Research Journal of Mathematical and Statistical Sciences ISSN 2320–6047
Vol. **2(6),** 1-3, June **(2014)** *Res. J. Mathematical and Statistical Sci.*

On The Non Linear Indeterminate Equation $Ny^2 +m^2 =x^2$

Nidhi Handa[1] and Tarun Kumar Gupta[2]
Department of Mathematics and Statistics Gurukula Kangri University, Haridwar-249404 Uttarakhand, INDIA

Available online at: www.isca.in, www.isca.me
Received 7th April 2014, revised 12th May 2014, accepted 8th June 2014

Abstract

Let m, N∈ ℝ *be non zero. This paper deals with The Principle of Composition (Brahmagupta's Composition law) "Bhāvanā" and its some reflections of Modern Algebra using the non linear indeterminate equation* $Ny^2 + m^2 = x^2$.

Keywords: Bhāvanā, Non linear quadratic indeterminate equation.

Introduction

Suppose $N \neq 1$ be a positive non square integer and m being a fixed positive integer. Then the indeterminate equation $Ny^2 \pm m = x$ is usually called Pell's equation. This equation has an interesting history. John Pell (1611-1685) was an English mathematician and clergyman. He made no actual contributions to the history of this equation. This equation is a Diophantine equation that was named Pell's equation after a mistaken historical reference made by Leonhard Euler[1]. It is speculated that Euler actually meant to call the equation Fermat's equation [2]. Fermat was the first to propose a challenge to the mathematicians in Europe to find integer solutions for Pell's equation with certain values for N. An algorithm that gives solutions to special cases of this equation can also be linked back to Indian mathematicians Bhãskara (1114-1185) and Brahmagupta (598-670), although they provided no proof of the efficiency or sufficiency of their procedure [3].

Brahmagupta's identity and Bhāvanā

The equation $x^2 - Ny^2 = m$ was tackled by the Indian mathematician Brahmagupta (620 A.D.) in his treatise Brahma Sphuta Siddhanta Brahmagupta considered the identity [4].

$$(x^2 - Ny^2)(p^2 - Nq^2) = (xp + Nyq)^2 - N(xq + yp)^2$$
$$(x^2 - Ny^2)(p^2 - Nq^2) = (xp - Nyq)^2 - N(xq - yp)^2 \qquad (1)$$

From this two equations we see that if $x^2 - Ny^2 = 1$ and $p^2 - Nq^2 = 1$

$$(xp + Nyq)^2 - N(xq + yp)^2 = 1$$
$$(xp - Nyq)^2 - N(xq - yp)^2 = 1 \qquad (2)$$

So if (y, x) and (q, p) are solutions to Pell's equation then $(qx + py, px + Nqy)$ and $(qx - py, px - Nqy)$ are also solutions. This is important fact generalizes easily to give Brahmagupta's identity.

Brahmagupta made use of (1) in the following manner:

Suppose that there exist integers m, m' such that $x^2 - Ny^2 = m, p^2 - Nq^2 = m'$ are both solvable with $x = \alpha, y = \beta, p = \alpha', q = \beta' \text{and} \beta\beta' \neq 0.$ Then, there exists a solution of the equation

$$x^2 - Ny^2 = mm' \qquad (3)$$

In fact, $x = \alpha\alpha' \pm \beta\beta', y = \alpha\beta' \pm \alpha'\beta$ is also a solution. When $m' = m$ one has $x^2 - Ny^2 = m^2$ and it is solvable, provided $x^2 - Ny^2 = m$ is solvable. That is if $\alpha^2 - N\beta^2 = m$ we write $\lambda = \alpha^2 + N\beta^2, \mu = 2\alpha\beta.$ Then $\lambda^2 - N\mu^2 = m^2$

Theorem (Brahmagupta's Bhāvanā)

The solution space of the equation $Ny^2 + m = x^2$ admits the binary operations[5].

