Hardy-Ramanujan Journal 48 (2025) Part A, 1-9 submitted 28/02/2025, accepted 23/09/2025, revised 07/12/2025

On the simultaneous 3-divisibility of class numbers of quadruples of real quadratic fields

Kalyan Banerjee, Ankurjyoti Chutia and Azizul Hoque

Abstract. In this paper, we construct infinitely many quadruples of real quadratic fields whose class numbers are all divisible by 3. To the best of our knowledge, this is the first result towards the divisibility of the class numbers of certain tuples of real quadratic fields. At the end, we give an application of this result to produce some elliptic curves having a 3-torsion subgroup.

Keywords. Real quadratic field, Class number, Spiegelungssatz, Iizuka's conjecture, Hilbert class field.

2010 Mathematics Subject Classification. 11R11, 11R29, 11G05

1. Introduction

It was conjectured by Gauss that there are infinitely many real quadratic fields with class number one, which is still open. In contrast, the situation for imaginary quadratic fields is completely understood: only nine such fields have class number one, and all imaginary quadratic fields with class numbers up to 100 have been classified (cf. [Wat04]). These results highlight the importance of understanding the arithmetic of class numbers. In particular, their divisibility properties shed light on the structure of the associated ideal class groups. A striking development in this direction is the proof that, for any positive integer n, there exist infinitely many real (resp. imaginary) quadratic fields whose class numbers are divisible by n (see, [AnCh55, CHYP18, Hoq21, Yam70]). Moreover, there is a "Spiegelungssatz" due to Scholz [Sch32], which relates the ideal class group of a real quadratic field to that of an imaginary quadratic field. As a consequence of this Spiegelungssatz, we can deduce that if 3 divides the class number of a real quadratic field $\mathbb{Q}(\sqrt{d})$, then 3 also divides the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3d})$. Komatsu [Kom02] was motivated by this consequence, who proved the existence of an infinite family of pairs of quadratic fields of the form $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{md})$ with $m, d \in \mathbb{Z}$ whose class numbers are divisible by 3. He further extended this result in [Kom17] to the n-divisibility of the class numbers of pairs of imaginary quadratic fields of the above form. Later, Iizuka [Iiz18] considered an analogous problem, and proved the existence of infinitely many pairs of imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+1})$ with $d \in \mathbb{Z}$ whose class numbers are all divisible by 3. This helped him to frame the following conjecture.

Conjecture 1.1. ([Iiz18, 126 p.], Conjecture) *For any prime number p and any positive integer m, there is an infinite family of $m+1$ successive real (or imaginary) quadratic fields,*

$$\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \cdots, \mathbb{Q}(\sqrt{d+m})$$

with $d \in \mathbb{Z}$ whose class numbers are all divisible by p.

In [ChMu21], Chattopadhyay and Muthukrishnan extended the result of Iizuka [Iiz18, Theorem 1] by proving the 3-divisibility of the class numbers of an infinite family of triples of imaginary quadratic fields. Their proof is based on the construction of an unramified, cyclic cubic extension of a quadratic field and the classical Spiegelungssatz of Scholz. Krishnamoorthy and Pasupulati [KrPa21] further extended Iizuka's result [Iiz18, Theorem 1] from 3-divisibility to p-divisibility for any prime p. In

We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

particular, it resolved Conjecture 1.1 when $m = 1$. In [XiCh20], Xie and Chao proved that there are infinitely many pairs of imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+m})$, whose class groups have an element of order n respectively. They used Yamamoto's [Yam70] construction to prove this result. The third author [Hoq22] constructed an infinite family of quintuples of imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \mathbb{Q}(\sqrt{d+4}), \mathbb{Q}(\sqrt{d+36})$ and $\mathbb{Q}(\sqrt{d+100})$ whose class numbers are all divisible by a given odd integer $n \geq 3$. This result helped the author to give a complete proof of Conjecture 1.1 in a more general case, when $m = 1$. Analogously, it gives an affirmative answer to a weaker version of Conjecture 1.1 for $m \geq 3$. Chakraborty and the third author [ChHo23] constructed an infinite family of certain tuples of imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \mathbb{Q}(\sqrt{4d+1})$ and $\mathbb{Q}(\sqrt{2d+4^m})$ with $d, m \in \mathbb{Z}$ and $1 \leq m \leq 2|d|$ satisfying the n-divisibility of their class numbers for a given odd integer $n \geq 3$. In the spirit of Conjecture 1.1, the third author [Hoq] considered the problem of n-divisibility of class numbers of the tuples of imaginary quadratic fields of the form,

