Glasgow Math. J. **64** (2022) 352–357. © The Author(s), 2021. Published by Cambridge University Press on behalf of Glasgow Mathematical Journal Trust.
doi:10.1017/S001708952100015X.

NOTE ON THE p-DIVISIBILITY OF CLASS NUMBERS OF AN INFINITE FAMILY OF IMAGINARY QUADRATIC FIELDS

SRIlAKSHMI KRISHNAMOORTHY and SUNIL KUMAR PASUPULATI
Indian Institute of Science Education and Research, Thiruvananthapuram, India
e-mails: srilakshmi@iisertvm.ac.in; sunil4960016@iisertvm.ac.in

(Received 2 October 2020; revised 31 March 2021; accepted 25 April 2021;
first published online 20 May 2021)

Abstract. For any odd prime p, we construct an infinite family of imaginary quadratic fields whose class numbers are divisible by p. We give a corollary that settles Iizuka's conjecture for the case $n = 1$ and $p > 2$.

2020 *Mathematics Subject Classification*. Primary 11R29; Secondary 11R11

1. Introduction. Let K be a number field. The ideal class group Cl_K is defined to be the quotient group J_K/P_K, where J_K is the group of fractional ideals of K and P_K is the group of principal fractional ideals of K. It is well known that Cl_K is finite. The class number h_K of a number field K is the order of Cl_K. The ideal class group is one of the most basic and mysterious objects in algebraic number theory. The class group has drawn the attention of several authors. The divisibility properties of the class number of number fields play a significant role in understanding the structure of the ideal class groups of number fields. Cohen–Lenstra heuristics are a set of conjectures about this structure. In general, given a positive integer n, there is no characterization to find all quadratic fields whose class numbers are divisible by n. For $n = 3$, these fields were characterized in [**12**]. For a given integer $n > 1$, the Cohen–Lenstra heuristic [**4**] predicts that the proportion of imaginary quadratic fields with class number divisible by n should be positive. It has been proved by several authors that for every $n > 1$, there exist infinitely many quadratic fields whose class number is divisible by n ([**2**, **5**, **7**, **10**, **11**, **14**]).

B. H. Gross and D. E. Rohrlich proved that for any odd integer $n > 3$, there are infinitely many imaginary quadratic fields ($\mathbb{Q}\left(\sqrt{1-4U^n}\right)$, $U > 1$) whose class numbers are divisible by n. Furthermore, Stéphane Louboutin [**14**] proved the same result by simplifying the Gross and Rohrlich's proof and proved the following result on divisibility of class number of $\mathbb{Q}(\sqrt{1-4U^k})$ for $U > 2$.

THEOREM 1. *If $k \in \mathbb{Z}^+$ be odd number, then for any integer $U \geq 2$ the ideal class groups of the imaginary quadratic fields $\mathbb{Q}(\sqrt{1-4U^k})$ contain an element of order k.*

Murty [**15**] proved that the class number of $\mathbb{Q}\left(\sqrt{1-U^n}\right)$ is divisible by n if $1 - U^n$ is square-free. We study the divisibility of class number of families $\mathbb{Q}(\sqrt{1-2m^p})$ by all odd primes p.

The following result on the 3-divisibility of the class number is proved by K. Chakraborty and A. Hoque (Theorem 3.2, [**8**]).

THEOREM 2. *The class number of $\mathbb{Q}(\sqrt{1-2m^3})$ is divisible by 3 for any odd integer $m > 1$.*

We study the family $\mathbb{Q}(\sqrt{1-2m^p})$ for all odd primes p and prime power $m=q^r$, $r\in\mathbb{N}$. In the following theorem, we prove the p-divisibility of class numbers for this family by using the results of Yann Bugeaud and T. N. Shorey [1].

