Mohit Mishra

Lower bound for class numbers of certain real quadratic fields

Czechoslovak Mathematical Journal, Vol. 73 (2023), No. 1, 1–14

Persistent URL: `http://dml.cz/dmlcz/151500`

Czechoslovak Mathematical Journal, 73 (148) (2023), 1–14

LOWER BOUND FOR CLASS NUMBERS OF CERTAIN REAL QUADRATIC FIELDS

Mohit Mishra, Kanpur

Received July 28, 2021. Published online December 7, 2022.

Abstract. Let d be a square-free positive integer and $h(d)$ be the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$. We give an explicit lower bound for $h(n^2+r)$, where $r=1,4$. Ankeny and Chowla proved that if $g>1$ is a natural number and $d=n^{2g}+1$ is a square-free integer, then $g \mid h(d)$ whenever $n>4$. Applying our lower bounds, we show that there does not exist any natural number $n>1$ such that $h(n^{2g}+1)=g$. We also obtain a similar result for the family $\mathbb{Q}(\sqrt{n^{2g}+4})$. As another application, we deduce some criteria for a class group of prime power order to be cyclic.

Keywords: real quadratic field; class group; class number; Dedekind zeta values

MSC 2020: 11R29, 11R42, 11R11

1. Introduction

Throughout this paper $d=n^2+r$ will be a square-free integer. Let $h(d)$ and $\mathfrak{C}(k_n)$ denote the class number and the class group of a real quadratic field $k_n=\mathbb{Q}(\sqrt{d})$, respectively. The symbol $\mathcal{P}$ will always denote the principal ideal class in the class group and $N(\mathcal{I})$ denotes the norm of an ideal $\mathcal{I}$. By $p^t \mid\mid n$ we mean that $p^t \mid n$ but $p^{t+1} \nmid n$.

Gauss conjectured that there exist infinitely many real quadratic fields of class number 1, which is yet to be proved. More precisely, he conjectured that there exist infinitely many real quadratic fields of the form $\mathbb{Q}(\sqrt{p})$, $p \equiv 1 \pmod 4$, of class number 1. Much fruitful research have been done in this direction. In this connection, the following two conjectures were given by Chowla (see [10]) and Yokoi, see [25].

(C) If $m>26$ and $d=m^2+1$ is a prime, then $h(d)>1$.

This work is partially supported by the Infosys grant.

DOI: 10.21136/CMJ.2022.0264-21

(Y) Let $d = m^2 + 4$ be a square-free integer for some positive integer m. Then there exist exactly 6 real quadratic fields $\mathbb{Q}(\sqrt{d})$ of class number one, viz. $m \in \{1, 3, 5, 7, 13, 17\}$.

Mollin in [19] considered $m^2 + 1$ to be square-free and proved that:

Theorem 1.1. *If $m \neq 1, 2q$, where q is a prime, and $m^2 + 1$ is a square-free integer, then $h(m^2 + 1) > 1$.*

He also deduced that if $h(m^2 + 1) = 1$, then $m^2 + 1$ is a prime. Assuming the generalized Riemann hypothesis, Mollin and Williams in [20] proved (C) in 1988. Kim, Leu and Ono in [12] proved that at least one of (C) and (Y) is true, and for the other case at most 7 real quadratic fields $\mathbb{Q}(\sqrt{d})$ of class number 1 are there. Finally, Biró in [3], [4] proved (C) and (Y). For a given fixed number h, it is interesting to find necessary and sufficient conditions for a real quadratic field to have class number h. Yokoi in [25] established such a kind of criterion for $h = 1$ and he proved the following result:

Theorem 1.2. *The class number $h(4m^2 + 1) = 1$ if and only if $m^2 - t(t + 1)$ is a prime for all $1 \leqslant t \leqslant m - 1$.*

Byeon and Kim in [6], [7] obtained an equivalent criterion for R-D type real quadratic fields to have class number 1 and class number 2. In [8], the author along with Chakraborty and Hoque obtained analogous criteria for the class number to be 3. Some more interesting results on the class number one problem of R-D type fields can be found in the works of Biró and Lapkova, cf. [5], [15].

It is also interesting to find bounds for the class number of a number field. Hasse in [11] and Yokoi in [23], [24] studied lower bounds for class numbers of certain real quadratic fields. Mollin in [17], [18] generalized their results for certain real quadratic and bi-quadratic fields. The author along with Chakraborty and Hoque (see [9]) derived a lower bound for class number of $\mathbb{Q}(\sqrt{n^2 + r})$, where $r = 1, 4$, to classify the class group of order 4. The bound obtained was not so effective.

In this paper, we establish an efficient lower bound for the class number of $\mathbb{Q}(\sqrt{n^2 + r})$, where $r = 1, 4$. In particular, we prove the following results:

Theorem 1.3. *Let $d = n^2 + 1 \equiv 5 \pmod 8$ be a square-free integer, and let $n = 2{p_1}^{a_1}{p_2}^{a_2} \ldots {p_m}^{a_m}$ with p_i's distinct odd primes and a_i's some positive integers.*

(i) *If $m > 2$, then $h(d) \geqslant 2(a_1 + a_2 + \ldots + a_m) - m + 1$.*

(ii) *If $m = 2$, then $h(d) \geqslant 2(a_1 + a_2) - 2$.*

(iii) *If $n = 2p^t$, where p is an odd prime and $t \geqslant 1$ is an integer, then $h(d) \geqslant t$.*

Theorem 1.4. *Let $d = n^2 + 1 \equiv 1 \pmod 8$ be a square-free integer, and let $n = 2^s {p_1}^{a_1} {p_2}^{a_2} \dots {p_m}^{a_m}$, where p_i's are distinct odd primes, a_i's are positive integers and $s \geqslant 2$.*

(i) *If m is even, then $h(d) \geqslant 2(a_1 + a_2 + \dots + a_m) - m + 2s - 2$.*
(ii) *If $m > 1$ is odd, then $h(d) \geqslant 2(a_1 + a_2 + \dots + a_m) - m + 2s - 1$.*
(iii) *If $n = 2^s$, then $h(d) \geqslant s - 1$.*
(iv) *If $n = 2^s p^t$, where p is an odd prime, $s > 1$ and $t \geqslant 1$, then $h(d) \geqslant 2(t + s) - 4$.*

Theorem 1.5. *Let $d = n^2 + 1 \equiv 2 \pmod 4$ be a square-free integer, and let $n = {p_1}^{a_1} {p_2}^{a_2} \dots {p_m}^{a_m}$, with p_i's distinct odd primes and a_i's some positive integers.*

(i) *If $m \geqslant 2$, then $h(d) \geqslant 2(a_1 + a_2 + \dots + a_m) - m + 2$.*
(ii) *If $n = p^t$, with $t \geqslant 1$ an integer, then $h(d)$ is even and $h(d) \geqslant 2t$.*

We also obtain similar results for a square-free d of the form $n^2 + 4$.

