Journal of Nepal Mathematical Society (JNMS)
ISSN: 2616-0153 (Print), 2616-0161 (Online)
Vol. 6, Issue 2, 2024 (February): 1-6
DOI: https://doi.org/10.3126/jnms.v6i2.63005
©*Nepal Mathematical Society*

Research Article
Received Date: Nov 26, 2023
Accepted Date: Feb 08, 2024
Published Date: Feb 26, 2024

Efficient Approaches to Solve Quadratic Diophantine Equations and their Time Complexity

Bal Bahadur Tamang[1,*] and Ajaya Singh[2]

[1]Department of Mathematics, Mahendra Ratna Multiple Campus, Ilam, Tribhuvan University, Nepal
[2]Central Department of Mathematics, Tribhuvan University, Nepal

[*]Correspondence to: Bal Bahadur Tamang, Email: bal.785709@iost.tu.edu.np

Abstract: *In this paper, we present an efficient approach to solve quadratic Diophantine equations and analyze their time complexity. We propose a deterministic polynomial-time algorithm that provides an upper bound on the elementary operations required to solve such equations. We also present a non-deterministic polynomial-time algorithm for the construction of quadratic non-resiude modulo d, which is a more efficient alternative to the deterministic approach.*

Keywords: Diophantine equations, Continued fraction, Quadratic residue, Pythagorean triples, Time complexity

1 Introduction

Diophantine equations are particularly valuable because their solutions are positive integers. The investigation of a nontrivial integer solution to the quadratic Diophantine equation is of the form $x^2 - dy^2 = N$, where $x, y \in \mathbb{Z}$ and $N \in \mathbb{Z}, N \neq 0$, and $d > 1$ is square-free, which is known as the general Pell's equation in [3]. Positive Pell's equation of the form

$$x^2 - dy^2 = 1 \tag{1}$$

was first investigated by Brahmagupta and Bhaskara in [2]. Lagrange [10] found an infinite number of solutions to the equation (1). It is found that there is a nontrivial solution (x_0, y_0), called the least solution, and other solutions represented by (x_n, y_n), where $(x_n + y_n\sqrt{d}) = (x_0 + y_0\sqrt{d})^n$, where $n \in \mathbb{N}$. On the other hand, the negative Pell's equation of the form

$$x^2 - dy^2 = -1 \tag{2}$$

does not always have a solution. Etienne Fouvry and Jurgen Kluners [5] have also derived an asymptotic expression for the integer d, where the least solution of the equation (2) has a norm of -1. If the periodic length of the continued fraction expansion of $\sqrt{d}$ is even, the equation (2) is unsolvable. However, if the periodic length of $\sqrt{d}$ is odd, the equation (2) is solvable and there is an infinite number of integer solutions. In addition, if a prime number $d \equiv 3(\bmod 4)$ or if d is divisible by 4, the equation (2) is unsolvable. Assume that the equation (2) is solvable and the least solution is (r_0, t_0). The general solution of the equation (2) is (r_k, t_k), where

$$r_k = r_0 a_k + d t_0 b_k,\ t_k = t_0 a_k + r_0 b_k \tag{3}$$

and (a_k, b_k) is the solution of Pell's equation $a^2 - db^2 = 1$, where $k \geq 0$. The relationship between (r_0, t_0) and (a_0, b_0) is $(a_0 + b_0\sqrt{d}) = (r_0 + t_0\sqrt{d})^2 = \Big((r_0^2 + dt_0^2) + (2r_0t_0)\sqrt{d}\Big)$. It gives,

$$a_0 = r_0^2 + dt_0^2 \Rightarrow r_0 = \sqrt{\frac{a_0 - 1}{2}}, \quad b_0 = 2r_0t_0 \Rightarrow t_0 = \frac{b_0}{2r_0} = \frac{1}{\sqrt{2}}\sqrt{\frac{1}{a_0 - 1}}$$