THEOREM 3. *For prime numbers $p,q\geq 3$ and $m=q^r, r\in\mathbb{N}$ such that $\mathbb{Q}(\sqrt{1-2m^p})\neq\mathbb{Q}(\sqrt{-1})$, the class number of $\mathbb{Q}(\sqrt{1-2m^p})$ is divisible by p.*

The condition $\mathbb{Q}(\sqrt{1-2m^p})\neq\mathbb{Q}(\sqrt{-1})$, means that $2m^p-1$ is not a square. Siegel's theorem (Lemma 9) asserts that there are only finitely many $m\in\mathbb{Z}$ such that $2m^p-1$ is a square.

The Birch Swinnerton-Dyer conjecture is an elliptic curve analogue of the analytic class number formula. For any elliptic curve defined over $\mathbb{Q}$ of rank zero and square-free conductor N, if $p\mid |E(\mathbb{Q})|$, under certain conditions on the Shafarevich–Tate group $Ш_D$, the first author [13] showed that $p\mid |Ш_D|$ if and only if $p\mid h_K$, where $K=\mathbb{Q}(\sqrt{-D})$.

2. Iizuka's conjecture. Y.Iizuka recently proves the following result on divisibility of the class numbers of imaginary quadratic fields in [9].

THEOREM 4. *There is an infinite family of pairs of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+1})$ with $d\in\mathbb{Z}$ whose class numbers are both divisible by* 3.

Based on the above theorem, Iizuka conjectured the following.

CONJECTURE 5. *(Iizuka) For any prime p and any positive integer n, there is an infinite family of $n+1$ successive real (or imaginary) quadratic fields*

$$\mathbb{Q}(\sqrt{D}),\ \mathbb{Q}(\sqrt{D+1}),\ \cdots,\ \mathbb{Q}(\sqrt{D+n})$$

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

As a consequence of Theorems 1 and 3, we get a generalization of Theorem 4 for all odd prime numbers p and prove the following corollary.

COROLLARY 6. *For every odd prime number, there is an infinite family of pairs of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+1})$ with $d\in\mathbb{Z}$ whose class numbers are both divisible by p.*

Proof of the Corollary 6. Fix an odd prime p. Consider the set

$$S_0=\left\{m\in\mathbb{Z}^+ \mid \text{the class number of } \mathbb{Q}\left(\sqrt{1-2m^p}\right) \text{ is divisible by } p\right\}.$$

By Lemma 9, the equation $1-2x^p=-y^2$ has finitely many solutions $(x,y)\in\mathbb{Z}\times\mathbb{Z}$. Hence it follows from Theorem 3 that S_0 contains infinitely many odd prime powers, which implies that S_0 is an infinite set. For $m\in S_0$, the prime p divides the class number of

$$\mathbb{Q}(\sqrt{4(1-2m^p)^p})=\mathbb{Q}(\sqrt{1-2m^p}).$$

Let $U=2m^p-1$. Then $U\geq 2$. Furthermore, Theorem 1 implies that p divides the class number of $\mathbb{Q}(\sqrt{1-4U^p})$. Now look at

$$\mathbb{Q}(\sqrt{1-4U^p})=\mathbb{Q}\left(\sqrt{1-4(2q^p-1)^p}\right)=\mathbb{Q}\left(\sqrt{4(1-2q^p)^p+1}\right).$$

Let $d=4(1-2m^p)^p$. The prime p divides class numbers of $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{d+1})$.

https://doi.org/10.1017/S001708952100015X Published online by Cambridge University Press

Now to conclude the corollary, we need to prove the set $\mathcal{A} = \left\{\mathbb{Q}\left(\sqrt{1-2m^p}\right) | m \in S_0\right\}$ is an infinite set. For every square-free integer $d_0 \neq 0$, let $f(x) = \frac{1-2x^p}{d_0}$. The polynomial $f(x)$ has distinct roots in $\overline{\mathbb{Q}}$. Thus by Lemma 9, the equation $y^2 = f(x)$ has finitely many integral solutions. Hence the infiniteness of $\mathcal{A}$ follows from that of S_0.

