ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha*, Vol. 53(2) (2023), 40-43**
(Dedicated to Professor V. P. Saxena on His 80^{th} *Birth Anniversary Celebrations)*

SOLUTIONS OF PELL'S EQUATION INVOLVING SOPHIE GERMAIN PRIMES

Manju Somanath[1], V. A. Bindu[2] and Radhika Das[3]
Department of Mathematics,
[1]National College, (Affiliated to Bharathidasan University), Tiruchirappalli, India-620 002
[2,3]Rajagiri School of Engineering & Technology, Kakkanad, Cochin, Kerala, India-682 039,
(Research Scholars, National College, Affiliated to Bharathidasan University,
Tamil Nadu, India-620 002)
Email: manjusomanath@nct.ac.in, binduva@rajagiritech.edu.in, radhikad@rajagiritech.edu.in
(Received: March 07*,* 2023*; In format: March* 27*,* 2023*; Revised: September* 06*,* 2023*;*
Accepted: September 27*,* 2023*)*

DOI: https://doi.org/10.58250/jnanabha.2023.53204

Abstract

We bring forth one of the most sought after and intriguing space pertaining to the magical world of Number Theory; and our attempts to uncover the continuing research and developments to find solutions for different aspects of the Pells equation. As indicated in this research paper, we attempt to find the possible solutions for the Pells equation $x^2 = 41y^2 - 5^m$ for all choice of $m \in \mathbb{N}$. In this paper, we focused primarily on Pells equations involving the Sophie Germain primes and present to you another mysterious series and pattern typically associated with the Pells equation. As we proceed through the research, we will bring to the fore the recurrence relations among the identified solutions.
2020 Mathematical Sciences Classification: 11D09.
Keywords and Phrases: Pell's equation, Diophantine equations, Integer solutions, Recurrence relation, Sophie Germain Primes.

1 Introduction

Pells equation, the prime object in this research. It is a representation of Diophantine equation $x^2 - dy^2 = 1$, where a non-square positive integer d is given and will search for integer solutions in x and y. As an illustration, for d having value 5; one of the integer solutions is $x = 9, y = 4$. One thing to note about is that with d not a perfect square, Pells equation will certainly have infinitely many distinct integer solutions. For initial literature, we may refer to [2, 4, 6, 7, 9, 10, 11, 14, 15]. It has multiple references to various forms of Diophantine equations, which provide us the base knowledge to go about learning more about these equations. For additional references, we may also refer to another book [16]. We imbibed the problem identification as applied for exponential Diophantine equations. Further investigation and approach techniques can be referred to [15]. Assimilating and conceptualizing these learnings enabled to look ahead and ensure the concrete steps towards our research. To dive into the crux of the problem, major ideas were incorporated from the literatures due to [8, 12, 13]. Using these inputs, we develop our solution appropriately.

The focus of discussion in this paper is a negative Pells equation given as $x^2 - dy^2 = -N$, to be solved in positive integers x and y. As indicated here forth, we are using the Sophie Germain prime in negative Pells equation in finding the positive integer solutions. In number theory, a prime number p is a Sophie Germain prime if $2p + 1$ is also prime. A safe prime indicates the number $2p + 1$ associated with a Sophie Germain prime. In the Pells equation $x^2 = 41y^2 - 5^m$, $m \in \mathbb{N}$; we are using the Sophie Germain primes 41 and 5 and will attempt to search for its non-trivial integer solutions. To derive the solutions, we approached the quest with the case of choices of m generalized in all even and odd integers. We initiated the proof by involving the odd integers 1, 3, 5.

Applying Brahma Gupta lemma [1], we obtained the sequence of non-zero distinct integer solutions. This solution addresses the many positive integer solutions obtained thence. A few research driven relations with respect to the solutions are presented. Furthermore, the process is taken a bit ahead to derive the recurrence relations that addresses such types of Pells equations.

