SeMA (2016) 73:213–217
DOI 10.1007/s40324-016-0065-1

On the divisibility of class numbers of quadratic fields and the solvability of diophantine equations

Azizul Hoque[1] · **Helen K. Saikia**[1]

Received: 16 December 2015 / Accepted: 12 January 2016 / Published online: 1 February 2016

Abstract In this paper we provide criteria for the insolvability of the Diophantine equation $x^2 + D = y^n$. This result is then used to determine the class number of the quadratic field $\mathbb{Q}(\sqrt{-D})$. We also determine some criteria for the divisibility of the class number of the quadratic field $\mathbb{Q}(\sqrt{-D})$ and this result is then used to discuss the solvability of the Diophantine equation $x^2 + D = y^n$.

Keywords Diophantine equation · Imaginary quadratic field · Class number

Mathematics Subject Classification 11R29 · 11D61 · 11R41

1 Introduction

The class number problem of quadratic fields is one of the most intriguing unsolved problems in Number Theory and it has been the object of attention for many years of researchers. Ankeny et al. [1], Chakraborty et al. [5], Kishi et al. [14], Nagel [20], Soundararajan [25], Weinberger [26] and Yu [29] studied the class number problem of quadratic fields. It was proved by Nagel [20] that there are infinitely many quadratic number fields each with class number divisible by a given positive integer. Weinberger [26] showed that for all positive integers n, there are infinitely many real quadratic fields each with class number divisible by n. In [11], we have proved that there exist infinitely many imaginary quadratic fields whose class numbers are divisible by 3. Recently in [10–13], we have found some useful results on the divisibility of class numbers of real and imaginary quadratic fields. The class numbers of quadratic fields can be used in study of Diophantine equations. On the other hand, the class

✉ Azizul Hoque
ahoque.ms@gmail.com

Helen K. Saikia
hsaikia@yahoo.com

[1] Department of Mathematics, Gauhati University, Guwahati 781014, India

numbers of quadratic fields can be determined by the solvability of Diophantine equations. Thus there has been considerable attention given to the investigation of relationship between the solvability of Diophantine equations and the class numbers of related quadratic fields. The journey to this investigation has been started in 1853 by Lebesgue [15] in which he discussed the solvability of the Diophatine equation $x^2 + D = y^n$. He proved, using an elementary factorization argument, that this equation has no solution for $D = 1$, except $x = 0$ and $y = 1$. Many special cases of this equation have been considered over the several years, but most of the outcomes for general values of n are of honestly recent origin. Fermat showed, a proof is given in [9], that for $D = 2$ and $n = 3$, this equation has only one solution, that is, $x = 5$, $y = 3$. In 1943, Ljunggren [16] generalised Fermat's result and proved that this equation has no solution when $D = 2$ and $x \neq 5$. In 1954, this result was alternatively established by Nagell [22]. In 1923, Nagell [21] proved that this equation has no solutions when $D = 3$. This result was duplicated by Brown [4] in 1975 and subsequently by Cohn [7] in 1993. Nagell [21] also proved that this equation has no solution for $D = 5$. In 1955, Nagell [23] showed that for $D = 4$, this equation has only one solution, that is, $x = 2$ and $y = 11$. In 1992, Cohn [6] showed that for $D = 19$, this equation has only solution: $x = 18$, $y = 7$, $n = 3$ and $x = 22434$, $y = 55$, $n = 5$. Finally, Cohn [8] published a historical survey of this equation in 1993. For any positive integer D, Wren [27] in 1973 and Blass [2] in 1976, proved the impossibility of the solutions to this equation when $n = 5$. After a couple of year, Blass and Steiner [3] discussed the insolvability of this equation when $n = 7$.

The primary objective of this paper is to investigate the relationship between solvability of the Diophantine equation $x^2 + D = y^n$, $D > 1$ being an integer and the divisibility of the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. This type of relationships can be found in [17–19,24,28].

2 Main results

In this section we discuss and prove our main results. Throughout this section we consider $K = \mathbb{Q}(\sqrt{-D})$ and by $h(K)$ we denote the class number of the quadratic field K.

Theorem 2.1 *Let $D \equiv 1, 2\ (mod\, 4)$ be a square-free positive integer and $n > 1$ be an odd integer satisfying $na^{n-1} \not\equiv \pm 1\ (mod\, D)$, for some integer a. If $\gcd(n, h(K)) = 1$, then the Diophantine equation*

$$x^2 + D = y^n \tag{1}$$

has no solutions.