$$\left(\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \mathbb{Q}(\sqrt{2(d+2)}), \mathbb{Q}(\sqrt{3(d+3)}), \cdots, \mathbb{Q}(\sqrt{m(d+m)})\right)$$

with $d \in \mathbb{Z}$ for a given integer $m \geq 1$. In a similar spirit, we construct an infinite family of quadruples of real quadratic fields whose class numbers are all divisible by 3. The precise result in this paper is the following:

Theorem 1.1. *There are infinitely many quadruples of real quadratic fields of the form,*

$$\left(\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{216000D^3 + 457200D^2 + 322580D + 75866}), \mathbb{Q}(\sqrt{432D^3 + 1080D^2 + 900D + 223}),\right.$$
$$\left.\mathbb{Q}(\sqrt{40500D^3 + 89100D^2 + 65340D + 16215})\right)$$

with $D \in \mathbb{N}$ whose class numbers are all divisible by 3.

2. Construction of cyclic, cubic and unramified extensions

We recall the following beautiful result of Kishi and Miyake [KiMi00] to construct an unramified, cyclic cubic extension of a given quadratic field.

Theorem A. ([KiMi00, Main Theorem]) *For any two integers u and v, let*

$$F_{u,v}(Z) = Z^3 - uvZ - u^2. \tag{2..1}$$

If

(a) u and v are relatively prime;

(b) $F_{u,v}(Z)$ is irreducible over $\mathbb{Q}$;

(c) the discriminant $D_{F_{u,v}}$ of $F_{u,v}(Z)$ is not a perfect square in $\mathbb{Z}$;

(d) one of the following conditions holds:

(d.1) $3 \nmid v$,

(d.2) $3 \mid v, \quad uv \not\equiv 3 \pmod 9, \quad u \equiv v \pm 1 \pmod 9$,

(d.3) $3 \mid v, \quad uv \equiv 3 \pmod 9, \quad u \equiv v \pm 1 \pmod{27}$,

then the normal closure of $\mathbb{Q}(\alpha)$*, where* α *is a root of* $F_{u,v}(Z)$*, 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 suitable choices of integers* u *and* v*.*

Another approach to construct a cyclic, cubic and unramified extension of a quadratic field is due to Kishi [Kis00]. This approach is based on a cubic polynomial defined by an algebraic integer. Let $\mathbb{K}$ be a quadratic field and $\mathcal{O}_{\mathbb{K}}$ its ring of integers. Assume that $\alpha \in \mathcal{O}_{\mathbb{K}}$ with $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \in \mathbb{Z}^3$. We now define

$$P_\alpha(X) := X^3 - 3[N_{\mathbb{K}/\mathbb{Q}}(\alpha)]^{1/3}X - T_{\mathbb{K}/\mathbb{Q}}(\alpha).$$

In [Kis98], Kishi deduced the following criterion for the irreducibility of $P_\alpha(X)$ over $\mathbb{Q}$.