Therefore, the least solution of the equation (1) is (a_0, b_0), and for the integer $d \equiv 1, 2(\bmod 4)$, the solution of the equation (2) is

$$(r_0, t_0) = \left(\sqrt{\frac{a_0 - 1}{2}}, \frac{1}{\sqrt{2}}\sqrt{\frac{1}{a_0 - 1}}\right)$$

which is the least solution of the equation (2). Using the general solution (3), the explicit solutions of equation (2) are as follows:

$$\begin{aligned} r_k &= \frac{1}{2}\left\{(r_0+t_0\sqrt{d})(a_1+b_1\sqrt{d})^k+(r_0-t_0\sqrt{d})(a_1-b_1\sqrt{d})^k\right\} \\ t_k &= \frac{1}{2\sqrt{d}}\left\{(r_0+t_0\sqrt{d})(a_1+b_1\sqrt{d})^k+(r_0-t_0\sqrt{d})(a_1-b_1\sqrt{d})^k\right\},\ k\geq 1 \end{aligned}$$

Mollins and Srinivasan [14] proposed a condition $a_0 \equiv -1(\bmod 2d)$, which is simplified by the elementary approach, because it is obvious that $a_0 = r_0^2 + dt_0^2$. The continued fraction approach provides a solution for this equation, but it is not time saving. Lagarias [9] is faster than the continued fraction and provides an evaluation tool to conclude if an equation (2) has a solution when d is a complete factorization.

Grytczuk, Luca, and Wojtowicz [6] state that the solution of equation (2) can be found in positive integers x and y if there exists a primitive Pythagorean triple $(\alpha;\beta;\gamma)$ and positive integers u and v such that $d = u^2+v^2, |u\alpha - v\beta| = 1$, where $(\alpha;\beta;\gamma)$ is a primitive Pythagorean triple that is pairwise relatively prime and satisfies the conditions $\alpha^2+\beta^2=\gamma^2$. LeVeque [13] states that the solution of the equation (2) contains the primitive representation of d as the sum of two squares. Pythagorean triples are an essential part of the necessary and sufficient conditions to complete the solution of equation (2). Hardy and Williams [7] found that the equation (2) is solvable if and only if d is the sum of u^2 and v^2, where $u, v \in \mathbb{N}$ and u are odd numbers.

The Legendre symbol $\left(\frac{a}{p}\right)$ is a function of a and p, which represents an integer as a quadratic (non) residue modulo p. Legendre [11] was the first to use this symbol. He found that the equation (2) is unsolvable if a prime $d \equiv 3(\bmod 4)$. However, if a prime $d \equiv 1(\bmod 4)$, the equation (2) is solvable. Dirichlet [4] states that the equation (2) has a solution if $d = pq$, where a prime number $p \equiv 1(\bmod 4)$ such that $\left(\frac{p}{q}\right) = -1$, and p, q are distinct primes. Dirichlet also considered the case in which d is the product of three different primes. The residue symbol obtained from d can be used to create situations on d that prove the equation (2) is either solvable or unsolvable. For $d = p_1p_2\cdots p_N$, Tano [16] has found residues among the p_i which, if true, would confirm that the equation (2) is solvable. Scholz [15] used field theory and found that the equation (2) cannot be solved if $\left(\frac{p}{q}\right)_4 \neq \left(\frac{q}{p}\right)_4$ under the condition $d = pq$ with $p \equiv q \equiv 1(\bmod 4)$. However, the equation (2) is sometimes solvable and sometimes not in the case $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$.

Time complexity, also known as computational complexity, is a measure of the time it takes a computer to execute an algorithm. The most common method for estimating time complexity is to count the number of basic operations that the algorithm performs, assuming that each operation takes the same processing time. This results in the assumption that the time spent and the number of basic operations performed by the algorithm is related by a constant factor. Lenstra [12] gives an algorithm based on the power products and smooth numbers. The solution of the equation (1) is faster than the continued fraction in terms of running time. On the other hand, the residue symbol provides a more complete check of those d for which equation (2) can be solved. Hua [8] determined the upper bound for the period length of the continued fraction of $\sqrt{d}$ is $\mathbf{O}(\sqrt{d}\log d)$.