In 1955, Ankeny and Chowla in [1] studied the divisibility problem for the real quadratic fields $\mathbb{Q}(\sqrt{n^{2g}+1})$ and proved that, if $g > 1$ is a natural number and $d = n^{2g} + 1$ is a square-free integer, then $g \mid h(d)$, whenever $n > 4$. Weinberger in [22] extended the above divisibility result for the class numbers of $\mathbb{Q}(\sqrt{n^{2g}+4})$ and proved that, if $g > 1$ is a natural number and $d = n^{2g} + 4$ is a square-free integer, then, for infinitely many n, (i) $(\frac{1}{2}g) \mid h(d)$, if g is even, (ii) $g \mid h(d)$, if g is odd. One can ask the following two questions related to the class number of the family $\mathbb{Q}(\sqrt{n^{2g}+1})$ and $\mathbb{Q}(\sqrt{n^{2g}+4})$:

Question. Let $g > 1$ be a fixed natural number.

(1) Does there exist a natural number $n > 1$ such that $h(n^{2g} + 1) = g$?
(2) Does there exist a natural number $n > 1$ such that

$$h(n^{2g} + 4) = \begin{cases} \dfrac{g}{2} & \text{if } g \text{ is even,} \\ g & \text{if } g \text{ is odd?} \end{cases}$$

By Brauer-Siegel theorem (see [14], page 321), there exist only finitely many real quadratic fields of the form $\mathbb{Q}(\sqrt{n^{2g}+1})$ or $\mathbb{Q}(\sqrt{n^{2g}+4})$ which have class number equal to g. However, Brauer-Siegel theorem is ineffective in finding out the exact values of n such that the class number of $\mathbb{Q}(\sqrt{n^{2g}+1})$ or $\mathbb{Q}(\sqrt{n^{2g}+4})$ equals g. Applying our lower bounds, we obtain the following two results related to above question:

Theorem 1.6. *Let $g > 1$ be a natural number and let $d = n^{2g} + 1$ be a square-free integer. Then, for all $n > 1$, $h(d) > g$, i.e., there does not exist any natural number $n > 1$ such that $h(n^{2g} + 1) = g$.*

Theorem 1.7. *Let $g > 1$ be a natural number, and let $d = n^{2g}+4$ be a square-free integer.*

(i) *If g is even, then $h(d) \neq \frac{1}{2}g$.*

(ii) *If g is odd and n is not a prime, then $h(d) \neq g$. Moreover, if g is even and n is not a prime, then $h(d) > g$, i.e., $h(d) \neq g$.*

However, when g is even, there do exist primes p such that $d = p^{2g}+4$ is square-free and $h(d) = g$. For example, for $g = 2$, $h(3^4 + 4) = 2$ and $h(5^4 + 4) = 2$.

As an application of our lower bounds, we also give some criteria for the prime power order class group of a real quadratic field $\mathbb{Q}(\sqrt{n^2 + r})$, where $r = 1, 4$, to be cyclic.

Chowla and Friedlander in [10] proved that if $m^2 + 1$ is a prime with $m > 2$ and $h(m^2+1) = 1$, then $g(m^2+1)$ is $\frac{1}{2}m$, where $g(n)$ is the least prime which is a quadratic residue of n. We generalize this result and give an upper bound on $g(1+4p^2)$, where p is a prime and $h(1+4p^2) > 1$, and for $g(p^2+4)$, where p is a prime and $h(p^2+4) > 1$.

In Section 2 we state the results on computing the partial Dedekind zeta values of a real quadratic field. In Sections 3 and 4 we compute the partial Dedekind zeta values and with some group theoretic arguments we deduce a lower bound for the class number of $\mathbb{Q}(\sqrt{n^2 + r})$ for $r = 1, 4$. In Section 5 we give the proof of Theorems 1.6 and 1.7. Further, in Section 5 we study the structure of class group of prime power order. Finally, we conclude with some remarks.

2. Partial Dedekind zeta values

Let k be a real quadratic field, and let $\zeta_k(s)$ be the Dedekind zeta function attached to k. Siegel in [21] derived an expression for the Dedekind zeta values at $1 - 2n$, where n is a positive integer. For $n = 1$, this expression becomes simpler:

Proposition 2.1. *Let D be the discriminant of k. Then*

$$\zeta_k(-1) = \frac{1}{60} \sum_{\substack{|t|<\sqrt{D} \\ t^2 \equiv D \pmod 4}} \sigma\Big(\frac{D - t^2}{4}\Big),$$

where $\sigma(n)$ denotes the sum of divisors of n.

Lang gave another method to compute $\zeta_k(-1)$ by computing partial Dedekind zeta values and summing them up. For an ideal class $\mathfrak{A}$ of k, consider an integral ideal $\mathfrak{a}$ in $\mathfrak{A}^{-1}$ with integral basis $\{r_1, r_2\}$. Let r_1' and r_2' be the conjugates of r_1 and r_2, respectively, and

$$\delta(\mathfrak{a}) := r_1 r_2' - r_1' r_2.$$

Let ε be the fundamental unit of k. Then one has a matrix $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with integer entries satisfying:

$$\varepsilon \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = M \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}.$$

We recall Lang's result in [13].

