Annales Univ. Sci. Budapest., Sect. Comp. 47 (2018) 179–183

CLASS GROUPS OF IMAGINARY QUADRATIC FIELDS OF 3-RANK AT LEAST 2

Kalyan Chakraborty and Azizul Hoque

(Allahabad, India)

Communicated by Imre Kátai

(Received February 20, 2018; accepted March 8, 2018)

Abstract. We produce an infinite family of imaginary quadratic fields whose ideal class groups have 3-rank at least 2.

1. Introduction

The class group of a number field is one of the fundamental and mysterious objects in algebraic number theory. Starting from Gauss, this topic has been received serious attention of many mathematicians. It is well known that there are infinitely many imaginary quadratic fields with class number divisible by a given integer $n \geq 2$ (cf. [9, 1]). A closely related problem is concerning the p-rank of class groups of imaginary quadratic fields (in fact, any number fields). A result of Y. Yamamoto [10, Proposition 2] gives the existence of infinitely many imaginary quadratic fields whose class groups have p-rank at least 2 for any integer $p \geq 2$. In [2], F. Diaz y Diaz developed an algorithm for generating imaginary quadratic fields whose class groups have 3-rank at least 2. In [3], the authors obtained a parameterized family of quadratic fields whose class group has 3-rank at least 2. In 2013, Y. Kishi [6] gave a family of imaginary quadratic fields whose 3-rank of the class group is at least 2. In [8], P. Llorente and J.

Key words and phrases: Quadratic fields, ideal class groups, ranks.
2010 Mathematics Subject Classification: 11R29, 11R11.
The Project is supported by SERB N-PDF (No. PDF/2017/001958), Govt. of India.

Quer found 1824, 20 and 3 imaginary quadratic fields whose 3-rank of the class groups are $4, 5$ and 6, respectively. The aim of this paper is to produce an infinitely family of imaginary quadratic fields whose class groups have 3-rank at least 2.

For any three positive integers k, ℓ and n, we consider the quadratic fields:

$$K_- = \mathbb{Q}(\sqrt{\ell^2 - 2\ell k^{3n}}) \text{ and } K_+ = \mathbb{Q}(\sqrt{3(2\ell k^{3n} - \ell^2)}).$$

In this paper, we prove the following:

Theorem 1.1. *Let $k \equiv 4 \pmod{135}$, $\ell \equiv 2 \pmod{135}$ and n be three odd positive integers such that $\ell < 2k^{3n}$ and $\gcd(k, \ell) = 1$. If $n \not\equiv 0 \pmod{3}$, then the 3-rank of the class groups of K_- is at least 2.*

It is easy to see that Theorem 1.1 yeilds infinitely many imaginary quadratic fields whose class groups has 3-rank at least 2. The idea of the proof is to construct real quadratic fields of the form K_+ whose class number is divisible by 3, and then apply the relation [6, Theorem 1] between the ranks of real and imaginary quadratic fields.

2. Proof of Theorem 1.1

We begin the proof with the following crucial proposition.

Proposition 2.1. *Let k, ℓ and n be as in Theorem 1.1. Then the class number of K_+ is divisible by 3.*

The conditions $\ell < 2k^{3n}$ and $n \not\equiv 0 \pmod{3}$ are not necessary in Proposition 2.1. Therefore, we can suppress these two conditions to get real as well as imagainary quadratic fields of the form K_+ with class number divisible by 3. We give the proof of Proposition 2.1 in the most general case, that is without counting these two conditions.

The following characterization of Y. Kishi and K. Miayke [5, Main Theorem] is one of the main ingredients in the proof of Proposition 2.1.

Theorem 2.2. *For any two integers u and v, let*

$$f_{u,v}(x) = x^3 - uvx - u^2. \tag{2.1}$$

If

(K-1) *u and v are relatively prime,*

(K-2) *$f_{u,v}(x)$ is irreducible over $\mathbb{Q}$,*

(K-3) *discriminant $D_{f_{u,v}}$ of $f_{u,v}(x)$ is not a perfect square in $\mathbb{Z}$,*

(K-4) *one of the following conditions holds:*

(K-4.1) $3 \nmid v$,

(K-4.2) $3 \mid v, \quad uv \not\equiv 3 \pmod 9, \quad u \equiv v \pm 1 \pmod 9$,

(K-4.3) $3 \mid v, \quad uv \equiv 3 \pmod 9, \quad u \equiv v \pm 1 \pmod{27}$,

then the normal closure of α, where α is a root of $f_{u,v}(x)$, is a cyclic, cubic, unramified extension of $\mathbb{K} = \mathbb{Q}(\sqrt{D_{f_{u,v}}})$; in particular, $\mathbb{K}$ has class number divisible by 3. Conversely, every quadratic number field $\mathbb{K}$ with class number divisible by 3 and every unramified, cyclic and cubic extension of $\mathbb{K}$ is given by a suitable choices of integers u and v.

Proof of Proposition 2.1

We choose $u = 2\ell$ and $v = 3k^n$. Then $\gcd(u, v) = 1$ since $\gcd(k, \ell) = 1$ and $\ell \equiv 2 \pmod 3$. Also by (2.1), we obtain:

$$f_{u,v}(x) = x^3 - 6\ell k^n x - 4\ell^2.$$

The discriminant of $f_{u,v}$ is

$$D_{f_{u,v}} = 144\ell^2 D,$$

where $D = 3\ell(2k^{3n} - \ell)$. As both k and ℓ are odd, we see that $D \equiv 3 \pmod 4$, and thus D is not a square in $\mathbb{Z}$.