2 Approaches to Solving Quadratic Diophantine Equations

In this section, we discuss various efficient approaches for solving quadratic Diophantine equations. One efficient approach is the continued fraction, which represents a real number as an integer sequence. Another approach is the use of Pythagorean triples, i.e., sets of three positive integers (α,β,γ) such that $\alpha^2+\beta^2=\gamma^2$. The residue symbol plays a particular role in determining whether quadratic Diophantine equations can be solved.

The simple finite continued fraction expansion of $\sqrt{d}$ is the most effective way to find the least solution. If $d > 1$ is square-free, there is a positive integer r such that the continued fraction expansion of $\sqrt{d}$ is

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \cdots, a_r, 2a_0}]$$

where $a_0 = \lfloor\sqrt{d}\rfloor$ is the greatest integer and a_i for all $1 \leq i \leq r$, is the partial denominator of the continued fraction. The k^{th} convergent is given by

$$\frac{P_k}{Q_k} = [a_0; \overline{a_1, a_2, \cdots, a_r, 2a_0}]$$

where

$$P_k = a_k P_{k-1} + P_{k-2},\ P_{-2} = 0,\ P_{-1} = 1, Q_k = a_k Q_{k-1} + Q_{k-2},\ \ Q_{-2} = 1,\ Q_{-1} = 0,\ k \geq 0$$

Then the expression is given by

$$\frac{(P_k + \sqrt{d})}{Q_k} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}}$$

where

$$P_0 = 0, Q_0 = 1, a_0 = \lfloor\sqrt{d}\rfloor, P_k = a_{k-1}Q_{k-1} - P_{k-1}, a_k = \left\lfloor \frac{(P_k + \sqrt{d})}{Q_k} \right\rfloor, d = P_{k+1}^2 + Q_k Q_{k+1}, k \geq 1$$

The equation (2) can only be solved if the expansion of the continued fractions $\sqrt{d}$ has an odd period length r. Assuming that $r = 2n - 1$, positive solutions of equation (2) is

$$(r_s, t_s) = \left(A_{2(j-1)}, B_{2(j-1)}\right),\ j = n + s(2n - 1),\ s \geq 0$$

In fact, the general solution to equation (2) is

$$(r_s + t_s\sqrt{d}) = (r_0 + t_0\sqrt{d})^{2s+1},$$

where $(r_0, t_0) = \left(A_{2(n-1)}, B_{2(n-1)}\right)$ is the least solution to equation (2).
Moreover, if $r = u\beta + v\alpha$, $t = \gamma$, in $d = u^2 + v^2$ and $\alpha^2 + \beta^2 = \gamma^2$, then

$$dy^2 = (u^2 + v^2)(\alpha^2 + \beta^2) \Rightarrow dy^2 = x^2 + 1$$

Therefore, $(r, t) = (u\beta + v\alpha, \gamma)$ is a solution of equation (2). The primitive Pythagorean triples (α, β, γ) with α is even, are

$$\alpha = 2pq, \quad \beta = p^2 - q^2, \quad \gamma = p^2 + q^2, \quad p > q > 0, \quad \gcd(p, q) = 1$$

By counter example, if

$$(p, q) = (2, 1),\ (\alpha, \beta, \gamma) = (2pq, (p^2 - q^2), (p^2 + q^2)) = (4, 3, 5),\ (u, v) = (2, 3),\ d = 13$$

satisfies the condition $u\alpha - v\beta = -1$. Hence $(x, y) = (18, 5)$ is the least solution of equation $x^2 - 13y^2 = -1$.

Theorem 2.1. *Assume that $p_1, p_2, \cdots, p_r$ denotes distinct primes such that $d = p_1 p_2 \cdots p_r$, where r is either 2 or an odd number, and if the following conditions hold*

$$p_s \equiv 1 (\operatorname{mod} 4),\ 1 \leq s \leq r \tag{4}$$

$$\left(\frac{p_s}{p_t}\right) = -1,\ 1 \leq s,\ t \leq r, s \neq t \tag{5}$$

Then, there exists a solution to the equation $x^2 - dy^2 = -1$.