Theorem 2.1. *By keeping the above notations, we have*

$$\begin{aligned}\zeta_k(-1, \mathfrak{A}) = \frac{\operatorname{sgn} \delta(\mathfrak{a}) r_2 r_2'}{360 N(\mathfrak{a}) c^3} \{&(a+d)^3 - 6(a+d)N(\varepsilon) - 240c^3(\operatorname{sgn} c)S^3(a,c) \\ &+ 180ac^3(\operatorname{sgn} c)S^2(a,c) - 240c^3(\operatorname{sgn} c)S^3(d,c) + 180dc^3(\operatorname{sgn} c)S^2(d,c)\},\end{aligned}$$

where $S^i(-,-)$ denotes the generalized Dedekind sum as defined in [2].

In order to apply Theorem 2.1, one needs to know a, b, c, d and the generalized Dedekind sums. The following result (see [13], page 143, equation (2.15)) helps us to determine a, b, c and d.

Lemma 2.1. *With the same notations as above, we have*

$$M = \begin{bmatrix} \operatorname{Tr}\left(\dfrac{r_1 r_2' \varepsilon}{\delta(\mathfrak{a})}\right) & \operatorname{Tr}\left(\dfrac{r_1 r_1' \varepsilon'}{\delta(\mathfrak{a})}\right) \\ \operatorname{Tr}\left(\dfrac{r_2 r_2' \varepsilon}{\delta(\mathfrak{a})}\right) & \operatorname{Tr}\left(\dfrac{r_1 r_2' \varepsilon'}{\delta(\mathfrak{a})}\right) \end{bmatrix}$$

Moreover, $bc \neq 0$ *and* $\det(M) = N(\varepsilon)$.

Lastly, we recall the following result on generalized Dedekind sums, see, [13], page 155, equations (4.3)–(4.4).

Lemma 2.2. *For any positive integer m, we have*
(i) $S^3(\pm 1, m) = \pm(-m^4 + 5m^2 - 4)/120m^3$.
(ii) $S^2(\pm 1, m) = (m^4 + 10m^2 - 6)/180m^3$.

3. The field $\mathbb{Q}(\sqrt{n^2+1})$

In this case, the fundamental unit is $\varepsilon = n + \sqrt{n^2+1}$ and $N(\varepsilon) = -1$. We also know that if an odd prime p divides n, then p splits in k_n as

$$(3.1) \qquad (p) = \begin{cases} \left(p, \dfrac{1+\sqrt{d}}{2}\right)\left(p, \dfrac{1-\sqrt{d}}{2}\right) & \text{if } n^2+1 \equiv 1 \pmod 4, \\ (p, 1+\sqrt{d})(p, 1-\sqrt{d}) & \text{if } n^2+1 \equiv 2 \pmod 4. \end{cases}$$

By Theorem 2.3 of [6], we have

$$\zeta_{k_n}(-1,\mathcal{P}) = \begin{cases} \dfrac{n^3+14n}{360} & \text{if } n^2+1 \equiv 1 \pmod 4, \\ \dfrac{4n^3+11n}{180} & \text{if } n^2+1 \equiv 2 \pmod 4. \end{cases} \tag{3.2}$$

We first find the integral basis of some particular ideals. Using this and Theorem 2.1, we calculate the partial Dedekind zeta values for some ideal classes of k_n. Then we compare these Dedekind zeta values and use some elementary group theoretic arguments to establish our results.

Lemma 3.1. *Let p be an odd prime, $p^t \parallel n$, and let $n^2+1 \equiv 1 \pmod 4$. Consider $\mathfrak{a} = (p, \frac{1}{2}(1+\sqrt{d}))$ and $\mathfrak{a}' = (p, \frac{1}{2}(1-\sqrt{d}))$. Then $\{p^r, \frac{1}{2}(1+\sqrt{d})\}$ and $\{p^r, \frac{1}{2}(1-\sqrt{d})\}$ are integral bases for $\mathfrak{a}^r$ and $(\mathfrak{a}')^r$, respectively, for all $1 \leqslant r \leqslant t$.*

Proof. Consider

$$M_r = \left[p^r, \frac{1+\sqrt{d}}{2}\right],$$

a nonzero $\mathbb{Z}$-module in $\mathcal{O}_{k_n}$. Then, by [16], Propositions 2.6 and 2.11, M_r is an ideal and $N(M_r) = p^r$ for all $1 \leqslant r \leqslant t$. As $N(\mathfrak{a}^r) = p^r$ and $M_r \subseteq \mathfrak{a}^r$ for all $1 \leqslant r \leqslant t$, therefore, $M_r = \mathfrak{a}^r$. Hence, $\{p^r, \frac{1}{2}(1+\sqrt{d})\}$ is an integral basis for $\mathfrak{a}^r$ for all $1 \leqslant r \leqslant t$. Similarly, if $M'_r = [p^r, \frac{1}{2}(1-\sqrt{d})]$, then $M'_r = (\mathfrak{a}')^r$, and $\{p^r, \frac{1}{2}(1-\sqrt{d})\}$ is an integral basis for $(\mathfrak{a}')^r$ for all $1 \leqslant r \leqslant t$. □

Now if we consider nonzero $\mathbb{Z}$-modules $N_r = [p^r, 1+\sqrt{d}]$ and $N'_r = [p^r, 1-\sqrt{d}]$ in $\mathcal{O}_{k_n}$, where $n^2+1 \equiv 2 \pmod 4$, then, as before, one can prove the following:

Lemma 3.2. *Let p be an odd prime, $p^t \parallel n$, and let $n^2+1 \equiv 2 \pmod 4$. Consider $\mathfrak{a} = (p, 1+\sqrt{d})$ and $\mathfrak{a}' = (p, 1-\sqrt{d})$. Then $\{p^r, 1+\sqrt{d}\}$ and $\{p^r, 1-\sqrt{d}\}$ are integral bases for $\mathfrak{a}^r$ and $(\mathfrak{a}')^r$, respectively, for all $1 \leqslant r \leqslant t$.*

We derive our results in three subsections based on the congruence relations, i.e., $n^2+1 \equiv 1, 2, 5 \pmod 8$.

3.1. Congruence $n^2+1 \equiv 5 \pmod 8$.

We have $n^2 \equiv 4 \pmod 8 \Rightarrow n = 2n_0$, where n_0 is an odd integer.