REMARK 7. The above corollary settles Iizuka's conjecture (5) for the case $n = 1$ and $p > 2$. We found a similar result for a different families of imaginary quadratic fields in [**17**]. J. Chattopadhyay and S. Muthukrishnan [**3**] answer a weaker version of Iizuka's conjecture for $p = 3$.

3. Preliminaries. We recall some known results and prove some lemmas that are necessary for proving our main theorem.

DEFINITION 8. Let K be a number field and let S be a finite set of valuations on K, containing all the archimedean valuations. Then

$$R_S = \{\alpha \in K \mid \nu(\alpha) \geq 0 \textit{ for all } \nu \notin S\}$$

is called the set of S-integers.

LEMMA 9. *(Siegel's theorem, [**16**], Chapter IX, Theorem 4.3) Let K be a number field and S be a finite set of valuations on K, containing all the archimedean valuations. Let $f(X) \in K[X]$ be a polynomial of degree $d \geq 3$ with distinct roots in the algebraic closure $\overline{K}$ of K. Then the equation $y^2 = f(x)$ has only finitely many solutions in S-integers $x, y \in R_S$.*

We recall some results of Yann Bugeaud and T. N. Shorey [**1**] on solutions of Diophantine equation $D_1x^2 + D_2 = \lambda^2 k^y$, where D_1 and D_2 are coprime positive integers, $k \geq 2$ is an integer coprime with D_1D_2 and $\lambda = \sqrt{2}, 2$ such that $\lambda = 2$ if k is even.

Let us denote F_i to be the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$, and $F_i = F_{i-1} + F_{i-2}$ for all $i \geq 2$. Let L_i be the Lucas sequence defined by $L_0 = 2$, $L_1 = 1$ and satisfying $L_i = L_{i-1} + L_{i-2}$ for all $i \geq 2$. Define the subsets $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ by

$$\mathcal{F} := \left\{(F_{i-2\epsilon}, L_{i+\epsilon}, F_i) \mid i \geq 2, \epsilon \in \{\pm 1\}\right\},$$

$$\mathcal{G} := \left\{(1, 4k^r - 1, k) \mid k \geq 2, r \geq 1\right\},$$

$$\mathcal{H} := \Big\{(D_1, D_2, k) \mid \text{there exist positive integers } r \text{ and } s \text{ such that } D_1s^2 + D_2 = \lambda^2 k^r \textit{ and } 3D_1s^2 - D_2 = \pm\lambda^2\Big\}.$$

Define $\mathcal{N}(\lambda, D_1, D_2, p)$ to be the number of $(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ of the Diophantine equation $D_1x^2 + D_2 = \lambda^2 p^y$.

THEOREM 10. *([**1**], Theorem 1) Let p be a prime number. Then we have $\mathcal{N}(\lambda, D_1, D_2, p) \leq 1$ expect for $\mathcal{N}(2, 13, 3, 2) = \mathcal{N}(\sqrt{2}, 7, 11, 3) = \mathcal{N}(1, 2, 1, 3) = \mathcal{N}(2, 7, 1, 2) = \mathcal{N}(\sqrt{2}, 1, 1, 5) = \mathcal{N}(\sqrt{2}, 1, 1, 13) = \mathcal{N}(2, 1, 3, 7) = 2$ and when (D_1, D_2, p) belongs to one of the infinite families $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$.*

LEMMA 11. *For any odd prime q and any integer $D > 3$, the equation $Dx^2 + 1 = 2q^y$ has at most one solution $(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+$.*

Proof. Let $D_1 = D$ and $D_2 = 1$ and $\lambda = \sqrt{2}$. We first note that $(\lambda, D_1, D_2, q) \notin \{(2, 13, 3, 2), (\sqrt{2}, 7, 11, 3), (1, 2, 1, 3), (2, 7, 1, 2), (\sqrt{2}, 1, 1, 5), (\sqrt{2}, 1, 1, 13), (2, 1,$

https://doi.org/10.1017/S001708952100015X Published online by Cambridge University Press