Proof. Assume that (α, β) is no solution of equation $x^2 - dy^2 = -1$. If (α, β) is the solution of $x^2 - dy^2 = 1$, then we use the equation (4) and $\alpha^2 \equiv \beta^2 + 1(\bmod\ 4)$. Then we have α is odd and β is even. Consequently, we have $\frac{\alpha-1}{2d_1} \cdot \frac{\alpha+1}{2d_2} = \frac{\beta^2}{4}$ where $d_1 d_2 = d$, $\left(\frac{\alpha-1}{2d_1}, \frac{\alpha+1}{2d_2}\right) = 1$. It follows that

$$\frac{\alpha-1}{2d_1} = u^2 \Rightarrow \alpha - 1 = 2d_1 u^2, \quad \frac{\alpha+1}{2d_2} = v^2 \Rightarrow \alpha + 1 = 2d_2 v^2.$$

If we combine these two values, we get $d_2 v^2 - d_1 u^2 = 1$. Because $\alpha \neq 1$, $u \neq 0$. Let us assume that neither d_1 nor d_2 is equal to 1. Because r must be either 2 or odd, the product of an odd prime number must be either d_1 or d_2. If p is divided by d_2 and d_1 is the product of an odd prime number. Since the result of equation (5) is $\left(\frac{d_1}{p}\right) = -1$, which is the contradiction our assumption $d_1 u^2 \equiv -1(\bmod p)$.

Similarly, it can be proved that it is also impossible for d_2 to be the product of an odd prime number. Therefore, either $d_1 = 1, d_2 = d$, or $d_1 = d, d_2 = 1$ must be true. The assumption that $x^2 - dy^2 = -1$ has no solutions is refuted by the fact that $d_1 = 1, d_2 = d$ drives to $u^2 - dv^2 = -1$. It follows that $d_1 = d, d_2 = 1$ and $v^2 - du^2 = 1$. We have

$$u^2 = \frac{\alpha-1}{2d}, \ v^2 = \frac{\alpha+1}{2} \Rightarrow uv = \frac{\beta}{2} \Rightarrow u < \beta$$

It gives (α, β) is the least solution of equation $x^2 - dy^2 = -1$, which is contradiction our assumption. Consequently, there exists a solution (α, β) for equation $x^2 - dy^2 = -1$. □

Mollin established the relationship between the equations (1) and (2) and to solve the equation (2) for integers r and t, the least solution (a_0, b_0) of the equation (1) must satisfy $a_0 \equiv -1(\bmod 2d)$.

Theorem 2.2. *If d is a non-square integer such that $d \equiv 1, 2(\bmod 4)$, then a solution of $x^2 - dy^2 = -1$ exists if and only if $a_0 \equiv -1(\bmod 2d)$, where (a_0, b_0) is the least solution of $a^2 - db^2 = 1$.*

Proof. If the equation $x^2 - dy^2 = -1$ is solvable whose least solution is (r_0, t_0), then we have $a_0 = r_0^2 + dt_0^2 \equiv -1(\bmod 2d)$ this implies that $a_0 \equiv -1(\bmod 2d)$.

On the other hand, the least solution (a_0, b_0) to equation $a^2 - db^2 = 1$ satisfies $a_0 \equiv -1(\bmod 2d)$. It gives $a_0 = -1 + 2dk$, where $k \in \mathbb{Z}$. This gives

$$(-1 + 2dk)^2 - db_0^2 = 1 \Rightarrow dk^2 - k - b_0^{'2} = 0 \Rightarrow k(dk - 1) = b_0^{'2},$$

where $b_0^{'} = \frac{b}{2}$. Since k and $(dk - 1)$ is relatively prime and we substitute $k = v^2, dk - 1 = u^2$, gives $u^2 - dv^2 = -1$. Therefore, the equation $x^2 - dy^2 = -1$ is solvable. □

Theorem (2.2) describes the solution of equation (2) and relation between to the equation (1). If (a_0, b_0) is the smallest solution for equation (1), then finding the solution of equation (2) requires the condition $a_0 \equiv -1(\bmod 2d)$.

Theorem 2.3. *Let us assume that p is an odd prime number. The negative Pell equation $x^2 - py^2 = -1$ can be solved iff $p \equiv 1(\bmod 4)$.*

Proof. Assume $x^2 - py^2 = -1$ can be solved in positive integers. As p is an odd prime number, there are positive integers a, b such that $a^2 - pb^2 = -1$. This means $a^2 - (-1) = pb^2$ and it gives $\left(\frac{-1}{p}\right) = 1$. However, we know that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-2}{2}}$, which provides $p \equiv 1(\bmod 4)$.