Lemma 2.1. *Let* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$*. Suppose* $\alpha = \frac{a+b\sqrt{d}}{2} \in \mathcal{O}_{\mathbb{K}}$ *with* $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ *is a cube in* $\mathbb{Z}$*. Then* $P_\alpha(X)$ *is reducible over* $\mathbb{Q}$ *if and only if* α *is a cube in* $\mathbb{K}$*.*

Let d be a square-free integer other than 1 and -3. Set

$$D := \begin{cases} -d/3 & \text{if } 3 \mid d, \\ -3d & \text{otherwise.} \end{cases}$$

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ and $\mathbb{L} = \mathbb{Q}(\sqrt{D})$. We define,

$$R_d := \{\alpha \in \mathcal{O}_{\mathbb{K}} : \alpha \text{ is not a cube in } \mathbb{K}, \text{ but } N_{\mathbb{K}/\mathbb{Q}}(\alpha) \text{ is a cube in } \mathbb{Z}\}$$

and

$$R_D := \{\alpha \in \mathcal{O}_{\mathbb{L}} : \alpha \text{ is not a cube in } \mathbb{L} \text{ and } N_{\mathbb{L}/\mathbb{Q}}(\alpha) \text{ is a cube in } \mathbb{Z}\}.$$

It is very clear that the subset R_d (resp. R_D) contains all those units in $\mathbb{K}$ which are not cubes in $\mathbb{K}$ (resp. in $\mathbb{L}$). Further assume that

$$R_d^* := \{\alpha \in R_d : \gcd(N_{\mathbb{K}/\mathbb{Q}}(\alpha), T_{\mathbb{K}/\mathbb{Q}}(\alpha)) = 1\}$$

and

$$R_D^* := \{\alpha \in R_D : \gcd(N_{\mathbb{L}/\mathbb{Q}}(\alpha), T_{\mathbb{L}/\mathbb{Q}}(\alpha)) = 1\}.$$

With the help of elements in R_d^* (resp. R_D^*), one can construct a cyclic, cubic and unramified extension of $\mathbb{K}$ (resp. $\mathbb{L}$). Kishi used this idea to construct such unramified extensions except at 3. More precisely, he proved the following:

Theorem B. ([Kis00, Proposition 6.5]) *Let* $\alpha \in R_D^*$ *(resp.* $\alpha \in R_d^*$*). Then the splitting field,* $S_{\mathbb{Q}}(P_\alpha)$ *of* $P_\alpha(X)$ *over* $\mathbb{Q}$ *is an* S_3*-field containing* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *(resp.* $\mathbb{L} = \mathbb{Q}(\sqrt{D})$*) which is a cyclic cubic extension of* $\mathbb{K}$ *(resp.* $\mathbb{L}$*) unramified outside* 3 *and contains a cubic subfield* $\mathbb{K}'$ *with* $v_3(\Delta_{\mathbb{K}'}) \neq 5$*. Conversely, every* S_3*-field containing* $\mathbb{K}$ *(resp.* $\mathbb{L}$*) which is unramified outside* 3 *over* $\mathbb{K}$ *(resp.* $\mathbb{L}$*) and contains a cubic subfield* $\mathbb{K}'$ *satisfying* $v_3(\Delta_{\mathbb{K}'}) \neq 5$ *is given by* $S_{\mathbb{Q}}(P_\alpha)$ *with* $\alpha \in R_D^*$ *(resp.* $\alpha \in R_d^*$*).*

The above theorem helps us to construct cyclic, cubic and unramified extensions outside 3. Thus, we need to handle the prime 3, and the following result comes here to rescue us in this case. This result is a particular case of [LlNa83, Theorem 1].

Lemma 2.2. *Suppose that*

$$g(X) := X^3 - aX - b \in \mathbb{Z}[X]$$

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

(i) $1 \leq v_3(b) \leq v_3(a)$,

(ii) $3 \mid a,\ a \not\equiv 3 \pmod 9,\ 3 \nmid b$ *and* $b^2 \not\equiv a+1 \pmod 9$,

(iii) $a \equiv 3 \pmod 9,\ 3 \nmid b$ *and* $b^2 \not\equiv a+1 \pmod{27}$.

3. Some families of real quadratic fields with class number divisible by 3

Proposition 3.1. *For any positive integer x, the class number of the real quadratic field $\mathbb{Q}(\sqrt{216000x^3+457200x^2+322580x+75866})$ is divisible by 3.*

Proof. Let us choose $u=4$ and $v=3(180x+127)$. Then $\gcd(u,v)=1$. We set:

$$F_{u,v}(Z) := Z^3 - 12(180x+127)Z - 16.$$

Now, reading $F_{u,v}(Z)$ under modulo 5, we get $F_{u,v}(Z) \equiv Z^3 - 4Z - 1 \pmod 5$. It is easy to check that $F_{u,v}(Z) \pmod 5$ is irreducible, and thus $F_{u,v}(Z)$ is irreducible as a polynomial with integer coefficients as well.