Proof Let y be an even integer. Then $y^n \equiv 0 (mod\, 4)$ and thus Eq. (1) gives $x^2 \equiv 2, 3 (mod\, 4)$.

If $D \equiv 1\ (mod\, 4)$, then Eq. (1) implies x is odd and thus $x^2 \equiv 1\ (mod\, 4)$. This is a contradiction.

Again if $D \equiv 2\ (mod\, 4)$, then Eq. (1) implies x is even and thus $x^2 \equiv 0\ (mod\, 4)$. This is again a contradiction.

Thus y must be an odd integer.

Suppose p be a prime number such that $p|gcd(x, y)$, then by Eq. (1), $p|D$ and thus $p = D$. Therefore Eq. (1) implies $D^2|D$. This is a contradiction. Thus $gcd(x, y) = 1$.

Suppose (x_0, y_0) be an integral solution to the Eq. (1). Then by the above discussion, y_0 is odd and $gcd(x_0, y_0) = 1$.

Consider the following factorization in the ring of integers $\mathbb{Z}\left[\sqrt{-D}\right]$ of the quadratic field K:

$$(x_0 + \sqrt{-D})(x_0 - \sqrt{-D}) = y_0^n \tag{2}$$

If $\mathcal{P}$ is a prime ideal in $\mathbb{Z}\left[\sqrt{-D}\right]$ such that $\mathcal{P}$ is a common divisor of the ideals $(x_0 + \sqrt{-D})$ and $(x_0 - \sqrt{-D})$, then $\mathcal{P}|(2x_0)$.

Also Eq. (2) gives $\mathcal{P}|(y_0)$. This implies $\mathcal{P} \nmid (2)$ as y_0 is odd, and thus $\mathcal{P}|(x_0)$. This contradicts to the fact that $\gcd(x_0, y_0) = 1$. Therefore the ideals $(x_0 + \sqrt{-D})$ and $(x_0 - \sqrt{-D})$ are coprime to each other. Thus we can write

$$(x_0 + \sqrt{-D}) = \mathfrak{a}^n$$
$$(x_0 - \sqrt{-D}) = \mathfrak{b}^n$$

for some ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathbb{Z}\left[\sqrt{-D}\right]$.

Since $\gcd(n, h(K)) = 1$, therefore $\mathfrak{c}^{h(K)}$ is a principal ideal for any ideal $\mathfrak{c}$ in $\mathbb{Z}\left[\sqrt{-D}\right]$, and moreover $\mathfrak{a}^n$ and $\mathfrak{b}^n$ are principal ideals, so that the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are principal. Furthermore, since 1 and -1 are the only units in $\mathbb{Z}\left[\sqrt{-D}\right]$, thus we have

$$(x_0 + \sqrt{-D}) = (a + b\sqrt{-D})^n$$

for some $a, b \in \mathbb{Z}$.

Comparing imaginary part, we see that

$$1 = \binom{n}{1} a^{n-1} b - \binom{n}{3} a^{n-3} b^3 D + \cdots + (-1)^{\frac{n-1}{2}} b^n D^{\frac{n-1}{2}} \tag{3}$$

Thus $b|1$ and hence $b = \pm 1$.

Now Eq. (3) implies $\pm 1 = \binom{n}{1} a^{n-1} - \binom{n}{3} a^{n-3} D + \cdots + (-1)^{\frac{n-1}{2}} D^{\frac{n-1}{2}}$. This implies $na^{n-1} \equiv \pm 1 (mod D)$. This contradicts to the hypothesis.

This completes the proof. □

As a consequence we have the following result.

Corollary 2.2 *Let $D \equiv 1, 2\ (mod\ 4)$ be a square-free positive integer and p be an odd prime satisfying $pa^{p-1} \not\equiv \pm 1\ (mod D)$, for some integer a. If $x^2 + D = y^p$ is has integral solution then $p|h(K)$.*

We now fix y as a prime, that is consider the Diophantine equation

$$x^2 + D = p^n \tag{4}$$

where p is a prime and $n > 1$ is an odd integer. Then the following cases arise:

(a) $D \equiv 0\ (mod\ 4)$ if one of the following conditions is satisfied:

(i) x is odd and $p \equiv 1\ (mod\ 4)$.
(ii) x is even and $p = 2$

(b) $D \equiv 1\ (mod\ 4)$ if x is even and $p \equiv 1\ (mod\ 4)$.
(c) $D \equiv 2\ (mod\ 4)$ if x is odd and $p \equiv 3\ (mod\ 4)$.
(d) $D \equiv 3\ (mod\ 4)$ if one of the following conditions is satisfied:

(i) x is even and $p \equiv 3\ (mod\ 4)$
(ii) x is odd and $p = 2$

We are now in a position to state and prove the following result.