On the other hand, assume (a_0, b_0) is the least solution to the Pell's equation $a^2 - pb^2 = 1$, then $a_0^2 - 1 = pb_0^2$. If a_0 cannot be even, use $-1 \equiv p(\bmod 4)$. As a result, a_0 is odd. The greatest common divisor of $a_0 - 1$ and $a_0 + 1$ is 2. Thus,

$$a_0 \pm 1 = 2\xi^2, a_0 \mp 1 = 2p\eta^2,$$

where ξ and η are positive integers such that $b_0 = 2\xi\eta$. It provides $\eta < b_0$. These relation can be obtained

$$2\xi^2 - 2p\eta^2 = (a_0 \pm 1) - (a_0 \mp 1) = \pm 2 \Rightarrow \pm 1 = \xi^2 - p\eta^2$$

We are not allowed to have either the upper sign or the lower sign since $\eta < b_0$. Thus, it is possible to solve negative Pell's equation $x^2 - py^2 = -1$. □

3 Time Complexity of Quadratic Diophantine Equations

The time complexity shows the efficiency of these approaches in terms of their runtime and the number of elementary operations. In particular, for large values of d, we can determine the time complexity to solving quadratic Diophantine equations.

The fundamental solution can be provided by the continued fraction expansion of $\sqrt{d}$. But this approach is inefficient for large values of d since the complexity of the continued fraction expansion of $\sqrt{d}$ is usually a polynomial in the input size, with the running time typically approximating $\mathbf{O}(\sqrt{d})$ in [12]. This is the upper bound on the growth rate of the function, which means that the growth rate of the function is asymptotically bounded by a constant time of the square root of d for a sufficiently large values of d.

For example, there is a solution to the equation $x^2 - dy^2 = 1$ in the sense that for a small value of $d = 217$, we have a large solution of $(x, y) = (3844063, 260952)$. On the other hand, a small solution of $(x, y) = (407, 4)$ can exist for a large value of $d = 10353$.

The binary information of d must be loaded into a circuit using $\log_2 d + 1$ elementary operations. The continued fraction approach is highly efficient for obtaining the solution of the equation $x^2 - dy^2 = -1$, and the solution could be very large, if the least solution of the equation $x^2 - dy^2 = -1$ exists.

The investigation of the worst-case complexity shows that an algorithm based on the residue symbol is better than the continued fraction approach. The residue symbol is described by the prime factors of d, which can be expanded to find an algorithm for solving quadratic Diophantine equations. In non-deterministic polynomial time, the quadratic non-residue modulo p can be constructed as $\mathbf{O}((\log p)^3)$ in [9], where the running time of the algorithm is asymptotically bounded by a constant time of p. The existence of $(\log p)^3$ indicates a polynomial growth rate. Then the expression $\mathbf{O}((\log d)^5(\log\log d)(\log\log\log d))$ shows how the number of actions increases with the size of input in [9].

The extended Riemann hypothesis states that for any prime number d, there exists a quadratic non-residue $n(\bmod d)$ such that $0 < T < (\log d)^2$, where T is an efficiently computable constant, that is independent of d. The algorithm describes the upper limit of growth and provides no information about the constant factors. Then the expression $\mathbf{O}((\log d)^3(\log\log d)(\log\log\log d))$ in [9]. The efficiency of an algorithm increases when d becomes very large, whereas its runtime does not increase significantly. The expression $\mathbf{O}((\log d)^5(\log\log d)(\log\log\log d))$ is a notation for the asymptotic behavior of a function when its argument becomes large. This means that the function is bounded above by a constant multiple of the expression. This expression indicates that the function grows very slowly and is efficient for large values of d. The function is $0 < n < T(\epsilon)d^{\frac{1}{4}+\epsilon}$ in [12], where $T(\epsilon)$ is a constant that can be calculated from ϵ. This function can be used to determine the equation $x^2 - dy^2 = -1$ has integer solutions for a given d using an algorithm that run time proportional to $d^{\frac{1}{4}+\epsilon}$. The exponent $\frac{1}{4} + \epsilon$ shows how fast the function grows with increasing the size of input d. The expression $\mathbf{O}(d^{\frac{1}{4}+\epsilon})$ in [12], is a notation for the asymptotic behavior of a function when its argument becomes large.