The discriminant of $F_{u,v}(Z)$ is

$$\Delta_{F_{u,v}} = 4(12(180x+127))^3 - 27\cdot 16^2.$$

This can be simplified as $\Delta_{F_{u,v}} = 12^4 D$, where $D = 216000x^3+457200x^2+322580x+75866$. Since $D \equiv 2 \pmod 4$, D is not a square in $\mathbb{Z}$ and so is $\Delta_{F_{u,v}}$.

We see that $3 \mid v$, and $uv \equiv 3 \pmod 9$. Further, $v+1 \equiv 4 \pmod{27}$. Therefore, $F_{u,v}(Z)$ satisfies the conditions (a)-(c) and (d.3) of Theorem A. This completes the proof by Theorem A.

Proposition 3.2. *For any positive integer y, the class number of the real quadratic field $\mathbb{Q}(\sqrt{432y^3+1080y^2+900y+223})$ is divisible by 3.*

Proof. The proof of this proposition is very similar to that of Proposition 3.1. Nevertheless, we give the proof in brief for the sake of completeness.

We put $u=2$ and $v=6y+5$. Then $\gcd(u,v)=1$, and we define,

$$F_{u,v}(Z) := Z^3 - 2(6y+5)Z - 4.$$

The discriminant of $F_{u,v}(Z)$ is

$$\Delta_{F_{u,v}} = 4(2(6y+5))^3 - 27\cdot 4^2,$$

which can be simplified as $4^2 d$ with $d = 432y^3+1080y^2+900y+223$. As $d \equiv 2 \pmod 3$, d is not a square in $\mathbb{Z}$ and so is $\Delta_{F_{u,v}}$. It is easy to see that $F_{u,v}(Z) \pmod 3$ is irreducible, and thus $F_{u,v}(Z)$ is irreducible over $\mathbb{Z}$ too. Since $3 \nmid v$, therefore by Theorem A, we conclude the proof.

In the next proposition, we will use the second method to construct unramified, cyclic cubic extension of a quadratic field. To establish the 3-divisibility of the class number, we need Hilbert class field. Therefore the for sake of completeness, we briefly recall the Hilbert class field. The Hilbert class field of a number field $\mathbb{K}$, denoted by $H(\mathbb{K})$, is defined as the maximal unramified abelian extension of $\mathbb{K}$, which contains all other unramified abelian extensions of $\mathbb{K}$.

Theorem C. ([Cox13, Theorem 5.23 (Artin Reciprocity)]) *Let $\mathbb{K}$ be a number field with its group of fractional ideals and class group respectively, $\mathcal{I}_{\mathbb{K}}$ and $Cl(\mathbb{K})$. If $H(\mathbb{K})$ is the Hilbert class field of $\mathbb{K}$, then the Artin map*

$$\Phi : \quad \mathcal{I}_{\mathbb{K}} \longrightarrow \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$$

is surjective, and its kernel is exactly the subgroup $P_{\mathbb{K}}$ of principal fractional ideals. Thus this map induces the following deep correspondence

$$\mathrm{Gal}(H(\mathbb{K})/\mathbb{K}) \cong Cl(\mathbb{K}).$$

Proposition 3.3. *For any positive integer k, the class number of the real quadratic field $\mathbb{Q}(\sqrt{40500k^3+89100k^2+65340k+16215})$ is divisible by 3.*

Proof. Assume that $d=-(13500k^3+29700k^2+21780k+5405)$. Then $d\not\equiv 0 \pmod 3$, and thus we set $D:=-3d=40500k^3+89100k^2+65340k+16215$. As $d\equiv 2 \pmod 3$ and $D\equiv 3 \pmod 4$, so that both d and D are not perfect squares.

