IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 12, Issue 5 Ver. I (Sep. - Oct.2016), PP 82-91
www.iosrjournals.org

Diophantine Equation Of The Form $x^2 - Dy^2 = 2z^2$

Nur Asyikin Hamdan, Abdul Latif Samian, Nazri Muslim
Malay World and Civilization (ATMA) National University of Malaysia

Abstract: *The purpose of this study is to investigate the solution of Diophantine equation. This study will be complete if we know more about the prime numbers of Mersenne. Besides that, this paper will discuss about Diophantine equation. It is about experiment with numbers and to discover patterns. Number theory plays an important role in the Diophantine equation. In this study, we consider Diophantine equation of the form:*

$$x^2 - Dy^2 = 2z^2$$

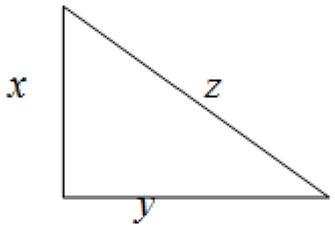
for any odd number D that is prime number. Using congruent method, this Diophantine equation could be solved.

Keywords: *Diophantine, prime numbers, patterns, numbers, odd number*

I. The History Of Diophantine Equation

According to Le Veque (1969), he defined Diophantine equation as the equation with one or more variables that have the power of one, two, and so on. If the equation has a variable with the highest power of one, two or three, then each equation is known as linear, quadratic or cubic Diophantine equation.

The common example is Pythagorean Theorem. It can help to understand this Diophantine equation. Pythagorean Theorem states that for any right-angled triangle, the square of the two longest sides is equal to the sum of the squares of the other two sides. The longest side is called the hypotenuse. Pythagorean Theorem equation is $x^2 + y^2 = z^2$, where x, y and z are the variables and this equation is called as quadratic Diophantine equation. Equation $x^2 + y^2 = z^2$ can be described as in the figure below:



Solutions for Diophantine equation must be in integer or ratio. For this example, two of the solutions are $(x, y, z) = (3,4,5)$ and $(x, y, z) = (5,12,13)$. Other solutions can be found through simple formula as follow:

$$x^2 = a^2 - b^2$$
$$y = 2ab \qquad , \quad a \text{ and } b \text{ are any integer}$$
$$z = a^2 + b^2$$

For example, to obtain solution (3, 4, 5), consider $a = 2$ and $b = 1$, so $3^2 + 4^2 = 5^2$.

Babylonians used the Pythagorean equation to build trigonometry draft schedule. With the structure of this draft schedule, Pythagorean equation will be emphasized. Level one equation $ax + by = c$ has appeared in Greek, Arabic and in Chinese word puzzles. However, the theory needed to solve equation $ax + by = c$ has been found in Eleven Euclid. Equation $ax + by = c$ is still regarded as Diophantine equation although it is not recorded in Diophantus writing as he might underestimate it.

The work of Diophantus was not known by public in Europe during the Middle Ages. However, the work has been discovered and translated twice in the 16th and 17th Century. One of the second translation copies by Bachet has reached Fermat, a mathematician who was determined to understand it in depth and attempted to continue the work of Diophantus. Fermat's efforts might be described as a turning point for the discovery of modern number theory. In most of Fermat's decision, he stated that the equation $x^4 + y^4 = z^4$ has no non-zero integer solution. He provided a detailed analysis of the problem by showing integer as a sum of squares of two numbers and demanded to prove each positive integer is the sum of the squares of four numbers. However, he was unable to prove it.

After 250 years later, mathematicians such as Euler, Lagrange, Gauss and Kummer continued the work of Fermat. Their results were limited to either the quadratic equation known as Pell equation $x^2 - d^2 = c$, or Fermat equation $x^n + y^n = z^n$ .Kummer showed that equation $x^n + y^n = z^n$ has no non-zero integer solution if n is less than 100.

Fermat's Theorem $x^n + y^n = z^n$, which has been stated previously has no integer solution if n is integer greater than or equal to three, also an example of Diophantine equation with three variables, x, y and z . Equation $y^2 = x^3 + 3x^2 + 3x + 1$ is also a Diophantine equation with two variables, x and y . This equation is called as cubic Diophantine equation because the highest power of the variable is three. There are many examples of Diophantine equation. This equation can be written in the form of regular equation or polynomial equation.

