numbers are multiples of n. Furthermore, it has been proven that there exist infinitely many imaginary (resp. real) quadratic number fields with the property that the ideal class group has a cyclic subgroup of order n. However, this does not necessarily mean that the ideal class group has an arbitrary abelian group of order n as a subgroup. We present our conjecture, as follows.

Conjecture. For any finite abelian group G, there exist infinitely many quadratic fields K such that the ideal class group of K contains a subgroup isomorphic to G.

In order to prove our conjecture, it suffices to show that there exist infinitely many quadratic fields K such that the ideal class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^m$, where m and n are arbitrary integers. However, even this statement is not close to having been proven so far. The best known quantitative result is as follows.

Received July 24, 2014, accepted April 9, 2015.
Communicated by Yu-Ru Liu.
2010 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R11.
Key words and phrases: Ideal class group, Real quadratic fields.

Theorem 1.1. (Theorem 2 of [11]). *For any integer $n \geq 1$, there are infinitely many imaginary quadratic fields with the ideal class group having a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

For real quadratic fields, less has been shown, except due to Craig [3] and Mestre [4, 5] for the cases that $n = 3, 5,$ or 7. In this article, we will prove that there exist infinitely many real quadratic number fields with an ideal class group having a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, for every natural number n. We approach this by modifying the method used in [11]. At the same time, we will also show that there exist infinitely many imaginary quadratic number fields with the ideal class group having a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. A sketch of our method is as follows. We will construct a quadratic number field that has three ideal classes, $[\mathfrak{a}]$, $[\mathfrak{a}']$, and $[\mathfrak{a}'']$, and also satisfies some local conditions on its discriminant K. In the case that $D < 0$, they are of order n and independent. In the case that $D > 0$, neither of them may be of order n, due to the existence of non-trivial units, but the subgroup $\langle [\mathfrak{a}], [\mathfrak{a}'], [\mathfrak{a}''] \rangle$ contains $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Next, we show that an infinite quantity of such fields exist in either case.

2. Review of Yamamoto's Paper [11]

Since our proof is based on Yamamoto's paper [11], we will review the method used there. Let $n \geq 3$ be a natural number. We will fix this definition of n throughout this article. Let K be a quadratic number field with discriminant D, where we assume $D \neq -3$ or -4 in order to simplify our argument in the following. Then, let σ be the nontrivial automorphism of K over $\mathbb{Q}$. Define ϵ by

$$\epsilon = \begin{cases} \text{a fundamental unit of } K & \text{if } D > 0, \\ 1 & \text{if } D < -4. \end{cases}$$

Lemma 2.1. (Lemma 1 of [11]). *Let x, y, z be a solution in $\mathbb{Z}$ of the Diophantine equation*

$$X^2 - Y^2 D = 4Z^n \tag{2.1}$$

satisfying $(x, z) = 1$. Then, there exists an (integral ideal) $\mathfrak{a}$ in K such that

(a) $\left(\frac{x+y\sqrt{D}}{2}\right) = \mathfrak{a}^n$,

(b) *$\mathfrak{a}$ and $\mathfrak{a}^\sigma$ are relatively prime,*

where (α) denotes the principal ideal in K generated by an element α of K.

Let p be a prime factor of n. Take another prime number ℓ with

$$\ell \equiv 1 \pmod{2p}, \tag{2.2}$$

so that -1 is a p-th power residue mod ℓ.

Suppose that we have a solution x, y, z of the equation (2.1) satisfying

(i) $(x, z) = 1$,

(ii) $\ell | z$,

(iii) x is a p-th power non-residue mod ℓ.

It can be easily deduced that

$$\left(\frac{D}{\ell}\right) = 1, \tag{2.3}$$

where the left side is the Kronecker symbol. By the decomposition law of primes we have $\ell = \tau\tau^\sigma$, where τ and τ^σ are distinct conjugate prime ideals in K. Now, we set

$$\alpha = \frac{x + y\sqrt{D}}{2},$$

so we have $\tau\tau^\sigma \mid (\alpha)(\alpha^\sigma)$. Therefore, we may assume that $\tau \mid (\alpha^\sigma)$, but $\tau \nmid (\alpha)$, because (α) and (α^σ) are relatively prime, by the above lemma. Then, we have the following:

Lemma 2.2. (Lemma 2 of [11]). *If ϵ is a p-th power residue mod τ, then the ideal (α) is not the p-th power of any principal ideal in K.*

Let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

be the prime decomposition of n. For each i $(1 \le i \le s)$, we fix a prime number ℓ_i, satisfying

$$\ell_i \equiv 1 \text{ (mod } 2p_i). \tag{2.4}$$

Suppose that we have a solution x, y, z of the equation (2.1), satisfying

(i)$'$ $(x, z) = 1$,

(ii)$'$ $\ell_i | z$, for $i = 1, 2, \ldots, s$,

(iii)$'$ x is a p_i-th power non-residue mod ℓ_i for $i = 1, 2, \ldots, s$.