Proof of Theorem 1.3 (iii). By (3.1) p splits in k_n, so let $\mathcal{A}$ be an ideal class containing $\mathfrak{a} = (p, \frac{1}{2}(1+\sqrt{d}))$. Then $\mathfrak{a}' = (p, \frac{1}{2}(1-\sqrt{d})) \in \mathcal{A}^{-1}$ and, by Lemma 3.1, $\{p^r, \frac{1}{2}(1+\sqrt{d})\}$ and $\{p^r, \frac{1}{2}(1-\sqrt{d})\}$ are integral bases for $\mathfrak{a}^r$ and $(\mathfrak{a}')^r$ for all $1 \leqslant r \leqslant t$. Now by using Lemmas 2.1, 2.2 and Theorem 2.1, we get

$$\zeta_{k_n}(-1,\mathcal{A}^r) = \frac{n^3 + n(4p^{4r}+10p^{2r})}{360p^{2r}} = \zeta_{k_n}(-1,\mathcal{A}^{-r}) \quad \forall\, 1 \leqslant r \leqslant t.$$

If for any $1 \leqslant r \leqslant t$, $\mathcal{A}^r = \mathcal{P}$, then $\zeta_{k_n}(-1, \mathcal{A}^r) = \zeta_{k_n}(-1, \mathcal{P})$, which gives $n = 2p^r$. Therefore, $\mathcal{A}^r$ is a non-principal ideal class for all $1 \leqslant r < t$. This implies $|\mathcal{A}| \geqslant t$ and hence $h(d) \geqslant t$. □

Proof of Theorem 1.3 (i). Since each p_i splits in k_n, as in (3.1), let $\mathcal{A}_i$ be the ideal class containing $\mathfrak{a}_i = (p_i, \frac{1}{2}(1+\sqrt{d}))$. Then again by using Lemmas 2.1, 2.2 and Theorem 2.1,

$$\zeta_{k_n}(-1, \mathcal{A}_i^{r_i}) = \frac{n^3 + n(4p_i^{4r_i} + 10p_i^{2r_i})}{360p_i^{2r_i}} = \zeta_{k_n}(-1, \mathcal{A}_i^{-r_i})$$

for all $1 \leqslant i \leqslant m$ and $1 \leqslant r_i \leqslant a_i$. Comparing the values of $\zeta_{k_n}(-1, \mathcal{A}_i^{r_i})$ and $\zeta_{k_n}(-1, \mathcal{P})$, we get that $\mathcal{A}_i^{r_i}$ are distinct nonprincipal ideal classes for all $1 \leqslant i \leqslant m$ and $1 \leqslant r_i \leqslant a_i$. If for any $1 \leqslant i \leqslant m$, $1 \leqslant r_i$, $s_i \leqslant a_i$ and $r_i \neq s_i$ we get $\zeta_{k_n}(-1, \mathcal{A}_i^{r_i}) = \zeta_{k_n}(-1, \mathcal{A}_i^{-s_i})$, then we have $n = 2p^{r_i+s_i}$, which is not possible. This implies that $\mathcal{A}_i^{r_i} \neq \mathcal{A}_i^{-s_i}$ for all $1 \leqslant i \leqslant m$, $1 \leqslant r_i$, $s_i \leqslant a_i$ and $r_i \neq s_i$. Therefore, $|\mathcal{A}_i| \geqslant 2a_i$, and hence, $h(d) \geqslant 2(a_1 + a_2 + \ldots + a_m) - m + 1$. □

The other part can be proved along the same lines.

Remark 3.1. If all the a_i's and t are zero, then $n_0 = 1$. Hence, $d = 5$ and $h(5) = 1$.

3.2. Congruence $n^2 + 1 \equiv 1 \pmod 8$. In this case, $4 \mid n$ and 2 splits in k_n as

$$(2) = \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right). \tag{3.3}$$

Proof of Theorem 1.4 (iv). Let $\mathcal{A}$ and $\mathcal{B}$ be the two ideal classes in k_n such that $\mathfrak{a} = (p, \frac{1}{2}(1+\sqrt{d})) \in \mathcal{A}$ and $\mathfrak{b} = (2, \frac{1}{2}(1+\sqrt{d})) \in \mathcal{B}$. Then as before,

$$\zeta_{k_n}(-1, \mathcal{A}^r) = \frac{n^3 + n(4p^{4r} + 10p^{2r})}{360p^{2r}} = \zeta_{k_n}(-1, \mathcal{A}^{-r}) \quad \forall 1 \leqslant r \leqslant t,$$

and

$$\zeta_{k_n}(-1, \mathcal{B}^j) = \frac{n^3 + n(4 \times 2^{4j} + 10 \times 2^{2j})}{360 \times 2^{2j}} = \zeta_{k_n}(-1, \mathcal{B}^{-j}) \quad \forall 1 \leqslant j \leqslant s-1.$$

If $\zeta_{k_n}(-1, \mathcal{P}) = \zeta_{k_n}(-1, \mathcal{A}^r)$, then $n = 2p^r$. This shows that $\mathcal{A}^r$ is a non-principal ideal class for all $1 \leqslant r \leqslant t$. As $\zeta_{k_n}(-1, \mathcal{A}^r) = \zeta_{k_n}(-1, \mathcal{A}^{-r})$ and we have $\zeta_{k_n}(-1, \mathcal{A}^r) \neq \zeta_{k_n}(-1, \mathcal{A}^s)$ for all $1 \leqslant r, s \leqslant t$, $r \neq s$, hence $\mathcal{A}^r \neq \mathcal{A}^{-s}$ for all $1 \leqslant r, s \leqslant t$ and $r \neq s$. Thus, $|\mathcal{A}| \geqslant 2t$. Now if $\zeta_{k_n}(-1, \mathcal{P}) = \zeta_{k_n}(-1, \mathcal{B}^j)$, we get $n = 2 \times 2^j$, therefore as above, $|\mathcal{B}| \geqslant 2(s-1)$. And if $\zeta_{k_n}(-1, \mathcal{A}^r) = \zeta_{k_n}(-1, \mathcal{B}^j)$, we have $n = 2 \times 2^j p^r$, this is only possible when $r = t$ and $j = s-1$. So, while calculating class number we have to take care of $\mathcal{A}^t$ and $\mathcal{B}^{s-1}$ as they may be equal and we have to count them once. Hence, $h(d) \geqslant (2t-1) + (2(s-1)-1) + 1 - 1$, i.e., $h(d) \geqslant 2(t+s) - 4$. □

Using similar arguments, one can prove the other parts as well.