For $x^n + y^n = z^n$, where $n = 2$, it has many solutions (x, y, z). For greater n value, Fermat's Last Theorem states that there is no solution for the positive integer numbers (x, y, z) that satisfy this equation.

Next, we will discuss quadratic equation of the form $x^2 - Dy^2 = 2z^2$, with condition $(xyz \neq 0)$ provided in the next chapter.

II. Diophantine Equation

Mersenne Prime Number

Mersenne prime number is a prime number written in the form of $a^n - 1$ with condition $n \geq 2$. For example, 31 is a prime number, $31 = 2^5 - 1$. See the table below:

Table 2.1 Example for $a^n - 1$ when $n \geq 2$

$2^2 - 1 = 3$	$2^3 - 1 = 7$	$2^4 - 1 = 3.5$	$2^5 - 1 = 31$
$3^2 - 1 = 2^3$	$3^3 - 1 = 2.13$	$3^4 - 1 = 2^4.5$	$3^5 - 1 = 2.11^2$
$4^2 - 1 = 3.5$	$4^3 - 1 = 3^2.7$	$4^4 - 1 = 3.4.17$	$4^5 - 1 = 3.11.31$
$5^2 - 1 = 2^3.3$	$5^3 - 1 = 2^2.31$	$5^4 - 1 = 2^4.3.13$	$5^5 - 1 = 2^2.11.71$
$6^2 - 1 = 5.7$	$6^3 - 1 = 5.43$	$6^4 - 1 = 5.7.37$	$6^5 - 1 = 5^2.311$
$7^2 - 1 = 2^4.3$	$7^3 - 1 = 2.3^2.19$	$7^4 - 1 = 2^5.3.5^2$	$7^5 - 1 = 2.3.2801$
$8^2 - 1 = 3^2.7$	$8^3 - 1 = 7.73$	$8^4 - 1 = 3^2.5.7.13$	$8^5 - 1 = 7.31.151$

Source: Joseph H. Silverman, 1997.

A simple observation can be seen easily from the table above which is, if a is an odd number, then $a^n - 1$ is the even number. Based on the table above, if a is an odd number, $a^n - 1$ can be divided by $a - 1$. This observation is very accurate because the statement can be proven by using the formula for geometric series. For example:

$$
\begin{aligned}
&= (x-1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1), \\
&= x.(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1) - 1.(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1), \\
&= (x^n + x^{n+1} + \ldots + x^3 + x^2 + x) - (x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1), \\
&= x^n - 1
\end{aligned}
$$

Based on this geometric formula, assume that $x = a$, $a^n - 1$ can always be divided by $a - 1$. So, $a^n - 1$ can represent many values besides $a - 1 = 1$, that is $a = 2$. However, if $a = 2$, formula $2^n - 1$ is satisfied. This is shown by the table below:

Table 2.2 Mersenne Prime Number

n	2	3	4	5	6	7	8	9	10
$2^n - 1$	3	7	3.5	31	$3^2.7$	127	3.5.17	7.73	3.11.31

Source: Joseph H. Silverman, 1997.

Although this table shows only a few values, but it can be explained that
When n is an even number, 2^n-1 can be divided by 3=2^2-1,
When n can be divided by 3, 2^n-1 can be divided by 7=2^3-1,
When n can be divided by 5, 2^n-1 can be divided by 31=2^5-1,

So, it can be concluded that if n can be divided by m, then 2^n-1 can be divided by 2^m-1. From the observation, it is clear that this statement is true. Consider $n=mk$, then $2^n=2^{mk}=(2^m)^k$. Geometric series formula with $x=2^k$ will be used to obtain

$$2^n-1=(2^m)^k=(2^m-1)\left((2^m)^{k-1}+(2^m)^{k-2}+...+(2^m)^2+(2^m)+1\right),$$

This suggests that, if n is a plural number, then 2^n-1 is also a plural number. Plural numbers are numbers other than prime numbers. This can be explained by the facts below.