Then, set

$$\alpha = \frac{x + y\sqrt{D}}{2}.$$

From Lemma 2.1, we have that $(\alpha) = \mathfrak{a}^n$ with an ideal $\mathfrak{a} \in K$, and every ℓ_i is decomposed in K as $\ell_i = \tau_i\tau_i^\sigma$. Assume that $\tau_i \mid (\alpha^\sigma)$. Denote by $[\mathfrak{a}]$ the ideal class containing α. Then, we have

$$[\mathfrak{a}]^n = [(\alpha)] = 1.$$

Proposition 2.3. *Let notations and assumptions be as above. If ϵ is a p_i-th power residue mod τ_i for every i $(1 \le i \le s)$, then the order of $[\mathfrak{a}]$ is equal to n.*

Proof. Assume that $[\mathfrak{a}]^m = 1$ for some m $(1 \le m < n)$. It is obvious that m is a divisor of n, so there exists at least one prime divisor p_i of n such that $mp_i \mid n$. Then, $[\mathfrak{a}]^{n/p_i} = 1$. Therefore, there exists an integer β in K such that $\mathfrak{a}^{n/p_i} = (\beta)$. Then, $(\alpha) = \mathfrak{a}^n = (\beta)^{p_i}$. However, this is impossible from Lemma 2.2. Therefore, we have $[\mathfrak{a}]^m \neq 1$ for $m = 1, 2, \ldots, n-1$. It follows that the order $[\mathfrak{a}]$ is equal to n. ■

Remark 2.4. In the case that $D < -4$, we do not require the condition on ϵ from Lemma 2.2 and Proposition 2.3, since $\epsilon = 1$.

3. Crucial Proposition

Take three systems of prime numbers $\{\ell_i\}$, $\{\ell'_i\}$, and $\{\ell''_i\}$, each satisfying the condition (2.4). Moreover, assume that ℓ_i, ℓ'_i, and ℓ''_i are pairwise distinct for every i $(1 \le i \le s)$. Our aim in this section is to prove the following proposition, which plays a crucial role in our derivation.

Proposition 3.1. *Let x, z, x', z', x'', and z'' constitute a non-trivial solution of the Diophantine equation*

$$X^2 - 4Z^n = X'^2 - 4Z'^n = X''^2 - 4Z''^n, \tag{3.1}$$

satisfying:

(i) $(x, z) = (x', z') = (x'', z'') = 1$,

(ii) $\ell_i | z$, $\ell' | z'$ *and* $\ell'' | z''$,

(iii) x *(resp.* x', x''*) is a* p_i*-th power non-residue mod* ℓ_i *(resp.* ℓ'_i, ℓ''_i*),*

(iv) $(x + x')/2$ *and* $(x + x'')/2$ *are* p_i*-th power residues mod* ℓ_i*,*

(v) $(x + x')/2$ *and* $(x' + x'')/2$ *are* p_i*-th power residues mod* ℓ'_i*,*

(vi) $(x' + x'')/2$ *and* $(x + x'')/2$ *are* p_i*-th power residues mod* ℓ''_i*,*

for every i $(1 \le i \le s)$*. Then, the ideal class group of the field*

$$K = \mathbb{Q}(\sqrt{x^2 - 4z^n})$$

has a subgroup N*, such that*

$$N \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \text{if } D < -4, \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \text{if } D > 0, \end{cases}$$

where D *is the discriminant of* K*.*

Proof. From equation 3.1, we set

$$x^2-4z^n=x'^2-4z'^n=x''^2-4z''^n=y^2D, \tag{3.2}$$

for some $y\in\mathbb{Z}$. Thus, we have

$$x^2-y^2D=4z^n, \tag{3.3}$$

$$x'^2-y^2D=4z'^n \tag{3.4}$$

and

$$x''^2-y^2D=4z''^n. \tag{3.5}$$

Therefore, we obtain three solutions (x,y,z), (x',y,z'), and (x'',y,z'') of the Diophantine equation (2.1). It follows from Lemma 2.1 that there are ideals $\mathfrak{a}$, $\mathfrak{a}'$, and $\mathfrak{a}''$ in K, such that $(\alpha)=\mathfrak{a}^n$, $(\alpha')=\mathfrak{a}'^n$, and $(\alpha'')=\mathfrak{a}''^n$, where

$$\alpha=\frac{x+y\sqrt{D}}{2},\alpha'=\frac{x'+y\sqrt{D}}{2}\text{ and }\alpha''=\frac{x''+y\sqrt{D}}{2}.$$