Let $\mathbb{K}=\mathbb{Q}(\sqrt{-d})$, and define $\alpha\in\mathbb{K}$ as

$$\alpha:=\frac{9+\sqrt{-d}}{2}.$$

Then $T_{\mathbb{K}/\mathbb{Q}}(\alpha)=9$ and $N_{\mathbb{K}/\mathbb{Q}}(\alpha)=-(15k+11)^3$, and thus $\gcd(T_{\mathbb{K}/\mathbb{Q}}(\alpha),N_{\mathbb{K}/\mathbb{Q}}(\alpha))=1$. Therefore with this α, we define

$$f_\alpha(Z):=Z^3-3\left(N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right)^{1/3}Z-T_{\mathbb{K}/\mathbb{Q}}(\alpha),$$

which is

$$f_\alpha(Z)=Z^3+3(15k+11)Z-9.$$

If $Z=p/q$ is a root of $f_\alpha(Z)$ in $\mathbb{Q}$, then $p\mid 9$ and $q\mid 1$, which further imply that

$$Z=\pm 1,\pm 3,\pm 9.$$

However, $f_\alpha(\pm 1)\neq 0$, $f_\alpha(\pm 3)\neq 0$ and $f_\alpha(\pm 9)\neq 0$. This confirms that $f_\alpha(Z)$ is irreducible over $\mathbb{Q}$. Therefore by Lemma 2.1, α is not a cube in $\mathbb{K}$, and hence $\alpha\in R_d$. As $\gcd(T_{\mathbb{K}/\mathbb{Q}}(\alpha),N_{\mathbb{K}/\mathbb{Q}}(\alpha))=1$, so that $\alpha\in R_d^*$. Therefore by Theorem B, $S_{\mathbb{Q}}(f_\alpha)$ is a cyclic cubic extension of $\mathbb{L}$ which is unramified outside 3.

It remains to check the unramification of $S_{\mathbb{Q}}(f_\alpha)$ at 3. To see this, we will apply Lemma 2.2. By the assumptions, we see that $v_3(3(15k+11))=1$ and $v_3(b)=v_3(9)=2$. Thus (i) of Lemma 2.2 does not hold. Rest of two conditions of Lemma 2.2 do not hold since $b=9\equiv 0 \pmod 3$. Thus by Lemma 2.2, we can conclude that $S_{\mathbb{Q}}(f_\alpha)$ is unramified over $\mathbb{L}$ at 3 as well. Therefore, we complete the proof by Theorem C.

4. Proof of Theorem 1.1

To prove that our construction can generate infinitely many quadruples of quadratic fields of a specific form with class numbers divisible by 3, we recall a particular case of the celebrated result on integral points due to Siegel (cf. [Sil09, Chapter IX, Theorem 4.3], [Sie29]). Let $V_{\mathbb{Q}}$ be the set of all standard absolute values on $\mathbb{Q}$.

Theorem D. ([Sil09, Siegel's Theorem]) *Assume that S is a finite set such that $\{\infty\}\subset S\subset V_{\mathbb{Q}}$. Let $f(x)\in\mathbb{Q}[x]$ be a polynomial of degree at least 3 with distinct roots in $\mathbb{C}$. Then the set*

$$\{(x,y)\in R_S\times R_S \mid y^2=f(x)\}$$

is finite, where $R_S=\{x\in\mathbb{Q}\mid v_p(x)\geq 0$ for all $p\in V_{\mathbb{Q}}\setminus S\}$; so-called the ring of S-integers of $\mathbb{Q}$.