3, 7)}. By Theorem 10, it is enough to show that $(D_1, D_2, q) \notin \mathcal{F}$. If $(F_{i-\epsilon}, L_{i+\epsilon}, F_i) = (D_1, D_2, p)$, then $i = 2, \epsilon = -1$. Hence $D = 2$. This is not possible because $D > 3$. Therefore $(D_1, D_2, q) \notin \mathcal{F}$. If $(1, 4k^r - 1, k) = (D_1, D_2, q)$, then $D = D_1 = 1$. This is not possible. Therefore $(D_1, D_2, q) \notin \mathcal{G}$. If $D_1x^2 + 1 = 2q^y$, then $3D_1x^2 - 1 \geq D_1x^2 - 1 \geq 2q^y - 2 \geq 4$. Hence $(D_1, D_2, q) \notin \mathcal{H}$. □

PROPOSITION 12. *For prime numbers $p, q \geq 3$ and $m = q^r, r \in \mathbb{N}$, let $\alpha = 1 + \sqrt{1 - 2m^p}$, then $\pm 2^{\frac{p-1}{2}}\alpha$ is not a pth power of an algebraic integer in $\mathbb{Q}(\sqrt{1 - 2m^p})$.*

Proof. Let d be the square-free part of $\sqrt{1 - 2m^p}$ with signature. Let $K = \mathbb{Q}(\sqrt{d})$ and $\mathcal{O}_K$ be the ring of integers of K. Note that $-2^{\frac{p-1}{2}}\alpha$ is a pth power in $\mathcal{O}_K$ if and only if $2^{\frac{p-1}{2}}\alpha$ is a pth power in $\mathcal{O}_K$. It is enough to show $2^{\frac{p-1}{2}}\alpha$ is not a pth power. Suppose that,

$$2^{\frac{p-1}{2}}\alpha = \beta^p \text{ for some } \beta = a + b\sqrt{d} \in \mathcal{O}_K. \tag{3.1}$$

Then ,

$$2^{\frac{p-1}{2}}\left(1 + \sqrt{1 - 2m^p}\right) = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{p-2j} b^{2j} d^j + \gamma\sqrt{d} \text{ for some } \gamma \in \mathbb{Z}. \tag{3.2}$$

By comparing constant terms on both sides, we have

$$2^{\frac{p-1}{2}} = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{p-2j} b^{2j} d^j. \tag{3.3}$$

This implies that

$$2^{\frac{p-1}{2}} = a\left(\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{p-2j-1} b^{2j} d^j\right).$$

Hence a divides $2^{\frac{p-1}{2}}$.

Case 1 : a is even.
We look at (3.1)

$$2^{\frac{p-1}{2}}\alpha = \left(a + b\sqrt{d}\right)^p, \tag{3.4}$$

applying the norm map on the both sides

$$(2m)^p = \left(a^2 - b^2 d\right)^p.$$

Hence we have

$$2m = a^2 - b^2 d.$$

Since $2 \mid a$, we obtain $2 \mid b^2 d$. We deduce that $2 \mid b$ since d is odd. Taking divisibility of a^2, b^2 by 4 into consideration, we conclude that $4 \mid 2m$ but m is odd, which contradicts the assumption that a is even.