$$(x_1, y_{1,} m_1) \odot (x_2, y_{2,} m_2) = (x_1 y_{2,} \pm y_1 x_2 , x_1 x_{2,} \pm N y_1 y_2 , m_1 m_{2,})$$

Brahmagupta's Composition Law (Bhāvanā) with Modern Algebra

We have the indeterminate second degree equation $Ny^2 + m^2 = x^2$

Let m, N∈ ℝ *be* non zero. Let us consider X, Y∈ ℝ are such that $NY^2 + m^2 = X^2$. Equivalently $\left(\frac{X}{m}\right)^2 - N\left(\frac{Y}{m}\right)^2 = 1$. Then for all n $\left(\frac{X}{m} + \sqrt{N}\frac{Y}{m}\right)^n \left(\frac{X}{m} - \sqrt{N}\frac{Y}{m}\right)^n = 1.$

(If $N < 0$, we take $\sqrt{N} \to i\sqrt{N}$). For n= 0, 1, 2 put the explicit formulae for the solution to the equation $X^2 - NY^2 = m$ are as follows [6].

$$x_n = \frac{m}{2}\left(\left(\frac{X}{m} + \sqrt{N}\frac{Y}{m}\right)^n + \left(\frac{X}{m} - \sqrt{N}\frac{Y}{m}\right)^n\right). \qquad (4)$$

$$y_n = \frac{m}{2\sqrt{N}}\left(\left(\frac{X}{m}+\sqrt{N}\frac{Y}{m}\right)^n - \left(\frac{X}{m}-\sqrt{N}\frac{Y}{m}\right)^n\right)$$

Then

$$x_n + \sqrt{N}y_n = m\left(\frac{X}{m}+\sqrt{N}\frac{Y}{m}\right)^n \tag{5}$$

$$x_n - \sqrt{N}y_n = m\left(\frac{X}{m}-\sqrt{N}\frac{Y}{m}\right)^n$$

And

$$x_n{}^2 - Ny_n{}^2 = m^2\left(\frac{X}{m}+\sqrt{N}\frac{Y}{m}\right)^n\left(\frac{X}{m}-\sqrt{N}\frac{Y}{m}\right)^n = m^2$$

By (5) we have for (k, n≥0)

$$x_{n+k} + \sqrt{N}y_{n+k} = m\left(\frac{X}{m}+\sqrt{N}\frac{Y}{m}\right)^n\left(\frac{X}{m}+\sqrt{N}\frac{Y}{m}\right)^n$$

$$= (x_n+\sqrt{N}y_n)\left(\frac{x_k+\sqrt{N}y_k}{m}\right) \tag{6}$$

$$x_{n+k} + \sqrt{N}y_{n+k} = \frac{1}{m}\left(\left(x_nx_k+Ny_ny_k\right)+\sqrt{N}\left(x_ny_k+y_nx_k\right)\right)$$

Both $\left(x_nx_k+Ny_ny_k\right)$ and $\left(x_ny_k+y_nx_k\right)$ are inner products.

$$x_nx_k + Ny_ny_k = \begin{bmatrix} x_k \\ Ny_k \end{bmatrix}^T \begin{bmatrix} x_n \\ y_n \end{bmatrix}$$

$$x_ny_k + y_nx_k = \begin{bmatrix} y_k \\ x_k \end{bmatrix}^T \begin{bmatrix} x_n \\ y_n \end{bmatrix}$$

So $x_{n+k} + \sqrt{N}y_{n+k} = \frac{1}{m}\left\{\begin{bmatrix} x_k \\ Ny_k \end{bmatrix}^T \begin{bmatrix} x_n \\ y_n \end{bmatrix} + \sqrt{N}\begin{bmatrix} y_k \\ x_k \end{bmatrix}^T \begin{bmatrix} x_n \\ y_n \end{bmatrix}\right\}$

$$\begin{bmatrix} x_{n+k} \\ y_{n+k} \end{bmatrix} = \frac{1}{m}\begin{bmatrix} x_k & Ny_k \\ y_k & x_k \end{bmatrix}\begin{bmatrix} x_n \\ y_n \end{bmatrix} \tag{7}$$