Given an integer a, we define the curve $ay^2=40500x^3+89100x^2+65340x+16215$. Assume that

$$A=\{(x,y)\in\mathbb{Z}\times\mathbb{Z}\mid ay^2=40500x^3+89100x^2+65340x+16215\}.$$

If we take $S=\{\infty\}$, then $R_S=\mathbb{Z}$. Thus, by Theorem D the set A is finite. Therefore, the set $\mathfrak{S}=\{\mathbb{Q}(\sqrt{40500x^3+89100x^2+65340x+16215})\mid x\in\mathbb{Z}^+\}$ contains infinitely many elements. Hence, by Proposition 3.3, we have the following:

Proposition 4.1. *The set*

$$\mathcal{S}=\{k\in\mathbb{Z}^+\mid \text{the class number of } \mathbb{Q}(\sqrt{40500k^3+89100k^2+65340k+16215}) \text{ is divisible by } 3\}$$

is infinite.

Proof of Theorem 1.1

Given a positive integer k, we assume that $D = 40500k^3 + 89100k^2 + 65340k + 16215$. Then by Proposition 3.3, the class number of the real quadratic field $\mathbb{Q}(\sqrt{D})$ is divisible by 3.

Since D is a positive integer, by Proposition 3.3, the class number of the real quadratic field $\mathbb{Q}(\sqrt{40500D^3 + 89100D^2 + 65340D + 16215})$ is divisible by 3.

Similarly, by Propositions 3.1 and 3.2, the class numbers of the real quadratic fields $\mathbb{Q}(\sqrt{216000D^3 + 457200D^2 + 322580D + 75866})$ and $\mathbb{Q}(\sqrt{432D^3 + 1080D^2 + 900D + 223})$ are all divisible by 3. The infinitude of such fields follows from Proposition 4.1.

5. Torsion in certain elliptic curves

We consider the curve given by the equation,

$$y^2 = 40500x^3 + 89100x^2 + 65340x + 16215.$$

We can verify that this defines an elliptic curve, E_1.

For the next theorem, we need some preliminaries regarding the Picard group of an algebraic curve. Let C be a smooth projective curve over $\bar{\mathbb{Q}}$ and let $Div(C)$ denote the free abelian group generated by the closed points on the curve C. Any element is an integral linear combination of points on the curve. We denote such a combination by D a Weil divisor. We say that two Weil divisors D_1 and D_2 are linearly equivalent if there exists a rational function f on C such that

$$D_1 - D_2 = div(f).$$

Here the divisor of f is the divisor defined by

$$f^{-1}(0) - f^{-1}(\infty),$$

that is, the differences between the zeros and poles of the rational function.

For an elliptic curve E over $\bar{\mathbb{Q}}$, the Picard group is isomorphic to

$$Pic^0(E) \oplus \mathbb{Z} = E \oplus \mathbb{Z}\ .$$

Given a Zariski open subset U inside C, we have the following exact sequence at the level of Picard groups:

$$\oplus_i \mathbb{Z} \to Pic(C) \to Pic(U) \to 0\ .$$

The left hand side, $\oplus_i \mathbb{Z}$ of the above exact sequence corresponds to the free abelian group generated by the finitely many points of $C \setminus U$.

There is also the weak Mordell-Weil theorem [Sil09] in the context of elliptic curves. It says that the group

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus Tors(E(\mathbb{Q})).$$

That is $E(\mathbb{Q})$ is finitely generated.

We want to study the torsion subgroup of E_1. We claim that:

There exists a 3-torsion in the $\mathbb{Q}$-rational points on the elliptic curve E_1.

Proof of the claim

Suppose that the elliptic curve E_1 does not have 3-torsion in the group of $\mathbb{Q}$-rational points $E_1(\mathbb{Q})$. Then, if we spread the elliptic curve over the rational integers and consider a fixed smooth integral model $E_{1\mathbb{Z}}$ over $\mathbb{Z}$, by the Nagell-Lutz theorem [SiTa15, Theorem 2.5], the torsion points are all

integral-valued. So when we specialize these torsion points in the class group of the ring of integers of the aforementioned real quadratic field

$$\mathbb{Q}(\sqrt{40500k^3+89100k^2+65340k+16215}),$$

we obtain the torsion elements in the class group of the same order. Now by Theorem 1.1 there are infinitely many k such that the aforementioned real quadratic fields have 3-torsions in the class group. Consider the family