Case 2 : a is odd.
Suppose that a is odd. Since $a \mid 2^{\frac{p-1}{2}}$, this implies that $a = \pm 1$. Putting in equation (3.1) we have

https://doi.org/10.1017/S001708952100015X Published online by Cambridge University Press

$$2^{\frac{p-1}{2}}(1+\sqrt{1-2m^p}) = \left(\pm 1 + b\sqrt{d}\right)^p,$$

applying the norm map on both sides we get

$$(2m)^p = \left(1 - b^2 d\right)^p.$$

Rewriting the above equation using $D = -d$ and $m = q^r$, we get

$$1 + Db^2 = 2q^r. \tag{3.5}$$

We observe that $1 - 2m^p = 1 - 2(q^r)^p = b'^2 d$ for some $b' \in \mathbb{Z}$. Rephrasing this equation we have

$$1 + b'^2 D = 2q^{rp}. \tag{3.6}$$

Thus, from equations (3.5) and (3.6), we get (b, r), (b', rp) are solutions of the equation $Dx^2 + 1 = q^y$, which is a contradiction to Lemma 11. Hence $\pm 2^{\frac{p-1}{2}}\alpha$ is not a pth power in $\mathcal{O}_K$. □

4. Proof of the theorem. We now prove the main theorem of this article.

Proof of Theorem 3. Let d be the square-free part of $1-2m^p$ with signature then $d \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{d})$. Put $\alpha := 1 + \sqrt{1-2m^p}$, then $N_{K/\mathbb{Q}}(\alpha) = 2m^p$. Since $d \equiv 3 \pmod 4$, the ideal (2) is ramified, there exists a prime ideal $\mathcal{P}$ such that $(2) = \mathcal{P}^2$. Since the norm of α is $2m^p = 2q^{rp}$, the prime decomposition of (α) is given by $(\alpha) = \mathcal{P}\mathcal{Q}^t$, for some positive integer t, where $\mathcal{Q}$ is a prime that lies above q. Then $N_{K/\mathbb{Q}}((\alpha)) = 2q^t$, where $N(\mathcal{Q}) = q$ (since q splits in $\mathbb{Q}(\sqrt{d})$ as $\left(\frac{d}{q}\right) = 1$). Hence $t = rp$.

Consider the ideal $I := \mathcal{P}\mathcal{Q}^{\frac{t}{p}}$, of K. Observe that

$$I^p = \mathcal{P}^p\mathcal{Q}^t = (2)^{\frac{p-1}{2}}\mathcal{P}\mathcal{Q}^t = (2)^{\frac{p-1}{2}}(\alpha) = (2^{\frac{p-1}{2}}\alpha).$$

We claim that the order of the ideal I in ideal class group is p. Suppose not, let $(\beta) = I$ for some β in $\mathcal{O}_K$. Then

$$(\beta^p) = (\beta)^p = I^p = (2^{\frac{p-1}{2}}\alpha).$$

Since the only units of $\mathcal{O}_K$ are $\{1, -1\}$, this implies that I is a principal ideal if and only if $\pm 2^{\frac{p-1}{2}}\alpha$ is a power of p in $\mathcal{O}_K$. From Proposition 12, we know that $\pm 2^{\frac{p-1}{2}}\alpha$ is not a pth power in $\mathcal{O}_K$. Hence the class group of $\mathbb{Q}(\sqrt{1-2m^p})$ has an element I of order p. □

We prove a corollary of Theorem 3.

COROLLARY 13. *For every odd prime p, there exist infinitely many imaginary biquadratic fields whose class number is divisible by p.*

Proof. Fix an odd prime p. Consider the set

$$S_1 = \{m \in \mathbb{Z}^+ \mid m \text{ is not a square}, m \equiv 1 \pmod 4 \text{ and}$$
$$\text{the class number of } \mathbb{Q}(\sqrt{1-2m^p}) \text{ is divisible by } p\}.$$

By Lemma 9, the equation $1 - 2x^p = y^2$ has only finitely many solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Hence, it follows from Theorem 3 and Dirichlet's theorem on arithmetic

https://doi.org/10.1017/S001708952100015X Published online by Cambridge University Press

progression that S_1 contains infinitely many primes q with $q \equiv 1 \pmod 4$, which implies that S_1 is an infinite set.