3.3. Congruence $d = n^2 + 1 \equiv 2 \pmod 4$**.** In this case, we have $n^2 + 1 \equiv 2 \pmod 4$ and n is odd. If $\mathfrak{a} = (p, 1 + \sqrt{d}) \in \mathcal{A}$, then as before, using Lemmas 2.1, 2.1, 3.2 and Theorem 2.1, we get

$$\zeta_{k_n}(-1, \mathcal{A}^r) = \frac{8n^3 + n(2p^{4r} + 20p^{2r})}{360p^{2r}} = \zeta_{k_n}(-1, \mathcal{A}^{-r}) \quad \forall\, 1 \leqslant r \leqslant t. \tag{3.4}$$

Proof of Theorem 1.5 (ii). If $d \equiv 2 \bmod 4$, then 2 ramifies in $k_n = \mathbb{Q}(\sqrt{d})$, i.e.,

$$(2) = (2, \sqrt{d})^2.$$

If $\mathfrak{b} = (2, \sqrt{d})$ is in ideal class $\mathcal{B}$, then by [6], Theorem 2.3 we have

$$\zeta_{k_n}(-1, \mathcal{B}) = \frac{2n^3 + 28n}{360}.$$

Also if $\zeta_{k_n}(-1, \mathcal{P}) = \zeta_{k_n}(-1, \mathcal{B})$, then $d = 2$. Therefore, $\mathcal{B}$ is a nonprincipal ideal class and $|\mathcal{B}| = 2$. Hence, $h(d)$ is even.

Now if $\mathfrak{a} = (p, 1 + \sqrt{d}) \in \mathcal{A}$, then by (3.4) we have

$$\zeta_{k_n}(-1, \mathcal{A}^r) = \frac{8n^3 + n(2p^{4r} + 20p^{2r})}{360p^{2r}} = \zeta_{k_n}(-1, \mathcal{A}^{-r}) \quad \forall\, 1 \leqslant r \leqslant t.$$

Now if $\zeta_{k_n}(-1, \mathcal{P}) = \zeta_{k_n}(-1, \mathcal{A}^r)$, then $n = \frac{1}{2}p^r$, which is not possible. Therefore, $\mathcal{A}^r$ is a nonprincipal ideal class, for all $1 \leqslant r \leqslant t$. Also $\zeta_{k_n}(-1, \mathcal{A}^r) = \zeta_{k_n}(-1, \mathcal{A}^{-r})$ for all $1 \leqslant r \leqslant t$, and if $\zeta_{k_n}(-1, \mathcal{A}^r) = \zeta_{k_n}(-1, \mathcal{A}^s)$, where $1 \leqslant r, s \leqslant t$ and $r \neq s$, then $n = \frac{1}{2}p^{r+s}$, which is again not possible. This gives $|\mathcal{A}| \geqslant 2t$ and hence $h(d) \geqslant 2t$. □

Following similar arguments, one can prove the other part as well.

Remark 3.2. If all the a_i's and t are zero, then $n = 1$ and $d = 2$. Hence, $h(2) = 1$.

4. The field $\mathbb{Q}(\sqrt{n^2 + 4})$

We now study the class number of $k_n = \mathbb{Q}(\sqrt{d})$, where $d = n^2 + 4$ is a squarefree positive integer. Clearly $d \equiv 5 \pmod 8$ and n is odd. In this case, $\varepsilon = \frac{1}{2}(n + \sqrt{n^2 + 4})$, and $N(\varepsilon) = -4$. Let $p \mid n$ then

$$(p) = \left(p, \frac{p + 2 + \sqrt{d}}{2}\right)\left(p, \frac{p + 2 - \sqrt{d}}{2}\right). \tag{4.1}$$

By Theorem 2.3 of [6], we also know that

$$\zeta_{k_n}(-1, \mathcal{P}) = \frac{n^3 + 11n}{360}. \tag{4.2}$$

Lemma 4.1. *Let p be an odd prime, $p^t \parallel n$, and let $n^2+4 \equiv 5 \pmod 8$. Consider $\mathfrak{a} = (p, \frac{1}{2}(p+2+\sqrt{d})$ and $\mathfrak{a}' = (p, \frac{1}{2}(p+2-\sqrt{d}))$. Then $\{p^r, \frac{1}{2}(p+2+\sqrt{d})\}$ and $\{p^r, \frac{1}{2}(p+2-\sqrt{d})\}$ are integral bases for $\mathfrak{a}^r$ and $(\mathfrak{a}')^r$, respectively, for all $1 \leqslant r \leqslant t$.*

Proof. Consider

$$M_r = \left[p^r, \frac{p^r+2+\sqrt{d}}{2}\right],$$

a nonzero $\mathbb{Z}$-module in $\mathcal{O}_{k_n}$. Then, by Propositions 2.6 and 2.11 of [16], M_r is an ideal and $N(M_r) = p^r$. As $M_r \subseteq \mathfrak{a}^r$ for all $1 \leqslant r \leqslant t$ and $N(\mathfrak{a}^r) = p^r$, one has $M_r = \mathfrak{a}^r$ and hence $\{p^r, \frac{1}{2}(p+2+\sqrt{d})\}$ is an integral basis for $\mathfrak{a}^r$ for all $1 \leqslant r \leqslant t$. Similarly $\{p^r, \frac{1}{2}(p+2-\sqrt{d})\}$ is an integral basis for $(\mathfrak{a}')^r$ for all $1 \leqslant r \leqslant t$. □

Theorem 4.1. *If $n = p^t$ with p an odd prime and $t \geqslant 1$ an integer then $h(d) \geqslant t$.*