Theorem 2.3 *Let $n > 1$ be an odd integer, D be a square-free positive integer and p be a prime number satisfying the Eq. (4). The ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ has an element of order n if one of the following conditions is satisfied:*

(I) x is an integer and satisfying $x^2 < \frac{p^n}{2}$.
(II) x is an odd integer and $p = 2$ satisfying $x^2 < 2^{n-1}$.
(III) x is an even integer and $p \equiv 1(mod\, 4)$ satisfying $x^2 < \frac{p^n}{p-1}$.

Proof Let us first consider the conditions given in (I). Then by condition (c) and condition (i) of (d), we see that either $D \equiv 2\ (mod\, 4)$ or $D \equiv 3\ (mod\, 4)$ according as x is odd or even. In either cases, the ring of integers of $\mathbb{Q}(\sqrt{-D})$ is $\mathbb{Z}\left[\sqrt{-D}\right]$.

Consider the following factorization in $\mathbb{Z}\left[\sqrt{-D}\right]$:

$$(x + \sqrt{-D})(x - \sqrt{-D}) = p^n \tag{5}$$

Since $(x + \sqrt{-D})$ and $(x - \sqrt{-D})$ are coprime as ideals in $\mathbb{Z}\left[\sqrt{-D}\right]$, we have $(x + \sqrt{-D}) = \mathfrak{a}^n$ and $(x - \sqrt{-D}) = \mathfrak{b}^n$ for some ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathbb{Z}\left[\sqrt{-D}\right]$ with $\mathfrak{a}\mathfrak{b} = (p)$. Thus the order of $\mathfrak{a}$ in the ideal class group of $\mathbb{Q}(\sqrt{-D})$ is a divisor of n.

Let $\mathfrak{a}^m = (u + v\sqrt{-D})$ for some $u, v \in \mathbb{Z}$. Then

$$p^m = u^2 + v^2 D \tag{6}$$

If $v = 0$, then $p^m = u^2$. This contradicts to the fact that n is odd. Thus $v \neq 0$ and hence Eq. (6) implies $p^m \geq D$.

Again, $x^2 < \frac{p^n}{2}$ implies $D > \frac{p^n}{2}$. Thus $p^m \geq D > \frac{p^n}{2}$. This leads to a contradiction if $m < n$. Hence $\mathfrak{a}^n = (u + v\sqrt{-D})$ and $\mathfrak{a}^m$ is not principal for any $m < n$. Thus there is an element of order n in the ideal class group of $\mathbb{Q}(\sqrt{-D})$.

Similarly the result holds if we consider the conditions given in (II).

Finally we consider the conditions given in (III). Then by condition (b), we see that $D \equiv 1(mod\, 4)$. Thus the ring of integers of $\mathbb{Q}(\sqrt{-D})$ is $\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$. In the ring $\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$, we consider the factorization as given in the Eq. (5). However in this case the ideals $\mathfrak{a}$ and $\mathfrak{b}$ must be in $\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$.

Let $\mathfrak{a}^m = (\frac{u+v\sqrt{-D}}{2})$ for some $u, v \in \mathbb{Z}$. Then

$$4p^m = u^2 + v^2 D \tag{7}$$

If $v = 0$, then $4p^m = u^2$. This contradicts to the fact that n is odd. Thus $v \neq 0$ and hence Eq. (7) implies $4p^m \geq D$.

Again, $x^2 < \frac{p^n}{p-1}$ implies $D > p^n(\frac{p-2}{p-1})$. Thus $4p^m \geq D > p^n(\frac{p-2}{p-1})$. This leads to a contradiction if $m < n$. Thus $\mathfrak{a}^n = (\frac{u+v\sqrt{-D}}{2})$ and $\mathfrak{a}^m$ is not principal for any $m < n$. Hence there is an element of order n in the ideal class group of $\mathbb{Q}(\sqrt{-D})$.

As a consequence we provide the following criteria on the solvability of the Diophantine Eq. (4). □

Corollary 2.4 (x_0, y_0) *is an integral solution of the Eq. (4), where $n > 1$ is an odd integer and D is a positive square-free integer if one of the following conditions is satisfied:*

(i) x_0 is an integer and y_0 is a prime $\equiv 3\ (mod\, 4)$ satisfying $x_0^2 < \frac{y_0^n}{2}$.