The references that we had indicated above were just a stepping stone for us to take us to the next level. The objective we have in mind is to enable our study to put across the outcomes for understanding

the concepts and usage of cryptography. As is understood, that Cryptograph is an acknowledged area of application that involves the protection of information in the huge network of computing world. This concept goes a long way to ensure that only authorized personnel are enabled to read the concerned information and process it accordingly. It is also well understood that mathematics and mathematical concepts are the building blocks of cryptography and has gifted the world of computers a large set of algorithms and concepts to implement this protective logic involving cryptography. In the whole process, Pell's equation has been a major contributor in the science of cryptography. To generalize our research purpose, it is also come to the fore that the Sophie Germain primes are one of the leading contributors to this field. Since negative Pell equations are mostly unsolvable; it presents a complex method to undermine a strong security algorithm for cryptography. In due course, we intend to finetune our research to also generate an application to showcase the usage of Sophie Germain primes to devise a cryptographic solution.

2 Preliminaries

Theorem 2.1. *If x_1, y_1 is considered as the fundamental solution of $x^2 - dy^2 = 1$. Then to be noted is that every positive solution of the equation is given by x_n, y_n where x_n and y_n are the integers determined from $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, for $n = 1, 2, 3, ...$*

2.1 Solubility of the negative Pell equation - Our test approach

We assume that D is a positive integer, and considered not a perfect square. Then the negative Pell equation $x^2 - Dy^2 = -1$ is considered soluble if and only if D is expressed as $D = a^2 + b^2$, $gcd(a, b) = 1, a$ and b are positive, b is odd and the Diophantine equation, $-bV^2 + 2aVW + bW^2 = 1$ has a solution. (We highlight this as the case of solubility that occurs for exactly one such (a, b)). The solubility concepts were derived from article [3].

The Algorithm followed by us is illustrated below

(i) We will first find all expressions of D considered as a sum of two relatively prime squares using Cornacchia's method [5]. If none exists - the negative Pell equation is not soluble.

(ii) For each representation $D = a^2 + b^2, gcd(a, b) = 1, a$ and b positive, b odd, we will test the solubility of $-bV^2 + 2aVW + bW^2 = 1$ using the Lagrange-Matthews algorithm [3]. If soluble and it exists - the negative Pell equation is soluble.

(iii) If each representation yields no probable solution, then the negative Pell equation is insoluble.

Theorem 2.2. *Let us consider p to be a prime. The negative Pell equation $x^2 - py^2 = -1$ is considered solvable if and only if $p = 2$ or $p \equiv 1(mod 4)$.*

Proof. This paper focusses on a negative Pell equation $x^2 = 41y^2 - 5^m$, $m \in \mathbb{N}$. For the negative Pell equation, we will consider the prime $p = 41$, which satisfies the identified conditions of Theorem 2.2. Therefore, we can substantiate with certainty the proof that the negative Pells equation $x^2 = 41y^2 - 5^m$, $m \in \mathbb{N}$ is solvable and prevalent in integers.

Using the Algorithm as illustrated in Theorem 2.1 and testing for $(a, b) = (4, 5) : -bV^2 + 2aVW + bW^2 = 1$ has a solution $(V, W) = (2, 1)$, so $x^2 - 41y^2 = -1$ is soluble. □

3 Method of Analysis

Choice 1: $m = 1$

The Pell equation in focus is

$$x^2 = 41y^2 - 5. \tag{3.1}$$

Let (x_0, y_0) be the initial solution of (3.1) given by $x_0 = 6; y_0 = 1$.

In our quest to find the other solutions of (3.1), consider the generalized form of the Pell equation

$$x^2 = 41y^2 + 1. \tag{3.2}$$

The initial solution of (3.2) is (2049,320) and the general solution $(\tilde{x_n}, \tilde{y_n})$ given by Theorem 2.1 as $\tilde{x_n} = \frac{1}{2}f_n$, $\tilde{y_n} = \frac{1}{2\sqrt{41}}g_n$, where $f_n = (2049 + 320\sqrt{41})^{(n+1)} + (2049 - 320\sqrt{41})^{(n+1)}$, $g_n = (2049 + 320\sqrt{41})^{(n+1)} - (2049 - 320\sqrt{41})^{(n+1)}$, $n = 0, 1, 2 \cdots$.