Proof. Let $\mathcal{A}$ be an ideal class containing $\mathfrak{a} = (p, \frac{1}{2}(p+2+\sqrt{d}))$. Then by using Lemmas 2.1, 2.2, 4.1 and Theorem 2.1 we obtain:

$$\zeta_{k_n}(-1, \mathcal{A}^r) = \frac{n^3 + n(p^{4r} + 10p^{2r})}{360p^{2r}} = \zeta_{k_n}(-1, \mathcal{A}^{-r}) \quad \forall\, 1 \leqslant r \leqslant t.$$

If for any $1 \leqslant r < t$, $\zeta_{k_n}(-1, \mathcal{P}) = \zeta_{k_n}(-1, \mathcal{A}^r)$, then $n = p^r$. Hence, $|\mathcal{A}| \geqslant t$. This implies that $h(d) \geqslant t$. □

Using similar arguments one gets:

Theorem 4.2. *Let $n = {p_1}^{a_1}{p_2}^{a_2}\ldots{p_m}^{a_m}$ with p_i's distinct odd primes and a_i's some positive integers.*

(i) *If $m > 2$, then $h(d) \geqslant 2(a_1 + a_2 + \ldots + a_m) - m + 1$.*

(ii) *If $m = 2$, then $h(d) \geqslant 2(a_1 + a_2) - 2$.*

Remark 4.1. If all the a_i's are zero, then $n = 1$, $d = 5$ and $h(5) = 1$.

5. Applications

5.1. Proof of Theorems 1.6 and 1.7.

Proof of Theorem 1.6. If n is odd, then $n^{2g} + 1 \equiv 2 \pmod 4$. Therefore, by Theorem 1.5, $h(n^{2g} + 1) > g$. Assume n is even. Then $n^{2g} + 1 \equiv 1 \pmod 8$, since $g > 1$ and $2^{2g} \mid n^{2g}$. If there exists an odd prime p dividing n, then $h(d) > g$ (by Theorem 1.4). Now suppose $n = 2^s$, then $n^g = 2^{sg}$. By Theorem 1.4, $h(d) \geqslant sg - 1$. If $s > 1$, then $sg - 1 > g$. Hence, $h(d) > g$.

Now consider $s=1$ and $\mathfrak{b}=(2,\frac{1}{2}(1+\sqrt{d}))\in\mathcal{B}$. Then, as in the proof of Theorem 1.4,

$$\zeta_{k_n}(-1,\mathcal{B}^j)=\frac{n^3+n(4\times 2^{4j}+10\times 2^{2j})}{360\times 2^{2j}}=\zeta_{k_n}(-1,\mathcal{B}^{-j})\quad\forall\, 1\leqslant j\leqslant g-1,$$

and $|\mathcal{B}|\geqslant g-1$. If $h(d)=g>2$, then $|\mathcal{B}|=g$. Also, if $h(d)=g=2$ and $\mathcal{B}$ is principal ideal class, then $\zeta_{k_n}(-1,\mathcal{P})=\zeta_{k_n}(-1,\mathcal{B})$ which further implies $n=4$. But $h(4^2+1)=1$, therefore, if $h(d)=2$, then $|\mathcal{B}|=2$. Hence, if $h(d)=g>1$, then $|\mathcal{B}|=g$. Therefore, $\mathcal{B}^l\mathcal{B}^{g-l}=\mathcal{P}$, i.e., $(\mathcal{B}^l)^{-1}=\mathcal{B}^{g-l}$. This implies that $\zeta_{k_n}(-1,\mathcal{B}^l)=\zeta_{k_n}(-1,\mathcal{B}^{g-l})$, i.e.,

$$\frac{n^3+n(4\times 2^{4l}+10\times 2^{2l})}{360\times 2^{2l}}=\frac{n^3+n(4\times 2^{4(g-l)}+10\times 2^{2(g-l)})}{360\times 2^{2(g-l)}},$$

which gives $n=2^{g+1}$, a contradiction. Hence, $h(d)>g$. □

Proof of Theorem 1.7. The proof is a direct consequence of Theorems 4.1– 4.2. □

5.2. Class group of prime power order. In this section, we deduce conditions on the exponents of the prime factors of n so that the class group of prime power order is cyclic.

Throughout this subsection, p and p_i's will be distinct odd primes and s, m and t will be positive integers. Also, d will be a square-free positive integer and $h(d)=q^r$ for some prime q and positive integer $r\geqslant 2$.

Theorem 5.1. *Let p be an odd prime, $t\geqslant 1$ be an integer, $n=2p^t$, and let $d=n^2+1\equiv 5\pmod 8$. If $t>q^{r-1}$, then $\mathfrak{C}(k_n)\cong\mathbb{Z}/q^r\mathbb{Z}$.*

Proof. By Theorem 1.3, we have $h(d)\geqslant t$ and if $\mathcal{A}$ is an ideal class containing $\mathfrak{a}=(p,\frac{1}{2}(1+\sqrt{d}))$, then $\mathcal{A}$ is a nonprincipal ideal class, $|\mathcal{A}|>q^{r-1}$ and $|\mathcal{A}|\mid q^r$. This implies $|\mathcal{A}|=q^r$ and hence, the class group is cyclic. □

The following results can also be proved using Theorems 1.3, 1.4, 1.5 and some group theoretic arguments.

Theorem 5.2. *Let $d=n^2+1\equiv 5\pmod 8$.*

(I) *If $n=2{p_1}^{a_1}{p_2}^{a_2}\dots{p_m}^{a_m}$ with $m>2$ and if one of the following holds:*

(i) *For any $1\leqslant i\leqslant m$, $a_i\geqslant\frac{1}{2}(q^{r-1}+1)$.*

(ii) *For some $i\neq l$ and for any $2\leqslant j<r$, $a_i\geqslant\frac{1}{2}(q^{r-j}+1)$ and $a_l\geqslant\frac{1}{2}(q^{j-1}+1)$.*

Then $\mathfrak{C}(k_n)\cong\mathbb{Z}/q^r\mathbb{Z}$.