Let τ_i, τ_i', and τ_i'' $(1\le i\le s)$ be the prime ideals in K, such that

$$\ell_i=\tau_i\tau_i^\sigma\ \ \tau_i\mid(\alpha^\sigma),$$

$$\ell_i'=\tau_i'\tau_i'^\sigma\ \ \tau_i'\mid(\alpha'^\sigma),$$

$$\ell_i''=\tau_i''\tau_i''^\sigma\ \ \tau_i''\mid(\alpha''^\sigma).$$

Let R_i (resp. R_i' and R_i'') be the set of all integers in K that are a p_i-th power residue mod τ_i (resp. τ_i' and τ_i''). Since

$$\alpha\equiv x(\text{mod }\tau_i),\quad \alpha\equiv\frac{x+x'}{2}(\text{mod }\tau_i'),\quad \alpha\equiv\frac{x+x''}{2}(\text{mod }\tau_i''),$$
$$\alpha'\equiv\frac{x+x'}{2}(\text{mod }\tau_i),\quad \alpha'\equiv x'(\text{mod }\tau_i'),\quad \alpha'\equiv\frac{x'+x''}{2}(\text{mod }\tau_i''),$$

and

$$\alpha''\equiv\frac{x+x''}{2}(\text{mod }\tau_i),\quad \alpha'\equiv\frac{x'+x''}{2}(\text{mod }\tau_i'),\quad \alpha''\equiv x''(\text{mod }\tau_i''),$$

it follows form the conditions (iii)-(vi) of Proposition 3.1 that

$$\alpha\notin R_i,\quad \alpha\in R_i',\quad \alpha\in R_i'', \tag{3.6}$$

$$\alpha'\in R_i,\quad \alpha'\notin R_i',\quad \alpha'\in R_i'', \tag{3.7}$$

and

$$\alpha'' \in R_i, \quad \alpha'' \in R_i', \quad \alpha'' \notin R_i'', \tag{3.8}$$

for every i $(1 \leq i \leq s)$.

3.1. The case with $D < -4$.

It follows from Proposition 2.3 that the ideal classes $[\mathfrak{a}]$, $[\mathfrak{a}']$, and $[\mathfrak{a}'']$ have the same order n. Suppose that the following equation holds for $m, m', m'' > 0$:

$$[\mathfrak{a}]^m [\mathfrak{a}']^{m'} [\mathfrak{a}'']^{m''} = 1. \tag{3.9}$$

Then, there exists a number $\beta \in K$ such that

$$\mathfrak{a}^m \mathfrak{a}'^{(m')} \mathfrak{a}''^{(m'')} = (\beta). \tag{3.10}$$

Taking the n-th power of both sides of (3.10), we obtain

$$\alpha^m \alpha'^{(m')} \alpha''^{(m'')} = \pm\beta^n. \tag{3.11}$$

Define d_i by $p_i^{d_i} \| (m, m', m'')$, and e_i by $p_i^{e_i} \| n$ $(1 \leq i \leq s)$. We claim that $d_i \geq e_i$ for all i. Suppose that $d_i < e_i$ holds for some i, and set

$$m = p_i^d m_0, m' = p_i^d m_0', m'' = p_i^d m_0'', n = p_i^d n_0, \tag{3.12}$$

where $p_i \mid n_0$. It follows from (3.11) that

$$\alpha^{m_0} \alpha'^{(m_0')} \alpha''^{(m_0'')} = \pm\beta^{n_0}, \tag{3.13}$$

as K contains no root of 1 other than ± 1. Since $\alpha'^{(m_0')} \in R_i$, $\alpha''^{(m_0'')} \in R_i$, and $\pm\beta^{n_0} \in R_i$, we have that $\alpha^{m_0} \in R_i$. However, $\alpha \notin R_i$, so we have that $p_i \mid m_0$. Similarly, we also have that $p_i \mid m_0'$ and $p_i \mid m_0''$. Hence, and from (3.12), we have that $p_i^{d_i+1} \mid (m, m', m'')$. This contradicts the definition of d_i. Therefore, we have that $d_i \geq e_i$ for every i. Accordingly, we have that $n \mid m$, $n \mid m'$, and $n \mid m''$. Let N be the subgroup of the ideal class group generated by $[\mathfrak{a}]$, $[\mathfrak{a}']$, and $[\mathfrak{a}'']$. Then, N is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