By applying Brahma Gupta lemma [1] between (x_0, y_0) and $(\tilde{x_n}, \tilde{y_n})$ the possible sequence of non-zero distinct integer solutions to (3.1) are obtained as given below

$$x_{n+1} = x_0\tilde{x_n} + dy_0\tilde{y_n},\ y_{n+1} = x_0\tilde{y_n} + dy_0\tilde{x_n}, \tag{3.3}$$

$$x_{n+1} = \frac{1}{2}[6f_n + \sqrt{41}g_n],\ y_{n+1} = \frac{1}{2\sqrt{41}}[\sqrt{41}f_n + 6g_n]. \tag{3.4}$$

Also to be noted is the recurrence relation satisfied by the solution of (3.1) given by

$$x_{n+2} - 4098\ x_{n+1} + x_n = 0,\ y_{n+2} - 4098\ y_{n+1} + y_n = 0. \tag{3.5}$$

Choice 2: $m = 3$

The Pell equation is

$$x^2 = 41y^2 - 125. \tag{3.6}$$

Let (x_0, y_0) be the initial solution of (3.6) given by $x_0 = 30; y_0 = 5$. Applying Brahma Gupta lemma [1] between (x_0, y_0) and $(\tilde{x_n},\ \tilde{y_n})$ the possible sequence of non-zero distinct integer solutions to (3.6) are obtained by equation (3.3) as given below

$$x_{n+1} = \frac{1}{2}[30f_n + 5\sqrt{41}g_n],\ y_{n+1} = \frac{1}{2\sqrt{41}}[5\sqrt{41}f_n + 30g_n]. \tag{3.7}$$

The recurrence relation satisfied by the solution of (3.6) are given by the equations below

$$x_{n+2} - 4098\ x_{n+1} + x_n = 0,\ y_{n+2} - 4098\ y_{n+1} + y_n = 0. \tag{3.8}$$

Choice 3: $m = 5$

The Pell equation in focus is

$$x^2 = 41y^2 - 3125. \tag{3.9}$$

Let (x_0, y_0) be the initial solution of (3.9) given by $x_0 = 14; y_0 = 9$.

Applying Brahma Gupta lemma [1] between (x_0, y_0) and $(\tilde{x_n},\ \tilde{y_n})$ the possible sequence of non-zero distinct integer solutions to (3.9) obtained by equation (3.3) as

$$x_{n+1} = \frac{1}{2}[14f_n + 9\sqrt{41}g_n],\ y_{n+1} = \frac{1}{2\sqrt{41}}[9\sqrt{41}f_n + 14g_n]. \tag{3.10}$$

The recurrence relation satisfied by the solution of (3.9) are given by the equations below

$$x_{n+2} - 4098\ x_{n+1} + x_n = 0,\ y_{n+2} - 4098\ y_{n+1} + y_n = 0. \tag{3.11}$$

Choice 4: $m = 2k\ , k \in \mathbb{N}$

The Pell equation is

$$x^2 = 41y^2 - 5^{2k},\ k \in \mathbb{N}. \tag{3.12}$$

Let (x_0, y_0) be the initial solution of equation (3.12) given by $x_0 = 32\ (5)^k;\ y_0 = 5\ (5)^k$.

Applying Brahma Gupta lemma [1] between (x_0, y_0) and $(\tilde{x_n},\ \tilde{y_n})$ the possible sequence of non-zero distinct integer solutions to (3.12) are obtained by equation (3.3) as given below

$$x_{n+1} = \frac{5^k}{2}[32f_n + 5\sqrt{41}g_n],\ y_{n+1} = \frac{5^k}{2\sqrt{41}}[5\sqrt{41}f_n + 32g_n]. \tag{3.13}$$

The recurrence relation satisfied by the solution of (3.12) are given by the equations below

$$x_{n+2} - 4098\ x_{n+1} + x_n = 0,\ y_{n+2} - 4098\ y_{n+1} + y_n = 0. \tag{3.14}$$

Choice 5: $m = 2k + 5\ , k \in \mathbb{N}$

The Pell equation is

$$x^2 = 41y^2 - 5^{2k+5},\ k \in \mathbb{N}. \tag{3.15}$$

Let (x_0, y_0) be the initial solution of equation (3.15) given by $x_0 = 70\ (5)^{k-1};\ y_0 = 45\ (5)^{k-1}$.