(II) *If $n=2{p_1}^{a_1}{p_2}^{a_2}$ and a_1 or $a_2\geqslant\frac{1}{2}(q^{r-1}+1)$, then $\mathfrak{C}(k_n)\cong\mathbb{Z}/q^r\mathbb{Z}$.*

Theorem 5.3. *Let* $d = n^2 + 1 \equiv 1 \pmod 8$.

(I) *If* $n = 2^s p^t$, $s \geqslant 2$ *and* $t \geqslant \frac{1}{2}(q^{r-1}+1)$ *or* $s-1 \geqslant \frac{1}{2}(q^{r-1}+1)$. *Then* $\mathfrak{C}(k_n) \cong \mathbb{Z}/q^r\mathbb{Z}$.

(II) *If* $n = 2^s p_1^{a_1} p_2{}^{a_2} \dots p_m{}^{a_m}$, $s \geqslant 2$, $m \geqslant 2$, *and if one of the following holds:*

(i) *For any* $1 \leqslant i \leqslant m$, a_i *or* $s - 1 \geqslant \frac{1}{2}(q^{r-1} + 1)$.

(ii) *For some* $i \neq l$ *and for any* $2 \leqslant j < r$, $a_i \geqslant \frac{1}{2}(q^{r-j} + 1)$ *and* a_l *or* $s - 1 \geqslant \frac{1}{2}(q^{j-1} + 1)$.

Then $\mathfrak{C}(k_n) \cong \mathbb{Z}/q^r\mathbb{Z}$.

Theorem 5.4. *Let* $d = n^2 + 1 \equiv 2 \pmod 4$.

(I) *If* $n = p^t$ *and* $t \geqslant \frac{1}{2}(q^{r-1} + 1)$, *then* $\mathfrak{C}(k_n) \cong \mathbb{Z}/q^r\mathbb{Z}$.

(II) *If* $n = p_1{}^{a_1} p_2{}^{a_2} \dots p_m{}^{a_m}$, $m \geqslant 2$, *and if one of the following holds:*

(i) *For any* $1 \leqslant i \leqslant m$, $a_i \geqslant \frac{1}{2}(q^{r-1} + 1)$.

(ii) *For some* $i \neq l$ *and for any* $2 \leqslant j < r$, $a_i \geqslant \frac{1}{2}(q^{r-j}+1)$ *and* $a_l \geqslant \frac{1}{2}(q^{j-1}+1)$.

Then $\mathfrak{C}(k_n) \cong \mathbb{Z}/q^r\mathbb{Z}$.

Theorem 5.5. *Let* $d = n^2 + 4 \equiv 5 \pmod 8$.

(I) *If* $n = p^t$ *and* $t \geqslant q^{r-1} + 1$, *then* $\mathfrak{C}(k_n) \cong \mathbb{Z}/q^r\mathbb{Z}$.

(II) *If* $n = p_1{}^{a_1} p_2{}^{a_2}$ *and* a_1 *or* $a_2 \geqslant \frac{1}{2}(q^{r-1} + 1)$, *then* $\mathfrak{C}(k_n) \cong \mathbb{Z}/q^r\mathbb{Z}$.

(III) *If* $n = p_1{}^{a_1} p_2{}^{a_2} \dots p_m{}^{a_m}$, $m > 2$, *and if one of the following holds:*

(i) *For any* $1 \leqslant i \leqslant m$, $a_i \geqslant \frac{1}{2}(q^{r-1} + 1)$.

(ii) *For some* $i \neq l$ *and for any* $2 \leqslant j < r$, $a_i \geqslant \frac{1}{2}(q^{r-j}+1)$ *and* $a_l \geqslant \frac{1}{2}(q^{j-1}+1)$.

Then $\mathfrak{C}(k_n) \cong \mathbb{Z}/q^r\mathbb{Z}$.

6. Some remarks

Let $g(n)$ be the least prime number which is a quadratic residue modulo n. Chowla and Friedlander in [10] proved that if $p = m^2+1$ is a prime, $m > 2$ and $h(p) = 1$, then $g(p) = \frac{1}{2}m$. We get some upper bound for $g(4p^2 + 1)$, if $h(4p^2 + 1) > 1$, irrespective of $4p^2 + 1$ is a prime or not.

Theorem 6.1. *Let* $d = 4p^2 + 1$ *be a square-free integer, where* p *is a prime. Then* $g(d) < p$, *except for* $p = 2, 3, 5, 7$ *and* 13.

Proof. By Proposition 2.1,

$$\zeta_{k_p}(-1) = \frac{1}{60} \sum_{\substack{|t| < \sqrt{4p^2+1} \\ t^2 \equiv 4p^2+1 \ (\mathrm{mod}\ 4)}} \sigma\Big(\frac{4p^2 + 1 - t^2}{4}\Big) = \frac{1}{60} \sum_{\substack{|t| \leqslant 2p \\ t \text{ is odd}}} \sigma\Big(\frac{4p^2 + 1 - t^2}{4}\Big)$$

$$= \frac{2}{60} \sum_{0\leqslant n\leqslant p-1} \sigma\Big(\frac{4p^2+1-(2n+1)^2}{4}\Big) = \frac{1}{30} \sum_{0\leqslant n\leqslant p-1} \sigma(p^2-n(n+1))$$
$$\geqslant \frac{1}{30} \sum_{0\leqslant n\leqslant p-1} \{1+p^2-n(n+1)\} = \frac{8p^3+28p}{360}.$$

By Theorem 2.4 of [6] we have that $h(\sqrt{4p^2+1}) = 1 \Leftrightarrow \zeta_{k_p} = (8p^3+28p)/360$. Equality occurs only if the set $\{p^2-n(n+1)\}_{n=1}^{p-2}$ consists of only prime numbers. Since (C) is true (proved by Biró in [3]), therefore, the set $\{p^2-n(n+1)\}_{n=1}^{p-2}$ always contains a composite number, except for $p = 2, 3, 5, 7$ and 13. That is, for all p, except $p = 2, 3, 5, 7$ and 13, there exists a $1 \leqslant n_0 \leqslant p-2$ such that $p^2-n_0(n_0+1)$ is not a prime number. Since $p^2-n_0(n_0+1) < p^2$ is odd, there exists an odd prime $q < p$ such that $q \mid (p^2-n_0(n_0+1))$. So we have

$$p^2-n_0(n_0+1) \equiv 0 \pmod{q}.$$

This implies that $p^2-n(n+1)$ has a solution n_0 in $\mathbb{F}_q$ and

$$n_0 = \frac{-1 \pm \sqrt{1+4p^2}}{2}.$$

Therefore, $1+4p^2$ is a square in $\mathbb{F}_q$, i.e., $1+4p^2 = x^2$ in $\mathbb{F}_q$ for some $x \in \mathbb{F}_q$. Thus, $1+4p^2$ is a quadratic residue of some prime $q < p$. Hence, q is also a quadratic residue of $1+4p^2$ since $1+4p^2 \equiv 1 \pmod{4}$. □