3.2. The case with $D > 0$.

Let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

be the prime decomposition of n. We will show that the ideal class group of K has a subgroup isomorphic to $\mathbb{Z}/p^{e_i}\mathbb{Z} \times \mathbb{Z}/p^{e_i}\mathbb{Z}$ $(1 \leq i \leq s)$. Let ϵ be a fixed fundamental unit of K. Define

$$I := \{i \mid \epsilon \in R_i, 1 \leq i \leq s\},$$

$$I' := \{i \mid \epsilon \in R_i', 1 \leq i \leq s\},$$

and

$$I'' := \{i \mid \epsilon \in R_i'', 1 \leq i \leq s\}.$$

Then, let m, m', and m'' be the orders of the ideal classes $[\mathfrak{a}]$, $[\mathfrak{a}']$, and $[\mathfrak{a}'']$, respectively ($m \mid n$, $m' \mid n$, and $m'' \mid n$). It follows from Lemma 2.2 that m is a multiple of $\prod_{i\in I} p_i^{e_i}$. We claim that m' and m'' are multiples of $\prod_{i\notin I} p_i^{e_i}$. Assume that $p_i m' \mid n$, for some $i \notin I$. Then, there exists a number β in K such that

$$\mathfrak{a}'^{(n)} = (\alpha') = (\beta)^{p_i}.$$

Therefore, we have

$$\alpha' = \pm\epsilon^k \beta^{p_i} \text{ for some } k \in \mathbb{Z}.$$

Since $\alpha' \in R_i$, $\beta^{p_i} \in R_i$, and $\epsilon \notin R_i$, we obtain that $p_i \mid k$. It follows that $\pm\epsilon^k\beta^{p_i} \in R_i'$. Therefore, we see that $\alpha \in R_i'$. This is a contradiction. It follows that $p_i m' \nmid n$, for all $i \notin I$. Therefore, m' is a multiple of $\prod_{i\notin I} p_i^{e_i}$. Similarly, m'' is also a multiple of $\prod_{i\notin I} p_i^{e_i}$. By the same reasoning, we have that

$$\Big(\prod_{i\notin I'} p_i^{e_i}\Big)\Big|m, \ \Big(\prod_{i\in I'} p_i^{e_i}\Big)\Big|m', \text{ and } \Big(\prod_{i\notin I'} p_i^{e_i}\Big)\Big|m''.$$

In addition, we have

$$\Big(\prod_{i\notin I''} p_i^{e_i}\Big)\Big|m, \ \Big(\prod_{i\notin I''} p_i^{e_i}\Big)\Big|m', \text{ and } \Big(\prod_{i\in I''} p_i^{e_i}\Big)\Big|m''.$$

We claim that $p_j^{e_j}$ divides at least two of m, m', and m'', for each j.

3.2.1. Case 1 - $p_j^{e_j} \nmid m$

Without loss of generality, suppose that $p_j^{e_j} \nmid m$ for some j. We know that m is a multiple of $\Big(\prod_{i\notin I'} p_i^{e_i}\Big)$, and is also a multiple of $\Big(\prod_{i\notin I''} p_i^{e_i}\Big)$. Therefore,

$$p_j^{e_j} \nmid \Big(\prod_{i\notin I'} p_i^{e_i}\Big) \text{ and } p_j^{e_j} \nmid \Big(\prod_{i\notin I''} p_i^{e_i}\Big).$$

In other words,

$$p_j^{e_j} \Big| \Big(\prod_{i\in I'} p_i^{e_i}\Big) \text{ and } p_j^{e_j} \Big| \Big(\prod_{i\in I''} p_i^{e_i}\Big).$$

This implies that $p_j^{e_j}$ divides m' (resp. m''), and that j is contained in I' (resp. I''). Set $\tilde{n} := n/p_j^{e_j}$. Then, the ideal classes $[\mathfrak{a}'^{(\tilde{n})}]$ and $[\mathfrak{a}''^{(\tilde{n})}]$ have the same order, $p_j^{e_j}$. Suppose that the following equation holds for $m' >$ and $m'' > 0$:

$$[\mathfrak{a}'^{(\tilde{n})}]^{m'}[\mathfrak{a}''^{(\tilde{n})}]^{m''} = 1. \tag{3.14}$$

We know that a fundamental unit ϵ of K is a p_j-th power residue mod τ_j' and τ_j''. Then, we can show that the subgroup generated by $[\mathfrak{a}'^{(\tilde{n})}]$ and $[\mathfrak{a}''^{(\tilde{n})}]$ is isomorphic to $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$, in the same way as in the case where $D < -4$.