The Determinant of $\frac{1}{m}\begin{bmatrix} x_k & Ny_k \\ y_k & x_k \end{bmatrix} = 1$, so

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \frac{1}{m}\begin{bmatrix} x_k & -Ny_k \\ -y_k & x_k \end{bmatrix}\begin{bmatrix} x_{n+k} \\ y_{n+k} \end{bmatrix}$$

Or (When $n \geq k$)

$$\begin{bmatrix} x_{n-k} \\ y_{n-k} \end{bmatrix} = \frac{1}{m}\begin{bmatrix} x_k & -Ny_k \\ -y_k & x_k \end{bmatrix}\begin{bmatrix} x_n \\ y_n \end{bmatrix} \tag{8}$$

Adding (7) and (8) we have

$$\begin{bmatrix} x_{n+k} \\ y_{n+k} \end{bmatrix} + \begin{bmatrix} x_{n-k} \\ y_{n-k} \end{bmatrix} = \frac{2x_k}{m}\begin{bmatrix} x_n \\ y_n \end{bmatrix} \tag{9}$$

In particular k=1 $\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} + \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} = \frac{2x}{m}\begin{bmatrix} x_n \\ y_n \end{bmatrix}$ (10)

Notice that we never used R is order structure,nor that R is a metric space, nor that R is uncountable and we never used that R is a field. We did use that R is a commutative ring and in (4). So we can generalize the results by considering the solutions of x^2-Ny^2=m^2 in an arbitrary commutative ring R, where m,N∈R. Now if √N∉ R then many of the steps to derive an analog of (10) in R require considering R(√N). However, we show that (10) follows from an alternate definition of x_n and y_n (which does not involve √N), in which we can also get rid of the requirements that N∈R.

$$x_n = \frac{m^{1-n}}{2}\left\{\left(X+\sqrt{N}Y\right)^n + \left(X-\sqrt{N}Y\right)^n\right\} = \frac{m^{1-n}}{2}\sum_{i=0}^{n}\binom{n}{i}X^{n-i}\left(\sqrt{N}Y\right)^i\left(1+(-1)^n\right) \tag{11}$$

$$= m^{1-n}\sum_{\substack{i=0 \\ i\,\text{even}}}^{n}\binom{n}{i}X^{n-i}N^{\frac{i}{2}}Y^i$$

$$y_n = \frac{m^{1-n}}{2\sqrt{N}}\left\{\left(X+\sqrt{N}Y\right)^n - \left(X-\sqrt{N}Y\right)^n\right\} = \frac{m^{1-n}}{2\sqrt{N}}\sum_{i=0}^{n}\binom{n}{i}X^{n-i}\left(\sqrt{N}Y\right)^i\left(1+(-1)^n\right) \tag{12}$$

$$= m^{1-n}\sum_{\substack{i=0 \\ i\,\text{odd}}}^{n}\binom{n}{i}X^{n-i}N^{\frac{i-1}{2}}Y^i$$

If necessary, we are working in R(√N). If we define x_n and y_n by (11) and (12), we get

$$m\left(\frac{X}{m}+\sqrt{N}\frac{Y}{m}\right)^n = m^{1-n}(x+\sqrt{N}y)$$

$$= m^{1-n}\sum_{i=0}^{n}\binom{n}{i}X^{n-i}N^{\frac{i}{2}}Y^i$$

$$= m^{1-n}\sum_{\substack{i=0 \\ i\,\text{even}}}^{n}\binom{n}{i}X^{n-i}N^{\frac{i}{2}}Y^i + \sqrt{N}m^{1-n}\sum_{\substack{i=0 \\ i\,\text{odd}}}^{n}\binom{n}{i}X^{n-i}N^{\frac{i-1}{2}}Y^i$$

$$= x_n + \sqrt{N}y_n$$

and similarly $x_n - \sqrt{N}y_n = m\left(\frac{X}{m}-\sqrt{N}\frac{Y}{m}\right)^n$. It follows that

$$x_{n+k} + \sqrt{N}y_{n+k} = \frac{1}{m}\left(\left(x_nx_k+Ny_ny_k\right)+\sqrt{N}\left(x_ny_k+y_nx_k\right)\right) \tag{13}$$