Similarly, one can deduce the following result:

Theorem 6.2. *Let $d = p^2+4$ be a square-free integer, where p is a prime. Consider $\mathbb{Q}(\sqrt{d})$, then $g(d) < p$, except for $p = 3, 5, 7, 13$ and 17.*

We believe that our method should go through for other R-D type real quadratic fields as well. It will be interesting to extend these results for other real quadratic fields, whose fundamental unit is known. Then one can try to reduce the class number 1 problem for that particular family to its subfamily. One can also state further information about the prime power order class group. In Section 5, if r is small, say 2 or 3, then in most cases we can exactly determine the class group by just looking at the exponents of prime factors.

Acknowledgements. The author is grateful to the anonymous referee for his/her valuable suggestions and remarks which improved the exposition of the paper.

References

[1] *N. C. Ankeny, S. Chowla*: On the divisibility of the class numbers of quadratic fields. Pac. J. Math. *5* (1955), 321–324. zbl MR doi

[2] *T. M. Apostol*: Generalized Dedekind sums and transformation formulae of certain Lambert series. Duke Math. J. *17* (1950), 147–157. zbl MR doi

[3] *A. Biró*: Chowla's conjecture. Acta Arith. *107* (2003), 179–194. zbl MR doi

[4] *A. Biró*: Yokoi's conjecture. Acta Arith. *106* (2003), 85–104. zbl MR doi

[5] *A. Biró, K. Lapkova*: The class number one problem for the real quadratic fields $\mathbb{Q}(\sqrt{(an)^2+4a})$. Acta Arith. *172* (2016), 117–131. zbl MR doi

[6] *D. Byeon, H. K. Kim*: Class number 1 criteria for real quadratic fields of Richaud-Degert type. J. Number Theory *57* (1996), 328–339. zbl MR doi

[7] *D. Byeon, H. K. Kim*: Class number 2 criteria for real quadratic fields of Richaud-Degert type. J. Number Theory *62* (1997), 257–272. zbl MR doi

[8] *K. Chakraborty, A. Hoque, M. Mishra*: A note on certain real quadratic fields with class number up to three. Kyushu J. Math. *74* (2020), 201–210. zbl MR doi

[9] *K. Chakraborty, A. Hoque, M. Mishra*: On the structure of order 4 class groups of $\mathbb{Q}(\sqrt{n^2+1})$. Ann. Math. Qué. *45* (2021), 203–212. zbl MR doi

[10] *S. Chowla, J. Friedlander*: Class numbers and quadratic residues. Glasg. Math. J. *17* (1976), 47–52. zbl MR doi

[11] *H. Hasse*: Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper. Elem. Math. *20* (1965), 49–59. (In German.) zbl MR doi

[12] *H. K. Kim, M.-G. Leu, T. Ono*: On two conjectures on real quadratic fields. Proc. Japan Acad., Ser. A *63* (1987), 222–224. zbl MR doi

[13] *H. Lang*: Über eine Gattung elemetar-arithmetischer Klasseninvarianten reell-quadratischer Zahlkörper. J. Reine Angew. Math. *233* (1968), 123–175. (In German.) zbl MR doi

[14] *S. Lang*: Algebraic Number Theory. Graduate Texts in Mathematics 110. Springer, New York, 1994. zbl MR doi

[15] *K. Lapkova*: Class number one problem for real quadratic fields of a certain type. Acta Arith. *153* (2012), 281–298. zbl MR doi

[16] *F. Lemmermeyer*: Algebraic Number Theory. Bilkent University, Bilkent, 2006; Available at `http://www.fen.bilkent.edu.tr/~franz/ant06/ant.pdf`.

[17] *R. A. Mollin*: Lower bounds for class numbers of real quadratic fields. Proc. Am. Math. Soc. *96* (1986), 545–550. zbl MR doi

[18] *R. A. Mollin*: Lower bounds for class numbers of real quadratic and biquadratic fields. Proc. Am. Math. Soc. *101* (1987), 439–444. zbl MR doi

[19] *R. A. Mollin*: On the insolubility of a class of Diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud-Degert type. Nagoya Math. J. *105* (1987), 39–47. zbl MR doi

[20] *R. A. Mollin, H. C. Williams*: A conjecture of S. Chowla via the generalized Riemann hypothesis. Proc. Am. Math. Soc. *102* (1988), 794–796. zbl MR doi

[21] *C. L. Siegel*: Berechnung von Zetafunktionen an ganzzahligen Stellen. Nachr. Akad. Wiss. Gött., II. Math.-Phys. Kl. *10* (1969), 87–102. (In German.) zbl MR

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

[23] *H. Yokoi*: On real quadratic fields containing units with norm -1. Nagoya Math. J. *33* (1968), 139–152. zbl MR doi

[24] *H. Yokoi*: On the fundamental unit of real quadratic fields with norm 1. J. Number Theory *2* (1970), 106–115. zbl MR doi

[25] *H. Yokoi*: Class-number one problem for certain kind of real quadratic fields. Class Numbers and Fundamental Units of Algebraic Number Fields. Nagoya University, Nagoya, 1986, pp. 125–137. zbl MR

Author's address: Mohit Mishra, Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad 211 019, India, current affiliation: Department of Mathematics, Indian Institute of Technology Kanpur, Kalyanpur, Kanpur, Uttar Pradesh 208016, India, e-mail: `m.mishra0808@gmail.com`.