3.2.2. Case 2 - $p_j^{e_j}$ divides m, m' and m''

Next, we assume that $p_j^{e_j}$ divides m, m', and m''. Set $\tilde{n} := n/p_j^{e_j}$. For convenience, we will employ the following notations:

$$\tilde{\mathfrak{a}} := \mathfrak{a}^{\tilde{n}},\ \tilde{\mathfrak{a}}' := \mathfrak{a}'^{(\tilde{n})},\ \text{and}\ \tilde{\mathfrak{a}}'' := \mathfrak{a}''^{(\tilde{n})}.$$

Then, the ideal classes $[\tilde{\mathfrak{a}}]$, $[\tilde{\mathfrak{a}}']$, and $[\tilde{\mathfrak{a}}'']$ have the same order, $p_j^{e_j}$.

Without loss of generality, suppose that $\langle[\tilde{\mathfrak{a}}]\rangle \cap \langle[\tilde{\mathfrak{a}}']\rangle = 1$. Then, the subgroup generated by $[\tilde{\mathfrak{a}}]$ and $[\tilde{\mathfrak{a}}']$ is isomorphic to $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$. We are done.

Suppose that $\langle[\tilde{\mathfrak{a}}]\rangle \cap \langle[\tilde{\mathfrak{a}}']\rangle \neq 1$, i.e., $\langle[\tilde{\mathfrak{a}}]^{p_j^r}\rangle = \langle[\tilde{\mathfrak{a}}']^{p_j^r}\rangle$, for some r $(1 \leq r < e_j)$. This means that

$$[\tilde{\mathfrak{a}}]^{p_j^r s}[\tilde{\mathfrak{a}}']^{p_j^r} = 1, \tag{3.15}$$

for some integer s coprime to p_j. Then, there exists a number $\beta \in K$ such that

$$\tilde{\mathfrak{a}}^{p_j^r s} \cdot \tilde{\mathfrak{a}}'^{(p_j^r)} = (\beta). \tag{3.16}$$

Taking the $p_j^{(e_j-r)}$-th power of both sides of (3.16), we obtain

$$\pm\epsilon^k \alpha^s \alpha' = \beta^{p_j^{(e_j-r)}}. \tag{3.17}$$

As $e_j > r$, we have that $\pm\epsilon^k\alpha^s \in R_j$ and $\pm\epsilon^k\alpha' \in R_j'$. However, $\alpha \notin R_j$ and $\alpha' \notin R_j'$, so we have that $p_j \nmid k$. Because $\alpha^s \in R_j''$, $\alpha' \in R_j''$, and $\beta^{p_j^{(e_j-r)}} \in R_j''$, we have that $\epsilon^k \in R_j''$. Since k is relatively prime to p_j, we have that $\epsilon \in R_j''$. Suppose that $\langle[\tilde{\mathfrak{a}}]\rangle \cap \langle[\tilde{\mathfrak{a}}'']\rangle \neq 1$, i.e., $\langle[\tilde{\mathfrak{a}}]^{p_j^q}\rangle = \langle[\tilde{\mathfrak{a}}'']^{p_j^q}\rangle$, for some q $(1 \leq q < e_j)$. This implies that

$$[\tilde{\mathfrak{a}}]^{p_j^q t}[\tilde{\mathfrak{a}}'']^{p_j^q} = 1, \tag{3.18}$$

for some integer t that is relatively prime to p_j. Then, there exists a number $\gamma \in K$ such that

$$\tilde{\mathfrak{a}}^{p_j^q t} \cdot \tilde{\mathfrak{a}}''^{(p_j^q)} = (\gamma). \tag{3.19}$$

Taking the $p_j^{(e_j-q)}$-th power of both sides of (3.19), we obtain

$$\pm\epsilon^l \alpha^t \alpha'' = \gamma^{p_j^{(e_j-q)}}. \tag{3.20}$$

Since $e_j > q$, we have that $\pm\epsilon^l\alpha^t \in R_j$ and $\pm\epsilon^l\alpha'' \in R_j''$. We know that $\epsilon \in R_j''$. Therefore, we obtain that $\alpha'' \in R_j''$. This is a contradiction. Therefore, $\langle[\tilde{\mathfrak{a}}]\rangle$ and $\langle[\tilde{\mathfrak{a}}'']\rangle$ should only meet at the identity. It follows that the subgroup generated by $[\tilde{\mathfrak{a}}]$ and $[\tilde{\mathfrak{a}}'']$ is isomorphic to $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$. We are done.