From which we can drive (10).Indeed defining x_n and y_n by (11) and (12) gives us that x_n, y_n ∈ R regarding of √N∈R

Groups of the form $\left\{(x,y): Ny^2+m^2=x^2\right\}$

The Group {(x_n,y_n) : n∈ℤ }Let m, N∈ ℝ and let X,Y∈ ℝ be such that $NY^2+m^2=X^2$

Put G= {(x_n ,y_n) : n∈ℤ } where x_n and y_n are as in (11) (12) and define an operation ⊙ on G by Brahmagupta's Composition law (Bhāvanā)

$$(x_k, y_k)\odot(x_l, y_l) = \left(\frac{x_k x_l + N y_k y_l}{m}, \frac{x_k y_l + y_k x_l}{m}\right) \qquad (14)$$

By (13) we see that (x_{k+l}, y_{k+l}) **

Claim: (G, ⊙) is an abelian group, with identity (x_0, y_0).

Proof: Indeed, for j,k,l ∈ ℤ

$$\begin{aligned}(x_k, y_k)\odot(x_l, y_l) &= (x_{k+l}, y_{k+l}) = (x_{l+k}, y_{l+k})\\ &= (x_l, y_l)\odot(x_k, y_k)\\ (x_0, y_0)\odot(x_k, y_k) &= (x_k, y_k)\odot(x_0, y_0) = (x_{k+0}, y_{k+0})\\ &= (x_k, y_k)\\ (x_k, y_k)\odot(x_{-k}, y_{-k}) &= (x_{k-k}, y_{k-k}) = (x_0, y_0)\end{aligned}$$

$$\begin{aligned}(x_j, y_j)\odot(x_k, y_k)\odot(x_l, y_l) &= (x_{j+k}, y_{j+k})\odot(x_l, y_l)\\ &= (x_{j+k+l}, y_{j+k+l})\\ &= (x_j, y_j)\odot(x_{k+l}, y_{k+l})\\ &= (x_j, y_j)\odot(x_k, y_k)\odot(x_l, y_l)\end{aligned}$$

Definition 3.2 Let R be a commutative ring with identity[7,8] and let m,N ϵ ℝ. Let

$\mathcal{L}_{R=}$ $\{(x, y) \in \mathbb{R}\times\mathbb{R}: Ny^2+m^2=x^2\}$

When R is understood from the context, $\mathcal{L}$ will denote $\mathcal{L}_R$

Definition 3.3 If m is invertible, define an operation ⊙ on $\mathcal{L}$ by Brahmagupta's Composition law (Bhāvanā)

$$(x, y)\odot(x, y) = \{m^{-1}(xx' + Nyy'), m^{-1}(xy' + x'y)\}$$

Claim ($\mathcal{L}_R$, ⊙) is an Abelian group with identity $(m, 0)$

Proof: $\mathcal{L}_R$ is non empty. It contains both (m,0) and (-m,0). Since R is commutative, $xx' + Nyy' = x'x + Nyy'$

(and since R is a ring, $xy' + x'y = x'y + xy'$).

Then $(m, 0)\odot(x, y) = (x, y)\odot(m, 0)$ which is

$$\{m^{-1}(xm), m^{-1}(my)\} = (x, y)$$

If (x,y) ϵ $\mathcal{L}$, then also (x,-y) ϵ $\mathcal{L}$ (since $x^2 - N(-y)^2 = x^2 - Ny^2$) and $(x, y)\odot(x, -y) = \{m^{-1}(x^2 - Ny^2), m^{-1}.0\} = (m, 0)$.