For $m \in S_1$, consider the imaginary biquadratic field $K_m = \mathbb{Q}(\sqrt{1-2m^p}, \sqrt{m})$. Denote $L_m^1 := \mathbb{Q}(\sqrt{1-2m^p})$, $L_m^2 := \mathbb{Q}(\sqrt{m})$ and $L_m^3 := \mathbb{Q}\left(\sqrt{1-2m^p}\sqrt{m}\right)$. Since m is not a square, L_m^2 is actually a quadratic field. We observe that $L_m^1 \neq L_m^2$ because $1-2m^p \equiv 3 \pmod 4$. Thus L_m^1, L_m^2 and L_m^3 are the three quadratic subfields of K_m. Let h_m, h_m^1, h_m^2 and h_m^3 be the class numbers of K_m, L_m^1, L_m^2 and L_m^3 respectively. Then by Lemma 2 in [6], we have $h_m = \frac{h_m^1 h_m^2 h_m^3}{2^i}$ where $i = 0, 1$. Since $m \in S_1$, the prime p divides h_m^1. Since p is odd, p divides h_m. The infiniteness of the set $\{K_m | m \in S_1\}$ follows from that of the set S_1. □

ACKNOWLEDGEMENTS. We thank Prof. Kalyan Chakraborty for introducing this problem to us. We thank IISER Tiruvananthapuram for providing excellent working conditions. We thank Azizul Hoque for his comments and the careful reading of this article. We acknowledge SageMath for the numerical evidence of our theorems. We would like to express our deep gratitude to the anonymous referee for carefully analyzing the article, refining several arguments, and making suggestions for a better presentation.

REFERENCES

1. Y. Bugeaud and T. N. Shorey, On the number of solutions of the generalized Ramanujan-Nagell equation, *J. Reine Angew. Math.* **539** (2001), 55–74.

2. 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.

3. J. Chattopadhyay and S. Muthukrishnan, On the simultaneous 3-divisibility of class numbers of triples of imaginary quadratic fields, *Acta Arith.* **197**(1) (2021), 105–110.

4. H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Mathematics, vol. 1068 (Springer, Berlin, 1984), 33–62.

5. J. H. E. Cohn, On the class number of certain imaginary quadratic fields, *Proc. Amer. Math. Soc.* **130**(5) (2002), 1275–1277.

6. G. Cornell, A note on the class group of composita, *J. Number Theory* **39**(1) (1991), 1–4.

7. B. H. Gross and D. E. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, *Invent. Math.* **44**(3) (1978), 201–224.

8. A. Hoque and K. Chakraborty, Divisibility of class numbers of certain families of quadratic fields, *J. Ramanujan Math. Soc.* **34**(3) (2019), 281–289.

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

10. A. Ito, A note on the divisibility of class numbers of imaginary quadratic fields $\mathbf{Q}(\sqrt{a^2-k^n})$, *Proc. Japan Acad. Ser. A Math. Sci.* **87**(9) (2011), 151–155.

11. Y. Kishi, Note on the divisibility of the class number of certain imaginary quadratic fields, *Glasg. Math. J.* **51**(1) (2009), 187–191.

12. Y. Kishi and K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three, *J. Number Theory* **80**(2) (2000), 209–217.

13. S. Krishnamoorthy, A note on the Fourier coefficients of a Cohen-Eisenstein series, *Int. J. Number Theory* **12**(5) (2016), 1149–1161.

14. S. R. Louboutin, On the divisibility of the class number of imaginary quadratic number fields, *Proc. Am. Math. Soc.* **137**(12) (2009), 4025–4028.

15. M. Ram Murty, *The abc conjecture and exponents of class groups of quadratic fields*, Number theory (Tiruchirapalli, 1996), Contemporary Mathematics, vol. 210 (American Mathematical Society, Providence, RI, 1998), 85–95.

16. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, 2nd edition (Springer, Dordrecht, 2009).

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

https://doi.org/10.1017/S001708952100015X Published online by Cambridge University Press