$$E_{1\mathbb{Z}} \to \mathbb{A}^1_{\mathbb{Z}},$$

where $\mathbb{A}^1_{\mathbb{Z}}$ is the affine line over $\mathbb{Z}$ given by $Spec(\mathbb{Z}[x])$. The above map is the projection map

$$(x, y) \mapsto x$$

from $E_{1\mathbb{Z}} \to \mathbb{A}^1_{\mathbb{Z}}$. Suppose that there are no 3-torsions in the divisor class group of E_1, then the same is true for the generic fiber of the family $E_{1\mathbb{Z}} \to \mathbb{A}^1_{\mathbb{Z}}$. By generic fiber, we mean the elliptic curve E_1 scalar extended to $\mathbb{Q}(x)$. It is an isotrivial family in the sense that all fibers are isomorphic over $\mathbb{Q}$. The presence of 3-torsion on the generic fiber forces the same on the fiber E_1, since the family is isotrivial.

Now, the divisor class group of $E_{1\mathbb{Q}(x)}$ is the co-limit of the divisor class groups $Pic(E_{1U})$, where E_{1U} is the family over a Zariski open subset U of $\mathbb{A}^1_{\mathbb{Z}}$. Then it follows that, for all the Zariski open set $U \subset \mathbb{A}^1$, $Pic(E_{1U})$ has no 3-torsion. This is because the presence of 3-torsion in $Pic(E_{1U})$ gives the following. The 3-torsion in $Pic(E_{1U})$ goes to zero under restriction homomorphism to $Pic(E_{1\mathbb{Q}(x)})$ because the generic fiber does not have such an element. Therefore, there exists V a smaller open set such that the 3-torsion in $Pic(E_{1U})$ restricted to $Pic(E_{1V})$ is zero. At the level of torsions, the map

$$Pic(E_{1U}) \to Pic(E_{1V})$$

is an isomorphism, as the kernel is zero (there is no torsion element in the kernel.) This by using the localization exact sequence for Picard groups:

$$\oplus_i \mathbb{Z} \to Pic(E_{1U}) \to Pic(E_{1V}) \to 0.$$

The first term of the above sequence is the Neron-Severi components of the fibers in $E_{1U} \setminus V_{1U}$.

But each of the class groups of

$$\mathbb{Q}(\sqrt{40500k^3+89100k^2+65340k+16215})$$

has a 3-torsion subgroup for infinitely many k, such that the above square root is not an integer. So, the above torsion points in the class groups varies in a family in the sense that there is a Zariski open set U, such that $Pic(E_{1U})$ has a 3-torsion by [BH24, Theorem 4.3]. By the above claim, there is no such U. So by applying the Nagell-Lutz method and using that $Pic^0(E_{1\mathbb{Z}})$ has a 3-torsion, we find that the elliptic curve has a 3-torsion. Thus, we our claim is proved.

The same result holds for the elliptic curves E_2 and E_3 respectively given by the equations:

$$y^2 = 432x^3 + 1080x^2 + 900x + 223,$$

and

$$y^2 = 216000x^3 + 457200x^2 + 322580x + 75866$$

by arguing as above.

To sum up the above, we can state the following:

Theorem 5.1. *Assume that E_1, E_2 and E_3 are as defined above. Then there is a 3-torsion in the $\mathbb{Q}$-rational points on each of E_1, E_2 and E_3.*

Acknowledgement. The authors are grateful to the anonymous referees for their valuable comments that immensely improved the presentation of the paper. This work was supported by ANRF (SERB) Core Research Grant (CRG/2023/007323) and ANRF (SERB) MATRICS (MTR/2021/000762), Govt. of India.

References

[AnCh55] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324.

[CHYP18] K. Chakraborty, A. Hoque, Y. Kishi and P. P. Pandey, *Divisibility of the class numbers of imaginary quadratic fields*, J. Number Theory **185** (2018), 339–348.

[ChHo23] K. Chakraborty and A. Hoque, *Lehmer sequence approach to the divisibility of class numbers of imaginary quadratic fields*, Ramanujan J. **60** (2023), no. 4, 913–923.