To see that ⊙ is an associative binary operation on $\mathcal{L}$, first notice that each $(x, y) \in \mathcal{L}$ corresponds to unique matrix in $R^{2\times2}$ whose determinants is $m^2\left\{\text{namely,} \begin{bmatrix} x & Ny \\ y & x \end{bmatrix}\right\}$.

Also notice that left multiplication in $\mathcal{L}$ corresponds to left multiplication in $R^{2\times2}$ by the matrix

$$\begin{bmatrix} m^{-1}x & m^{-1}Ny \\ m^{-1}y & m^{-1}x \end{bmatrix} = m^{-1}\begin{bmatrix} x & Ny \\ y & x \end{bmatrix}$$

Suppose $(x, y), (x', y'), (x'', y'') \in \mathcal{L}$

Then $m^{-1}\begin{bmatrix} x & Ny \\ y & x \end{bmatrix}\begin{bmatrix} x' & Ny' \\ y' & x' \end{bmatrix}$ has

Determinant $m^2\{(x, y)\odot(x', y') \in \mathcal{L}\}$ and

$$m^{-1}\left(m^{-1}\begin{bmatrix} x & Ny \\ y & x \end{bmatrix}\begin{bmatrix} x' & Ny' \\ y' & x' \end{bmatrix}\right)\begin{bmatrix} x'' & Ny'' \\ y'' & x'' \end{bmatrix} =$$

$$m^{-1}\begin{bmatrix} x & Ny \\ y & x \end{bmatrix}\left(m^{-1}\begin{bmatrix} x' & Ny' \\ y' & x' \end{bmatrix}\begin{bmatrix} x'' & Ny'' \\ y'' & x'' \end{bmatrix}\right) \text{ So}$$

$$\{(x, y)\odot(x', y')\}\odot(x'', y'') = (x, y)\odot\{(x', y')\odot(x'', y'')\}$$

** When √N∉ R, {1, √N} is L.I over R so we can equate the like terms in (2.10). However, when √N∈R, we can show that $(x_{n+1}, y_{n+1}) = (x_n, y_n)\odot(x_1, y_1)$. Then by induction we have$(x_{k+l}, y_{k+l}) = (x_k, y_k)\odot(x_l, y_l)$.

Conclusion

The achievements on Pell's equation tend to overshadow the fact that, at least from the time of Brahmagupta, Indian algebraists had produced a large bulk of work involving ingenious solutions of various types of indeterminate equations. The study of indeterminate equations, especially the study of the equation $Ny^2+1=x^2$ played an important role in the evolution of classical Algebra in ancient India as well as in Modern Europe.

Indeed, Brahmagupta's composition law is of paramount significance in Group theory and Ring theory. Brahmagupta's composition law is the first known instance of an involved abstract algebraic thinking. Its pedagogic value stems from the fact that it is a self contained gem.

References

1. Lenstra H.W., Solving the Pell Equation, notices AMS, **49(2),** 182-192 **(2002)**
2. Murthy N.R. and M.N.S. Swamy, Cryptographic Applications of Brahmagupta-Bhãskara equation, IEEE Trans. Circuits Syst. I, *Reg. Papers,* **53(7), (2006)**
3. Gupta T.K. and Nidhi Handa, Computer Applications of Brahmagupta-Bhãskara equation, *New York (U.S.A) International Journal of Computer Applications (IJCA),* **ISSN-0975-8887**, **(2013)**
4. Dutta B. and Singh A.N., History of Hindu Mathematics, Part II, Asia publishing House **(1962)**
5. Emch G.G., Sridharan R. and Srinivas M.D. (ed), Contributions to the History of Indian Mathematics, CHOM 3, H.B.A, 77-114 **(2005)**
6. Lam. Katie, Pell's Equation, Parabola, **38(2), (2002)**
7. Fraleigh J.B., A first course in Abstract Algebra Pearson Education **(2004)**
8. Gallian J.A., Contemporary Abstract Algebra, 2nd Ed. Lexington, Mass: D.C. Heath,**(1990)**