**International Journal of Pure and Applied Mathematics**
**Volume 18 No. 4 2005, 441-444**

# DEFINING A GROUP OPERATION ON THE SET OF SOLUTIONS OF A PARAMETRISED QUADRATIC DIOPHANTINE EQUATION

Kenneth K. Nwabueze[1] §, Omar Kihel[2], Ajai Choudhry[3]

[1]Department of Mathematics
University of Brunei
Jaban Tinguka Link
Bander Seno Bgawan, Darussalam, BE 1210, BRUNEI

[2]Department of Mathematics
Brock University
St. Catharines, Ontario, L2S 3A1, CANADA
e-mail: okihel@brocku.ca

[3]High Commission of India
P.O. Box 439, M.P.C., Airport Lama
Berakas, BB 3577, BRUNEI
e-mail: ajaic203@yahoo.com

**Abstract:** Using basic elementary geometric ideas, a binary operation defining an algebraic group induced by the set of all integral solutions to the diophantine equation of the form $ax^2 + by^2 = az^2$ is exhibited.

**AMS Subject Classification:** 11D09, 20D15
**Key Words:** diophantine equation, group, elementary geometry

*

Consider the diophantine equation

$$ax^2 + by^2 \;=\; az^2\,, \tag{1}$$

where $a$ and $b$ are integers not equal to zero. Let

Received: November 29, 2004 

§Correspondence author

$$F = \{[x, y, z] \mid x, y, z \in \mathbf{Z}, \text{ and } x, y, z \text{ not all zero}\}$$

denotes the set of solutions to equation (1). It is easy to see that if $[x, y, z] \in F$, then for any rational number $\lambda \neq 0$ the triple $[\lambda x, \lambda y, \lambda z] \in F$ [see (2)].

Define an equivalence relation on $F$ by stipulating that $[x, y, z] \sim [\lambda x, \lambda y, \lambda z]$, for all nonzero rational number $\lambda$. The equivalence class of the triple $[x, y, z]$ in $F/\sim$ is typically written as $[x : y : z]$, in order to avoid confusion with the triple $[x, y, z]$.

The aim of this note is to define a group operation on $F/\sim$ using elementary geometric method.

Now from equation (1) we get the conic

$$X^2 + (\frac{b}{a})Y^2 \ = \ 1, \tag{2}$$

where $X = \frac{x}{z}$ and $Y = \frac{y}{z}$, are rational numbers and $z \neq 0$. Equation (2) is an ellipse if $\frac{b}{a} > 0$, and a hyperbola if if $\frac{b}{a} < 0$.

Let $\mathbf{N}\left(X \ + \ \sqrt{-\frac{b}{a}}\, Y\right)$ denotes the norm of $\left(X \ + \ \sqrt{-\frac{b}{a}}\, Y\right)$; that is

$$\mathbf{N}\left(X \ + \ \sqrt{-\frac{b}{a}}\, Y\right) = \left(X \ + \ \sqrt{-\frac{b}{a}}\, Y\right)\left(X \ - \ \sqrt{-\frac{b}{a}}\, Y\right) \ = \ X^2 + \frac{b}{a}Y^2. \tag{3}$$

So the set of all rational points on the conic (2) is clearly in one to one correspondence with numbers of the form $\left(X \ + \ \sqrt{-\frac{b}{a}}\, Y\right)$ of norm equal to 1 in the field $\mathbf{Q}\left(\sqrt{-\frac{b}{a}}\right)$.

Furthermore, for any two elements

$$\left(X_1 + \sqrt{-\frac{b}{a}}Y_1\right) \text{ and } \left(X_2 + \sqrt{-\frac{b}{a}}Y_2\right)$$

in the multiplicative group $\mathbf{Q}\left(\sqrt{-\frac{b}{a}}\right)^*$ of the field $\mathbf{Q}\left(\sqrt{-\frac{b}{a}}\right)$ we have

$$\left(X_1+\sqrt{-\frac{b}{a}}Y_1\right)\left(X_2+\sqrt{-\frac{b}{a}}Y_2\right) = X_1X_2-\frac{b}{a}Y_1Y_2+\sqrt{-\frac{b}{a}}\left(X_1Y_2+X_2Y_1\right). \quad (4)$$

Equating the norm of the right hand side of (4) to 1 yields

$$a\left(aX_1X_2-bY_1Y_2\right)^2+b\left(aX_1Y_2+aX_2Y_1\right)^2=a^3. \quad (5)$$

Substituting

$$X_1=\frac{x_1}{z_1}, \quad X_2=\frac{x_2}{z_2}, \quad Y_1=\frac{y_1}{z_1}, \quad Y_2=\frac{y_2}{z_2}$$

in equation (5) produces

$$a\left(ax_1x_2 - by_1y_2\right)^2+b\left(ax_1y_2 + ax_2y_1\right)^2=a\left(az_1z_2\right)^2. \quad (6)$$

Now by comparing equations (1) and (6), we get

$$x=ax_1x_2 - by_1y_2, \quad y=ax_1y_2 + ax_2y_1 \text{ and } z=az_1z_2. \quad (7)$$

Equations (7) are a defining set of binary operation which makes the set of all integral solutions (excluding the trivial solution $[0,0,0]$) of equation (1) a group. More precisely, under the operation in equation (7), the set of integral primitive solutions of the equation

$$ax^2+by^2=cz^2$$

forms a group. It is routine to check that the binary operation is well defined, closed, associative and commutative; the identity element is the class $[x,\ 0,\ x]$, the inverse of any triple $[x,\ y,\ z]$ is $[x,\ -y,\ z]$.

Observe that in a particular case where $a=b=1$, in equation (1), the operation defined in equation (7) and the operation for the Pythagorean group (see [1]) coincides.

## References

[1] A. Choudhry, K.K. Nwabueze, An example of a group, *International Journal of Pure and Applied Mathematics,* **15**, No. 3 (2004), 397-400.

[2] K.K. Nwabueze, *Lectures in the Theory of Numbers*, Second Edition, Education Technology Centre, University of Brunei Darussalam (2002).