Facts

If a^n-1 is prime number for some numbers with $a\geq 2$ and $n\geq 2$, then $a=2$ and n must be prime numbers. This means that the prime number is in the form of a^n-1 so, it is necessary to consider the case $a=2$ and n must be prime numbers. Prime numbers are in the form of

2^p-1 is known as Mersenne Prime Number
Among Mersenne Prime Numbers are
$2^2-1=3$, $2^3-1=7$, $2^5-1=31$, $2^7-1=127$, $2^{13}-1=8191$,
Not all numbers are prime numbers. Among them are:
$2^{11}-1=2047=23.89$, $2^{29}-1=536870911=233.1101.2089$,
Mersenne Prime Numbers are named according to the name of Father Marin Mersenne (1588-1648). In 1944, he claimed that 2^p-1 is prime number for the following numbers:
p =2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

The numbers above are prime numbers less than 258 that satisfy the formula 2^p-1 in order to become prime number. However, it is unknown how Father Marine Mersenne discovered that fact, especially after he stated that his previous research was not true. Finally, he submitted complete prime numbers p less than 10,000 which satisfied the formula 2^p-1 which is

p =2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,
3217, 4253, 4423, 9689, 9941

III. Quadratic Diophantine Equation System

Various results are obtained from the equation when functions $f_1(x,y)$ and $f_2(x,y)$ are quadratic polynomial. This fact was stated by Barnes (1953), Goldberg (1954) and Mills (1954). There are infinite numbers of trivial solutions of the equation. Apart from that, there are only infinite values possible for z. For example, quadratic equation with x and y values are either infinity or can be obtained from the Pell Equation or equivalent alkhawarizmi recursive.

The equation $x^2+y^2+x+y+1=xyz$ is equivalent to $x\,|\,y^2+1$ and $y\,|\,x^2+1$ which has a positive integer solution $(x,y)=(u_n,u_{n+1})$, when u is of a sequence of ..., 13, 5, 2, 1, 2, 5, 13, ... where $z=3$. This sequence also has an alternate form of a Fibonacci sequence 1, 1, 2, 3, 5, 8, 13,...

Equation $x^2+y^2+x+y+1=xyz$, with $x>0$ and $y>0$, has solution (x,y), two consecutive terms of the sequence 1, 1, 3, 15, ..., with $u_n=5u_{n+1}-u_{n-2}-1$. equation $x^2+y^2+x+y+1=xyz$, with $x>0$ and $y>0$ only has solution if $x=y=1$. Mordell (1969) showed that equation $ax^2+by^2+c=xyz$, where a,b and c are integers, has infinite solutions for any $x=y=1$. This solution can be provided in the form of polynomial in a,b and c. In this study, all integer solutions for the equation $x^2 - Dy^2 = 2z^2$ will be obtained.

The Solution Of Diophantine Equation Of The Form $x^2 - Dy^2 = 2z^2$

Next will be discussed on Diophantine equation of the form (Edward L. Cohen, 1982)

$$x^2 - Qy^2 = 2z^2 \ (xyz \neq 0), \qquad \textbf{(1)}$$

where Q is Mersenne prime number as described above. Prime numbers are any number of the form $Q = 2^p - 1$. In this case, p is a prime number. All Mersenne prime numbers are in the form of $Q = 2r^2 - 1$ except $Q = 3$. Our objective is to solve all general Diophantine equation solutions of the form

$$x^2 - Dy^2 = 2z^2 \ (xyz \neq 0), \qquad \textbf{(2)}$$

where D is a prime number of the form $D = 2r^2 - 1$. Therefore, for the next solution, we consider all prime numbers except number 3. The method used to find the solution is by changing equation (2) to a parametric form so that the equation obtained is much simpler. The equation is in the form of $ax^2 + by^2 + cz^2 = 0$.

For each integer number D obtained through $2r^2 - 1$, note that $x = 2r + 1,\ y = 1,\ z = r + 1$ are solutions to (2). Thus, we obtain the same identity equation which is $(2r+1)^2 - (2r^2 - 1) = 2(r+1)^2$. Parametric solution is obtained by assuming (x, y, z) as integer solutions for equation (2). The value of $xyz \neq 0$. From equation (2), we get that

$$\left(x + (2r+1)y\right)\left(x - (2r+1)y\right) = 2\left(z + (r+1)y\right)\left(z - (r+1)y\right),$$

If summarized, the result obtained is $x^2 - (2r^2 - 1)y^2 = 2z^2$. Hence, the solutions are as below,

$$x - (2r+1)y = \frac{2\left(z - (r+1)\right)\left(z + (r+1)\right)}{x + (2r+1)}, \quad K = \frac{2\left(z - (r+1)\right)}{x + (2r+1)},$$
$$x - (2r+1)y = K\left(z + (r+1)\right),$$
$$K\left(x + (2r+1)\right) = 2\left(z - (r+1)\right),$$