In conclusion, K has a subgroup isomorphic to $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$ for all j. That is, K has a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. ■

4. Main Theorem

Let us recall the prime decomposition of n:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}.$$

We need one more lemma before we state our main theorem.

Lemma 4.1. *For each prime number $p_i \neq 2$, there exist infinitely many prime numbers ℓ, such that*

(a) $\ell \equiv 1 \pmod{2p_i}$,

(b) -1 *is an n-th power residue mod ℓ,*

(c) 2 *is a p_i-th power non-residue mod ℓ.*

Proof. Define $F := \mathbb{Q}(2^{1/p_i}, \zeta_{2n})$. Then, F is Galois over $\mathbb{Q}$. It follows from Chebotarev's density theorem that there exist infinitely many prime numbers ℓ, whose decomposition fields are equal to $\mathbb{Q}(\zeta_{2n})$. We can easily deduce that such primes ℓ satisfy the conditions of the lemma. ■

The lemma below is for the case where $p_i = 2$, for some i.

Lemma 4.2. *There exist infinitely many prime numbers ℓ, such that*

(a) $\ell \equiv 1 \pmod 4$,

(b) *the p_i^2's and -1 are n-th power residues mod ℓ,*

(c) $p_1^2 p_2^2 \cdots p_s^2 + 1$ *is not a square mod ℓ.*

Proof. Define

$$F := \mathbb{Q}\Big(p_1^{2/n}, p_2^{2/n}, ..., p_s^{2/n}, \zeta_{2n}\Big) \quad \text{and} \quad \hat{F} := F\Big(\sqrt{(p_1^2 p_2^2 \cdots p_s^2 + 1)}\Big).$$

Then, $\hat{F}$ is Galois over $\mathbb{Q}$. Since $p_1^2 p_2^2 \cdots p_s^2 + 1$ is not a square, and is relatively prime to n, $\sqrt{p_1^2 p_2^2 \cdots p_s^2 + 1} \notin F$. It follows from Chebotarev's density theorem that there exist infinitely many prime numbers ℓ, whose decomposition fields are equal to F. We can easily see that such ℓ's satisfy the conditions of the lemma. ■

Main theorem. *For any $n > 0$, there exist infinitely many real (resp. imaginary) quadratic number fields K such that the ideal class group of K has a subgroup which is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (resp. $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$).*

Proof. For each p_i, fix three prime numbers ℓ_i, ℓ_i', and ℓ_i'', satisfying the three conditions from Lemma 4.1 and Lemma 4.2. We will assume that all of the ℓ_i's, ℓ_i''s, and ℓ_i'' are distinct. Therefore, we can find an integer c_i (resp. a_i, b_i) such that $c_i^n \equiv -1 \mod \ell_i$ (resp. $a_i^n \equiv -1 \mod \ell_i'$, $b_i^n \equiv -1 \mod \ell_i''$) when $p_i \neq 2$. If p_i is equal to 2 for some i, we can find an integer c_i (resp. a_i, b_i) such that $c_i^n \equiv -(p_1 p_2 \cdots p_s)^2 \mod \ell_i$ (resp. $a_i^n \equiv -(p_1 p_2 \cdots p_s)^2 \mod \ell_i'$, $b_i^n \equiv -(p_1 p_2 \cdots p_s)^2 \mod \ell_i''$). By the Chinese remainder theorem, we can find integers A, B, and C, satisfying

$$\text{(4.1)} \qquad \begin{cases} A \equiv 0, B \equiv 1, C \equiv c_i & (\text{mod } \ell_i) \text{ for all } i, \\ A \equiv a_i, B \equiv 0, C \equiv 1 & (\text{mod } \ell_i') \text{ for all } i, \\ A \equiv 1, B \equiv b_i, C \equiv 0 & (\text{mod } \ell_i'') \text{ for all } i, \end{cases}$$

and

$$\text{(4.2)} \qquad \begin{cases} B \equiv 1, C \equiv 0 & (\text{mod } q) \text{ for } q \in \mathfrak{S}_A \setminus \{\ell_i\}, \\ C \equiv 0 & (\text{mod } q) \text{ for } q \in \mathfrak{S}_B \setminus \{\ell_i'\}, \\ C \equiv 1 & (\text{mod } q) \text{ for } q \in \mathfrak{S}_{(B^n - A^n)}, \end{cases}$$

where $\mathfrak{S}_m$ denotes the set of prime factors of an integer m. (It can easily be checked that $(A, B) = 1$ and $\{\ell_i\}$, $\{\ell_i'\}$, $\{\ell_i''\}$, $\mathfrak{S}_A \setminus \{\ell_i\}$, $\mathfrak{S}_B \setminus \{\ell_i'\}$, and $\mathfrak{S}_{(B^n - A^n)}$ are disjoint sets.)