For example, if $f(d) = \mathbf{O}(d^{\frac{1}{4}+\epsilon})$, then there exists a constant c such that $f(d) \leq c(d^{\frac{1}{4}+\epsilon})$ for all sufficiently large d. This expression shows that the running time of the algorithm is efficient for large values of d, as it does not increase much compared to the size of input.

4 Conclusion

In this work, we used some efficient approaches to solving quadratic Diophantine equations and focused on the solvability of the negative Pell's equation. Efficient approaches such as continued fractions, Pythagorean triples, and quadratic residue are investigated to identify the solvability or unsolvability of such equations. The continued fraction expansion of $\sqrt{d}$ provides the least solution but becomes inefficient for large values of d. Similarly, the residue approach provides better time complexity with a deterministic polynomial time. An algorithm can be used for the solvability of quadratic Diophantine equations using the prime factorization of d and quadratic non-residue for each prime divisor of d.

Acknowledgments
The first author would like to express my heartfelt gratitude to the University Grants Commission (UGC), Nepal, for awarding PhD Fellowship & Research Support and Travel Grants for the PhD study (UGC Award No. PhD-78/79-S&T-10). The first author equally acknowledges to the Nepal Mathematical Society (NMS) for providing with an NMS-Nick Simon PhD Fellowship 2022 for the PhD study.

References

[1] Andreescu, T., and Andrica, D., 2015, *Quadratic Diophantine Equations*, Springer, USA.

[2] Arya, S. P., 1991, On the Brahmagupta-Bhaskara equation, *Math. Ed.*, 8(1), 23-27.

[3] Dickson, L. E., 1957, Introduction to the theory of numbers, *J. Theor. Nr. Bordx.*, 14, 257-270.

[4] Dirichlet, G. L., 1834, *Einige Neue Satze uber Unbestimmte Gleichungen*, Abh. kon. Akad. Wiss. Berlin and Gesammelte Werke I.

[5] Fouvry, E., and Kluners, J. 2010, On the negative Pell equation, *Ann. of Math.*, 172(2), 2035-2104.

[6] Grytchuk, A., Luca, F., and Wojtowicz, M., 2000, The negative Pell equation and Pythagorean triples, *Proc. Japan Acad. Ser. A Math.Sci.*, 76, 91-94.

[7] Hardy, K., and Willams, K. S., 1986, On the solvability of the Diophantine equation $dV^2 - 2eVW - dW^2 = 1$, *Pacific Journal of Mathematics*, 23, 145-158.

[8] Hua, L. K., 1942, On the least solution to Pell's equation, *Bull. Amer. Math. Soc.*, 48, 731-735.

[9] Lagarias, J. C., 1980, On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$. Trans, *Amer. Math. Soc.*, 260, 485-508.

[10] Lagrange, J. L., 1768, *Histoire de l Academie de Berlin, Vol. XXIV*, Berlin.

[11] Legendre, A. M., 1830, *Theorie des Nombres*, Third edition, Librairi Scientifique A. Hermann, Paris.

[12] Lenstra, Jr. H. W., 2002, Solving the Pell equation, *Amer. Math. Soc.*, 49, 182-192.

[13] LeVeque, W. J., 1977, *Fundamentals of Number Theory*, Addison-Wesley, Massachusetts-London-Amsterdam.

[14] Mollin, R. A., and Srinivasan, A., 2010, A Note on the Negative Pell Equation, *Int. J. of Algebra*, 4(19), 919-922.

[15] Scholz, A., 1934, Uber die Losbarkeit der Gleichung $t^2 - Du^2 = -4$, *Math. Z.*, 39, 93-111.

[16] Tano, F., 1889, Sur quelques theorems de Dirichlet, *J. Reine Angew. Math.*, 105, 160-169.