Applying Brahma Gupta lemma [1] between (x_0, y_0) and $(\tilde{x_n}, \tilde{y_n})$ the sequence of non-zero distinct integer solutions to (3.15) obtained by equation (3.3) as

$$x_{n+1} = \frac{5^{k-1}}{2}[70f_n + 45\sqrt{41}g_n],\ y_{n+1} = \frac{5^{k-1}}{2\sqrt{41}}[45\sqrt{41}f_n + 70g_n]. \tag{3.16}$$

The recurrence relation satisfied by the solution of (3.15) are given by the equations below

$$x_{n+2} - 4098\ x_{n+1} + x_n = 0,\ y_{n+2} - 4098\ y_{n+1} + y_n = 0. \tag{3.17}$$

4 Conclusion

As seen and proved with the research put forth, solving a negative Pells equation that involves the Sophie Germain primes has in fact provided a more intrinsic and dynamic interpretation for finding solutions to equations satisfying occurrences of the similar nature. In due course, our research will be one of the pointers going ahead to conceptualize the effort to making/ creating a security encryption model.

Acknowledgement. We are indebted and thankful to the Editor and Referee for providing us the platform to put across our research. We value the suggestions and inputs that enabled us to fine-tune and streamline our research.

References

[1] L. E. Dickson, *History of Theory of Numbers*, Chelsea Publishing Company, New York, 1952.

[2] L. Euler, *Elements of Algebra*, Springer, New York, 1984

[3] K. Hardy and K. S. Williams, On the solvability of the Diophantine equation $dV^2 - 2eVW - dW^2 = 1$, *Pacific Journal of Mathematics*, **124** (1986), 145-158

[4] J. P. Jones, Representation of solutions of Pell equations using Lucas sequences, *Acta Academia Pead*, Ag.sectio Mathematicae, **30** (2003), 75-86

[5] J. Kannan, M. Somanath and K. Raja, Solutions of Negative Pell's Equation Involving Pierpont Primes, Consecutive Good and Proth Primes, *London Journal of Research in Science: Natural and Formal*, **22** (7) (2022), 65-74

[6] J. Kannan and M. Somanath, *Fundamental Perceptions in Contemporary Number Theory*, Nova Science Publisher, Inc, NY,11788 USA.ISBN:979-8-88697-794-3, 2023.

[7] H. W. Lenstra Jr., Solving the Pell equation, *Notice of the American Mathematical Society*, **49**, 2 (2002), 182 192.

[8] K. Matthews, The Diophantine equations $x^2 = Dy^2 - N, D > 0$, *Expositiones Math.*, **18** (2000), 363-369.

[9] L. U. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[10] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to The Theory of Numbers*, Fifth Edition, John Wiley & Sons,Inc. New York, 1991.

[11] V. Pandichelvi and S. Saranya, Detection of Relative Prime Integer Solutions for two disparateforms of Mordell curves, *Jñānābha* , **53** (1)(2023), 77-86.

[12] V. Sangeetha, M. A. Gopalan and M. Somanath, On the integer solutions of the Pell equation $x^2 = 13y^2 - 3^t$, *International Journal of Applied Mathematical Research*, **3**, (1) (2014), 58-61.

[13] A. Tekcan, B. Gezer and O. Bizin, On the integer solutions of the Pell equation $x^2 - dy^2 = 2^t$, *World Academy of Science, Engineering and Technology*, **1** (2007), 104-108.

[14] A. Tekcan, The Pell equations $x^2 - Dy^2 = \mp 4$, *Applied Mathematical Sciences*, **1** (8)(2007), 363-369.

[15] A. Titu and D. Andrica, *An introduction to Diophantine equation*, Springer Publishing House, 2002.

[16] A. Weil, *Number theory: An approach through history from Hammurapi to Legendre*, Birkahasuser Boston, 1984.