So,

$$x - (2r+1)y = K\left(z + (r+1)y\right) \text{ and } K\left(x + (2r+1)y\right) = 2\left(z - (r+1)y\right),$$

K is constant

$$K = \frac{x - (2r+1)y}{z + (r+1)y},$$
$$K = \frac{z - (r+1)y}{x + (2r+1)y},$$

The initial solutions obtained are

$$x - \left((2r+1) + K(r+1)\right)y - Kz = 0, \qquad \textbf{(i)}$$
$$Kx + \left(K(2r+1) + 2(r+1)\right)y - 2z = 0, \qquad \textbf{(ii)}$$

Solving equations (i) and (ii) by removing z

=> $2\left(x-\left((2r+1)+K(r+1)\right)y-Kz=0\right)$,

$K\left(Kx+\left(K(2r+1)+2(r+1)\right)y-2z=0\right)$,

=> $2x-\left((2r+1)+K(r+1)\right)2y-2Kz = 0$,

$K^2x+\left((2r+1)+2(r+1)\right)Ky-2Kz=0$,

=> $(2-K^2)x-[\left((2r+1)+K(r+1)\right)2y+\left(K(2r+1)+2(r+1)Ky\right)]=0$,

=> $(2-K^2)x-[\left((2r+1)+2K(r+1)\right)+\left(K^2(2r+1)+2K(r+1)\right)]y=0$,

=> $(2-K^2)x=[2(2r+1)+4K(r+1)+K^2(2r+1)]y$,

=> $\dfrac{x}{2(2r+1)+4K(r+1)+K^2(2r+1)}=\dfrac{y}{2-K^2}$,

Next, getting the value of z by eliminating x

=> $K\left(x-\left((2r+1)+K(r+1)\right)y-Kz=0\right)$, **(iii)**

$Kx+\left(K(2r+1)+2(r+1)\right)y-2z=0$, **(iv)**

=> $Kx-\left((2r+1)+K(r+1)\right)Ky-K^2z=0$,

$Kx+\left(K(2r+1)+2(r+1)\right)y-2z=0$,

=> $-[\left((2r+1)K+K^2(r+1)\right)+K(2r+1)+2(r+1)]y+\left((-K^2+2)z\right)=0$,

=> $-[2K(2r+1)+K^2(r+1)+2(r+1)]y+\left(2-K^2\right)z$,

=> $[2K(2r+1)+K^2(r+1)+2(r+1)]y=\left(2-K^2\right)z$,

=> $\dfrac{z}{2K(2r+1)+K^2(r+1)+2(r+1)}=\dfrac{y}{2-K^2}$,

Consider $K=\dfrac{s}{t}$, the greatest common factor (FSTB) for $(s,t)=1, t>0$

=> $\dfrac{x}{(2r+1)\left(\dfrac{s}{t}\right)^2+4(r+1)\dfrac{s}{t}+2(2r+1)} = \dfrac{y}{2-\left(\dfrac{s}{t}\right)^2} = \dfrac{z}{(r+1)\left(\dfrac{s}{t}\right)^2+2(2r+1)\dfrac{s}{t}+2(r+1)}$,

=> $\dfrac{xt^2}{(2r+1)s^2+4st(r+1)+2t^2(2r+1)}=\dfrac{yt^2}{2t^2-s^2}=\dfrac{zt^2}{(r+1)s^2+2st(r+1)+2t^2(r+1)}$,

$\dfrac{x}{e}=\dfrac{y}{f}=\dfrac{z}{g}$ forms obtained are

$$\left.\begin{aligned}
&e=(2r+1)s^2+4st(r+1)+2t^2(2r+1),\\
&f=2t^2-s^2,\\
&g=(r+1)s^2+2st(r+1)+2t^2(r+1)\text{ (FSTB)},
\end{aligned}\right\}\qquad \textbf{(3)}$$

the greatest common factor of *d* for the denominator e, f, g are divided until

$(2r+1)e-2(r+1)g$, which are $(2r^2-1)(s^2+2t^2)$,

Note also *d* divides $f=2t^2-s^2$, and FSTB $(s^2+2t^2,2t^2-s^2)=1$ or 2. Therefore, it satisfies that *d* can divide $2(2r^2-1)=2D$. So, d = 1, 2, D or 2D. The new equation will be obtained, which is

$$\left.\begin{aligned} x&=\frac{c}{d}\left((2r+1)s^2+4(r+1)st+2(2r=1)t^2\right),\\ y&=\frac{c}{d}(2t^2-s^2),\\ z&=\frac{c}{d}\left((r+1)s^2+2(2r+1)st+2(r+1)t^2\right),\end{aligned}\right\} \quad \textbf{(4)}$$

where c is an integer. Next, values required will be obtained through equation (4), by taking into account $K=\frac{s}{t}$, where $t>0$. The values (x,y,z) are the solution for equation (2). Therefore, equation (2) is equivalent to equation (4).