Since $k \equiv 4 \pmod 5$ and $\ell \equiv 2 \pmod 5$, so that

$$f_{u,v}(x) \equiv x^3 + 2x - 1 \pmod 5.$$

Thus $f_{u,v}(x)$ is irreducible modulo 3 and hence it is irreducible as a polynomial with integer coefficients as well.

We again see that $3 \mid v$. As $m \equiv 4 \pmod 9$, we have $m^n \equiv 1, 4, 7 \pmod 9$ and thus $uv = 6\ell m^n = 3 \pmod 9$. Furthermore,

$$v + 1 = 3m^n + 1 \equiv 4 \equiv u \pmod{27}.$$

Thus we see that $f_{u,v}(x)$ satisfies the conditions (K-1)–(K-3) and (K-4.3). Therefore by Theorem 2.2 we complete the proof of Proposition 2.1. ■

We now extract the following proposition from [6, Theorem 1] which is needed in proving Theorem 1.1.

Proposition 2.3. *Let d be a square-free positive integer such that $d \not\equiv 0 \pmod 3$. Suppose r and s are the 3-ranks of the class groups of $\mathbb{Q}(\sqrt{-d})$ and $\mathbb{Q}(\sqrt{3d})$, respectively. Then $r = s+1$ if and only if there does not exist a triplet $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ satisfying the following conditions:*

(K-5) $x^2 - 4y^3 = 3z^2 d$,

(K-6) $\gcd(x, y) = 1$,

(K-7) $xyz \neq 0$,

(K-8) $y \equiv 1 \pmod 3$ *and* $x^2 \equiv 1, 7 \pmod 9$.

Proof of Theorem 1.1

Let r and s be the 3-ranks of K_- and K_+, respectively. To prove Theorem 1.1, it is sufficient to show $r = s + 1$ since $s \geq 1$ by Proposition 2.1.

We can express,

$$\ell^2 - 2\ell k^{3n} = -a^2 d, \tag{2.2}$$

where d is a square-free positive integer.

As $k \equiv 4 \pmod{27}$, so that $k^{3n} \equiv 10^n \pmod{27}$. Further $10^n \equiv 10, 19 \pmod{27}$ since $n \not\equiv 0 \pmod 3$. Therefore by reading (2.2) modulo 9, we see that $3 \mid a$. Furthermore reading (2.2) modulo 27, we obtain $a^2 d \equiv 9, 18 \pmod{27}$ and thus $d \equiv 1, 2 \pmod 3$ since a is odd and $3 \mid a$.

Let us assume that $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ be such that they satisfy all the conditions (K-5)–(K-8). Then reading the condition (K-5) modulo 4, we see that

$$x^2 \equiv 3z^2 \pmod 4.$$

This shows that both x and z are even.

Suppose that $x = 2u$ and $z = 2v$ for some positive integer u and v. Then the conditions (K-5)–(K-8) imply

$$u^2 - y^3 = 3v^2 d, \tag{2.3}$$

with $\gcd(u, y) = 1$, $uyv \neq 0$ and $u^2 \equiv 4, 7 \pmod 9$.

If y is odd, then u is even, and thus by (2.3), we see that v is odd, and hence reading (2.3) modulo 27 we arrive at a contradiction. Thus y is even and therefore u is odd. In this case reading (2.3) modulo 4, we obtain

$$1 \equiv 3v^2 \pmod 4$$

as $d \equiv 1 \pmod 4$. This is not possible. Thus we complete the proof. ■

Acknowledgements The second author is thankful to SERB, Govt. of India for their support under N-PDF scheme (No. PDF/2017/001758).
The authors are grateful of Professor Carl Erickson for his interests and comments on various aspects of related works in the literature.

References

[1] **Chakraborty, K., A. Hoque, Y. Kishi and P.P. Pandey,** Divisibility of the class numbers of imaginary quadratic fields, *J. Number Theory*, **185** (2018), 339–348.
[2] **Diaz y Diaz F.,** On some families of imaginary quadratic fields, *Math. Comp.*, **32** (1978), 637–650.
[3] **Erickson, C., N. Kaplan, N. Mendoza, A.M. Pacelli and T. Shayler,** Parameterized families of quadratic number fields with 3-rank at least 2, *Acta Arith.*, **130(2)** (2007), 141–147.
[4] **Hoque, A. and K. Chakraborty,** Divisibility of class numbers of certain families of quadratic fields, *J. Ramanujan Math. Soc.*, (2018), To appear.
[5] **Kishi, Y. and K. Miyake,** Parametrization of the quadratic fields whose class numbers are divisible by three, *J. Number Theory*, **80** (2000), 209–217.
[6] **Kishi, Y.,** On the 3-rank of the ideal class group of quadratic fields, *Kodai Math. J.*, **36** (2013), 275–283.
[7] **Llorente, P. and E. Nart,** Effective determination of the decomposition of the rational prime in a cubic field, *Proc. Amer. Math. Soc.*, **87** (1983), 579–585.
[8] **Llorente, P. and Quer, J.,** On the 3-Sylow subgroups of the class group of quadratic fields, *Math. Comp.*, **50** (1988), 321–333.
[9] **Nagell, T.,** Über die Klassenzahl imaginär quadratischer, Zählkörper, *Abh. Math. Sem. Univ. Hamburg.*, **1** (1922), 140–150.
[10] **Yamamoto, Y.,** On unramified Galois extensions of quadratic number fields, *Osaka J. Math.*, **7** (1970), 57–76.

K. Chakraborty and A. Hoque
Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhunsi, Allahabad 211 019
INDIA
kalyan@hri.res.in
azizulhoque@hri.res.in