[ChMu21] J. Chattopadhyay and S. Muthukrishnan, *On the simultaneous* 3*-divisibility of class numbers of triples of imaginary quadratic fields*, Acta Arith. **197** (2021), no. 1, 105–110.

[CFGKY23] G. Cherubini, A. Fazzari, A. Granville, V. Kala and P. Yatsyna, *Consecutive real quadratic fields with large class numbers*, Int. Math. Res. Not. IMRN, 2023 (2023), no. 14, 12052–12063.

[Cox13] David A. Cox, *Primes of the form* $x^2 + ny^2$*: Fermat, class field theory, and complex multiplication*, second edition, Wiley, USA, 2013.

[Hoq21] A. Hoque, *On the exponents of class groups of some families of imaginary quadratic fields*, Mediterr. J. Math. **18** (2021), no. 4, Paper No. 153, 13 pp.

[Hoq22] A. Hoque, *On a conjecture of Iizuka*, J. Number Theory **238** (2022), 464–473.

[Hoq] A. Hoque, *Class number divisibility of tuples of imaginary quadratic fields: á la Iizuka*, submitted.

[BH24] K. Banerjee and A. Hoque, *Chow groups, pull back and class groups*, Monatsh. Math. **205** (2024), no. 3, 433–454.

[Iiz18] Y. Iizuka, *On the class number divisibility of pairs of imaginary quadratic fields*, J. Number Theory **184** (2018), 122–127.

[Kis98] K. Kishi, A criterion for a certain type of imaginary quadratic fields to have 3-ranks of the ideal class groups greater than one, *Proc. Japan Acad.* **74**, Ser. A (1998), 93–97.

[KiMi00] Y. Kishi and K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three, *J. Number Theory* **80** (2000), 209–217.

[Kis00] Y. Kishi, A constructive approach to Spiegelung relations between 3-ranks of absolute ideal class groups and congruent ones modulo $(3)^2$ in quadratic fields, *J. Number Theory* **83** (2000), 1–49.

[Kom17] T. Komatsu, *An infinite family of pairs of imaginary quadratic fields with ideal classes of a given order*, Int. J. Number Theory **13** (2017), no. 2, 253–260.

[Kom02] T. Komatsu, *An infinite family of pairs of quadratic fields* $\mathbb{Q}(\sqrt{D})$ *and* $\mathbb{Q}(\sqrt{mD})$ *whose class numbers are both divisible by* 3, Acta Arith. **104** (2002), 129–136.

[KrPa21] S. Krishnamoorthy and S. Pasupulati, *Note on the p-divisibility of class numbers of an infinite family of imaginary quadratic fields*, Glasgow Math. J. **64** (2022), 2, 352–357.

[LlNa83] P. Llorente and E. Nart, Effective determination of the decomposition of the rational prime in a cubic field, *Proc. Amer. Math. Soc.* **87** (1983), 579–585.

[Sch32] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201–203.

[Sie29] C. L. Siegel, *Über einige Anwendungen Diophantischer approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. **1** (1929), 1-70; Ges. Abh., Band **1**, 209–266.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. **106**, Springer-Verlag, New York, 2009.

[SiTa15] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, Switzerland, 2015.

[Wat04] M. Watkins, *Class numbers of imaginary quadratic fields* Math. Comp. **73**(246) (2004), 907–938.

[XiCh20] C. -F. Xie and C. F. Chao, *On the divisibility of class numbers of imaginary quadratic fields* $\left(\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+m})\right)$, Ramanujan J. **53** (2020), 517–528.

[Yam70] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

Kalyan Banerjee
Department of Mathematics
SRM University AP, Mangalagiri-Mandal
Amaravati-522240, Andhra Pradesh, India.

e-mail: kalyan.b@srmap.edu.in

Ankurjyoti Chutia
Department of Mathematics
Gauhati University
Guwahati-781014, Assam, India.

e-mail: ankurjyoti878@gmail.com

Azizul Hoque
Department of Mathematics
Gauhati University
Guwahati-781014, Assam, India.

e-mail: ahoque.ms@gmail.com