Since $(A, B) = 1$ and $(C, B^n - A^n) = 1$, we have

$$\text{(4.3)} \qquad (A, B^n - C^n) = 1 \text{ and } (B, C^n - A^n) = 1.$$

4.1. Case 1 - Real quadratic number fields

We now set

$$\begin{cases} x = A^n + B^n - C^n, & z = AB, \\ x' = -A^n + B^n + C^n, & z' = BC, \\ x'' = A^n - B^n + C^n, & z'' = CA. \end{cases} \tag{4.4}$$

Then, we have

$$\begin{aligned} A^{2n} + B^{2n} + C^{2n} - 2(AB)^n - 2(BC)^n - 2(CA)^n =& x^2 - 4z^n \\ =& x'^2 - 4z'^n \\ =& x''^2 - 4z''^n, \end{aligned} \tag{4.5}$$

and

$$x \equiv \begin{cases} 2 & \text{(mod } \ell_i) \text{ if } p_i \neq 2, \\ p_1^2 p_2^2 \cdots p_s^2 + 1 & \text{(mod } \ell_i) \text{ if } p_i = 2, \end{cases} \qquad z \equiv 0, \text{ (mod } \ell_i),$$

$$x' \equiv \begin{cases} 2 & \text{(mod } \ell_i') \text{ if } p_i \neq 2, \\ p_1^2 p_2^2 \cdots p_s^2 + 1 & \text{(mod } \ell_i') \text{ if } p_i = 2, \end{cases} \qquad z' \equiv 0, \text{ (mod } \ell_i'),$$

$$x'' \equiv \begin{cases} 2 & \text{(mod } \ell_i'') \text{ if } p_i \neq 2, \\ p_1^2 p_2^2 \cdots p_s^2 + 1 & \text{(mod } \ell_i'') \text{ if } p_i = 2, \end{cases} \qquad z'' \equiv 0 \text{ (mod } \ell_i''),$$

for all i $(1 \leq i \leq s)$. In addition, we have

$$\frac{x + x'}{2} = B^n, \quad \frac{x' + x''}{2} = C^n, \quad \frac{x + x''}{2} = A^n.$$

From (4.3), we also have that $(x, z) = (x', z') = (x'', z'') = 1$. It follows from this that x, z, x', z', x'', z'' is a solution of the Diophantine equation (3.1), satisfying all of the conditions of Proposition 3.1 (note that $p_i | n$, for all $1 \leq i \leq s$). Since it holds that

$$\begin{aligned} x^2 - 4z^n &= A^{2n} + B^{2n} + C^{2n} - 2(AB)^n - 2(BC)^n - 2(CA)^n \\ &= C^{2n} - 2C^n(A^n + B^n) + (A^n - B^n)^2, \end{aligned} \tag{4.6}$$

and C is determined by a congruence condition, we can let the value $x^2 - 4z^n$ be positive, by choosing a suitable C. Now, we set $K = \mathbb{Q}(\sqrt{x^2 - 4z^n})$. It follows from Proposition 3.1 that the ideal class group of a real quadratic number field K has $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as a subgroup. The infinite property follows directly from the existence, as follows. Assume that there exist only a finite number of such K's, and denote the set of them by $\mathfrak{K}$. Let k be the maximum value of the class number of such K's (note that the class number is a finite ring of integers of number fields). Then, we can obtain $(nt)^2 > k$, by choosing a suitable t. Let K' be a real quadratic field, having a subgroup isomorphic to $\mathbb{Z}/nt\mathbb{Z} \times \mathbb{Z}/nt\mathbb{Z}$. Then, K' is also contained in $\mathfrak{K}$. This contradicts the maximality of k.

4.2. Case 2 - Imaginary quadratic number fields

Let t be a multiple of the product of all of prime numbers in

$$\{\ell_i\}, \{\ell_i'\}, \{\ell_i''\}, \mathfrak{S}_{[(B-A)^n-(C-A)^n]}, \mathfrak{S}_{[(B-A)^n-(B-A)^n]}, \text{ and } \mathfrak{S}_{[(C-A)^n-(C-B)^n]}.$$

From (4.3), we can check that

$$\begin{aligned} 1 &= \bigl(t-A, (B-A)^n-(C-A)^n\bigr) \\ &= \bigl(t-B, (B-A)^n-(B-C)^n\bigr) \\ &= \bigl(t-C, (C-A)^n-(C-B)^n\bigr). \end{aligned} \tag{4.7}$$