(ii) x_0 *is an odd integer and* $y_0 = 2$ *satisfying* $x_0^2 < 2^{n-1}$.

(iii) x_0 *is an even integer and* $y_0 \equiv 1\ (mod\ 4)$ *is a prime satisfying* $x_0 < \frac{y_0^n}{y_0-1}$.

Acknowledgments Both Authors acknowledge UGC for financial support.

References

1. Ankeny, N.C., Artin, E., Chowla, S.: The class number of real quadratic fields. Ann. Math. **56**, 479–493 (1952)
2. Blass, J.: A note on Diophantine equation $y^2 + k = x^5$. Math. Comp. **30**, 638–640 (1976)
3. Blass, J., Steiner, R.: On the equation $y^2 + k = x^7$. Utilitas Math. **13**, 293–297 (1978)
4. Brown, E.: Diophantine equations of the form $x^2 + D = y^n$. J. Reine Angew. Math. **274**, 385–389 (1975)
5. Chakraborty, K., Murty, R.: On the number of real quadratic fields with class number divisible by 3. Proc. Am. Math. Soc. **131**, 41–44 (2002)
6. Cohn, J.H.E.: The diophantine equation $x^2 + 19 = y^n$. Acta Arith. **61**(2), 193–197 (1992)
7. Cohn, J.H.E.: The Diophantine equation $x^2 + 3 = y^n$. Glasgow Math. J. **35**, 203–206 (1993)
8. Cohn, J.H.E.: The Diophantine equation $x^2 + C = y^n$. Acta Arith. **65**(4), 367–381 (1993)
9. Euler, L.: Algebra, vol. 2, 2nd edn. J. Johnson and Co., London (1810)
10. Hoque, A., Saikia, H.K.: A note on quadratic fields with class number divisible by 3, SeMA J., 2015 (in Press). doi:10.1007/s40324-015-0051-z
11. Hoque, A., Saikia, H.K.: A family of imaginary quadratic fields whose class numbers are multiples of three. J. Taibah Univ. Sci. **9**, 399–402 (2015)
12. Hoque, A., Saikia, H.K.: On generalized Mersenne primes and class-numbers of equivalent quadratic fields and cyclotomic fields. SeMA J. **67**, 71–75 (2015)
13. Hoque, A., Saikia, H.K.: On generalized Mersenne primes. SeMA J. **66**, 1–7 (2014)
14. Kishi, Y., Miyake, K.: Parametrization of the quadratic fields whose class numbers are divisible by three. J. Number Theory **80**, 209–217 (2000)
15. Lebesgue, V.A.: Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. N. Ann. Math. **9**, 178 (1850)
16. Ljunggren, W.: Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen, Ark. Mat. Astr. Fys. **29A**(13), 1–11 (1943)
17. Mollin, R.A.: Diophantine equations and class numbers. J. Number Theory **24**, 7–19 (1986)
18. Mollin, R.A.: Class numbers of quadratic fields determined by solvability of Diophantine equations. Math. Comp. **48**(177), 233–242 (1987)
19. Mollin, R.A.: Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields. Glasgow Math. J. **38**, 195–197 (1996)
20. Nagel, T.: Über die Klassenzahl imaginär quadratischer zahlkorper. Abh. Math. Sem. Univ. Hamburg **1**, 140–150 (1922)
21. Nagell, T.: Sur l'impossibilité de quelques équations à deux indéterminées. Norsk. Mat. Forensings Skrifter **13**, 65–82 (1923)
22. Nagell, T.: Verallgemeinerung eines Fermatschen Satzes. Arch. Math. **5**, 153–159 (1954)
23. Nagell, T.: Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns. Nova Acta Regiae Soc. Sci. Upsaliensis, **16**(2), 1–38 (1955)
24. Pekin, A.: On some solvability results of Diophantine equations and the class number of certain real quadratic fields. Int. J. Contemp. Math. Sci. **4**(32), 1605–1609 (2009)
25. Soundararajan, K.: Divisibility of class numbers of imaginary quadratic fields. J. Lond. Math. Soc. **61**, 681–690 (2000)
26. Weinberger, P.J.: Real quadratic fields with class number divisible by n. J. Number Theory **5**, 237–241 (1973)
27. Wren, B.M.E.: $y^2 + D = x^5$. Eureka **36**, 37–38 (1973)
28. Yokoi, H.: On the Diophantine equation and the class number of real subfields of a cyclotomic field. Nagoya Math. J. **91**, 151–161 (1983)
29. Yu, G.: A note on the divisibility of class numbers of real quadratic fields. J. Number Theory **97**, 35–44 (2002)