Journal of Number Theory 185 (2018) 339–348

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Divisibility of the class numbers of imaginary quadratic fields

K. Chakraborty[a], A. Hoque[a], Y. Kishi[b,*], P.P. Pandey[c]

[a] *Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad 211019, India*
[b] *Department of Mathematics, Aichi University of Education, 1 Hirosawa Igaya-cho, Kariya, Aichi 448-8542, Japan*
[c] *Department of Mathematics, IISER Berhampur, Berhampur 760010, Odisha, India*

A R T I C L E I N F O

Article history:
Received 9 December 2016
Received in revised form 22 June 2017
Accepted 20 September 2017
Available online 16 October 2017
Communicated by L. Smajlovic

MSC:
11R11
11R29

Keywords:
Imaginary quadratic field
Class number
Ideal class group

A B S T R A C T

For a given odd integer $n > 1$, we provide some families of imaginary quadratic number fields of the form $\mathbb{Q}(\sqrt{x^2 - t^n})$ whose ideal class group has a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

* Corresponding author.
E-mail addresses: kalyan@hri.res.in (K. Chakraborty), azizulhoque@hri.res.in (A. Hoque), ykishi@auecc.aichi-edu.ac.jp (Y. Kishi), prem.p2506@gmail.com (P.P. Pandey).

https://doi.org/10.1016/j.jnt.2017.09.007

1. Introduction

The divisibility properties of the class numbers of number fields are very important for understanding the structure of the ideal class groups of number fields. For a given integer $n > 1$, the Cohen–Lenstra heuristic [3] predicts that a positive proportion of imaginary quadratic number fields have class number divisible by n. Proving this heuristic seems out of reach with the current state of knowledge. On the other hand, many families of (infinitely many) imaginary quadratic fields with class number divisible by n are known. Most of such families are of the type $\mathbb{Q}(\sqrt{x^2 - t^n})$ or of the type $\mathbb{Q}(\sqrt{x^2 - 4t^n})$, where x and t are positive integers with some restrictions (for the former see [1,10,11,13,16–19,22, 24], and for the later see [5,8,9,12,15,23]). Our focus in this article will be on the family $K_{t,x} = \mathbb{Q}(\sqrt{x^2 - t^n})$.

In 1922, T. Nagell [18] proved that for an odd integer n, the class number of imaginary quadratic field $K_{t,x}$ is divisible by n if t is odd, $(t, x) = 1$, and $q \mid x$, $q^2 \nmid x$ for all prime divisors q of n. Let b denote the square factor of $x^2 - t^n$, that is, $x^2 - t^n = b^2 d$, where $d < 0$ is the square-free part of $x^2 - t^n$. Under the condition $b = 1$, N.C. Ankeny and S. Chowla [1] (resp. M.R. Murty [16, Theorem 1], [17]) considered the family $K_{3,x}$ (resp. $K_{t,1}$, $K_{t,x}$). M.R. Murty also treated the family $K_{t,1}$ with $b < t^{n/4}/2^{3/2}$ ([16, Theorem 2]). Moreover, K. Soundararajan [22] (resp. A. Ito [10]) treated the family $K_{t,x}$ under the condition that $b < \sqrt{(t^n - x^2)/(t^{n/2} - 1)}$ holds (resp. all of prime divisors of b divide d). On the other hand, T. Nagell [19] (resp. Y. Kishi [13], A. Ito [11] and M. Zhu and T. Wang [24]) studied the family $K_{t,1}$ (resp. $K_{3,2^k}$, $K_{p,2^k}$ and $K_{t,2^k}$) unconditionally for b, where p is an odd prime. In the present paper, we consider the case when both t and x are odd primes and b is unconditional and prove the following:

Theorem 1.1. *Let $n \geq 3$ be an odd integer and p, q be distinct odd primes with $q^2 < p^n$. Let d be the square-free part of $q^2 - p^n$. Assume that $q \not\equiv \pm 1 \pmod{|d|}$. Moreover, we assume $p^{n/3} \neq (2q + 1)/3, (q^2 + 2)/3$ whenever both $d \equiv 1 \pmod 4$ and $3 \mid n$. Then the class number of $K_{p,q} = \mathbb{Q}(\sqrt{d})$ is divisible by n.*

In Table 1 (respectively Table 2), we list $K_{p,q}$ for small values of p, q for $n = 3$ (respectively for $n = 5$). It is readily seen from these tables that the assumptions in Theorem 1.1 hold very often. We can easily prove, by reading modulo 4, that the condition "$p^{n/3} \neq (2q + 1)/3, (q^2 + 2)/3$" in Theorem 1.1 holds whenever $p \equiv 3 \pmod 4$. Further, if we fix an odd prime q, then the condition "$q \not\equiv \pm 1 \pmod{|d|}$" in Theorem 1.1 holds almost always, and, this can be proved using the celebrated Siegel's theorem on integral points on affine curves. More precisely, we prove the following theorem in this direction.

Theorem 1.2. *Let $n \geq 3$ be an odd integer not divisible by 3. For each odd prime q the class number of $K_{p,q}$ is divisible by n for all but finitely many p's. Furthermore, for each q there are infinitely many fields $K_{p,q}$.*