Now, we set

$$\begin{cases} x=(A-t)^n+(B-t)^n-(C-t)^n, & z=(A-t)(B-t), \\ x'=-(A-t)^n+(B-t)^n+(C-t)^n, & z=(B-t)(C-t), \\ x''=(A-t)^n-(B-t)^n+(C-t)^n, & z=(A-t)(C-t). \end{cases} \tag{4.8}$$

Then, we also have

$$x^2-4z^n = x'^2-4z'^n = x''^2-4z''^n, \tag{4.9}$$

and

$$x \equiv \begin{cases} 2 & \text{(mod } \ell_i\text{) if } p_i \neq 2, \\ p_1^2p_2^2\cdots p_s^2+1 & \text{(mod } \ell_i\text{) if } p_i = 2, \end{cases} \qquad z \equiv 0, \ \text{(mod } \ell_i\text{)},$$

$$x' \equiv \begin{cases} 2 & \text{(mod } \ell_i'\text{) if } p_i \neq 2, \\ p_1^2p_2^2\cdots p_s^2+1 & \text{(mod } \ell_i'\text{) if } p_i = 2, \end{cases} \qquad z' \equiv 0, \ \text{(mod } \ell_i'\text{)},$$

$$x'' \equiv \begin{cases} 2 & \text{(mod } \ell_i''\text{) if } p_i \neq 2, \\ p_1^2p_2^2\cdots p_s^2+1 & \text{(mod } \ell_i''\text{) if } p_i = 2, \end{cases} \qquad z'' \equiv 0 \text{ (mod } \ell_i''\text{)},$$

for all i $(1 \leq i \leq s)$. In addition, we have

$$\frac{x+x'}{2} = (B-t)^n, \frac{x'+x''}{2} = (C-t)^n, \frac{x+x''}{2} = (A-t)^n.$$

From (4.7), we also have $(x,z)=(x',z')=(x'',z'')=1$. It follows from this that x, z, x', z', x'', z'' is a solution of the Diophantine equation (3.1), satisfying all of the conditions of Proposition 3.1 (note that $p_i \mid n$ for all $1 \leq i \leq s$). Since it holds that

$$x^2-4z^n = -3t^{2n} + \{\text{terms of lower degree in } t\}, \tag{4.10}$$

we can let the value $x^2 - 4z^n$ be negative by taking a sufficiently large t. Now, set $K = \mathbb{Q}(\sqrt{x^2 - 4z^n})$. It follows from Proposition 3.1 that the ideal class group of an imaginary quadratic number field K has $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as a subgroup. The infinite property can be shown in the same way as for the previous case. ■

References

1. N. Ankeny and S. Chowla, On the divisibility of the class numbers of quadratic fields, *Pacific J. Math.*, **5** (1955), 321-324.
2. D. Byeon, Imaginary quadratic fields with noncyclic ideal class groups, *Ramanujan J.*, **11(2)** (2006), 159-163.
3. M. Craig, A construction for irregular discriminants, *Osaka J. Math.*, **14(2)** (1977), 365-402.
4. J. F. Mestre, *Courbes elliptiques et groups de classes d'idéaux de certains corps quadratiques*, Seminar on Number Theory, 1979-1980, Exp. No. 15, 18 pp., Univ. Bordeaux I, Talence, 1980.
5. J. F. Mestre, *Groupes de classes d'idéaux non cyclique de corps de nombre*, Seminar on Number Theory, Paris 1981-1982 (Paris, 1981/1982), Progr. Math., 38, Birkhäuser Boston, Boston, MA, 1983, pp. 189-200.
6. S. R. Louboutin, On the divisibility of the class number of imaginary quadratic number fields, *Proc. Amer. Math. Soc.*, **137(12)** (2009), 4025-4028.
7. M. R. Murty, Exponents of class groups of quadratic fields, in: *Topics in Number Theory,* (*University Park, PA, 1997*), Mathematical Applications, Vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 229-239.
8. T. Nagell, Über die Klassenzahl imaginar quadratischer Zahkörper, *Abh. Math. Seminar Univ. Hambrug*, **1** (1922), 140-150.
9. K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.*, **61(2)** (2000), 681-690.
10. P. Weinberger, Real quadratic fields with class numbers divisible by n, *J. Number Thoery*, **5** (1973), 237-241.
11. Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.*, **7** (1970), 57-76.
12. G. Yu, A note on the divisibility of class numbers of real quadratic fields, *J. Number Theory*, **97** (2002), 35-44.

Kwang-Seob Kim
School of Mathematics
Korea Institute for Advanced Study (KIAS) 85 Hoegiro
Seoul 130-722
Republic of Korea
E-mail: kwang12@kias.re.kr