Note the following:
1. When *s* is an odd number, then FSTB (e,f,g) = 1 or D
2. When s is an even number, then FSTB (e,f,g) = 2 or $2D$

if it is odd, it can be concluded that H = D. similarly, if it is even, then, H= $2D$.

Theorem 1: H = $FSTB(e,f,g)$ if and only if $s\equiv -2rt(\bmod D)$

Proven by equation (3)

$$\begin{aligned} (2r+1)s^2+4st(r+1)+2t^2(2r+1)&\equiv 0(\bmod D),\\ 2t^2-s^2 \quad &\equiv 0(\bmod D),\end{aligned} \quad \textbf{(5)}$$

So, to solving these two equations are through deleting method

$$2(2r+1)s^2+4(r+1)st+2t^2(2r+1)\equiv 0(\bmod D), \quad \textbf{(i)}$$
$$-(2r+1)s^2-2t^2(2r+1)\equiv 0(\bmod D), \quad \textbf{(ii)}$$

The following equations are obtained

$$\begin{aligned} &(2r+1)s^2+2(r+1)st\equiv 0(\bmod D),\\ &(2r+1)s+2(r+1)t\equiv 0(\bmod D),\end{aligned} \quad \textbf{(6)}$$

Multiply equation (6) with $(2r-1)$ will produce $s+2rt\equiv 0(\bmod D)$. To prove this statement is true, then it must show that equation (5) and (6) are satisfied. Generally, it is known $(2r+1)(2r-1)\equiv 0(\bmod D)$, so, equation (5) is satisfied when $s+2rt$ is multiply by $2r+1$. For equation (6), when $s+2rt\equiv 0(\bmod D)$, it shows that $s^2\equiv 4r^2t^2(\bmod D)$. Finally, since $4r^2-2\equiv 0(\bmod D)$, then $s^2\equiv 2t^2(\bmod D)$.

Corollary: H = $FSTB(e,f,g)$, if and only if $t\equiv -rs(\bmod D)$.

Theorem 2

For equations that have specific solutions, there are many infinite solutions. Each solution (x,y,z) of equation (4) is obtained from four ratio numbers, $K=\frac{s}{t}$ which is the highest common factor (FSTB).

Theorem 3

$$\underset{s\to\infty}{had}\frac{x}{z}=\underset{t\to\infty}{had}\frac{x}{z}=\frac{2r+1}{r+1},$$

Theorem 4
When $D=7(r=2)$, the priority of this solution are $x=2r+1, y=1, z=r+1$, that have been mentioned earlier. It is also equal to FSTB for four numbers that are 1, 2, 7, 14. Note the table below:

Table 2.3 Example of FSTB when $D=7(r=2)$

FSTB	S	T
1	1	0
2	0	1
7	-5	3
14	-6	5

Source: Edward L. Cohen, 1982.

It has been stated that $t\neq 0$, so we definitely will not use equation (3) and (4).

The Similarities Of Linear Diophantine, Linear Congruent And Matrix

THEOREM 1
Consider that r_n is the last divider in Eukledean alkhawarizmi for the purpose of finding FSTB for two positive integers which are $a=r_1$ and $b=r_0$ where $a\geq b>0$. Consider that $Q_i=\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$, and $Q=\prod_{i=0}^{n}Q_i$, where $r_{i-1}=q_ir_i+r_{i+1}$, for $0\leq i\leq n$. So, $\begin{pmatrix} a \\ b \end{pmatrix}=Q\begin{pmatrix} r_n \\ 0 \end{pmatrix}$, then $\begin{pmatrix} r_n \\ 0 \end{pmatrix}=Q^{-1}\begin{pmatrix} a \\ b \end{pmatrix}$. So, $Q^{-1}=\begin{pmatrix} \alpha & \beta \\ \gamma & \sigma \end{pmatrix}$ and $\begin{pmatrix} \alpha & \beta \\ \gamma & \sigma \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} r_n \\ 0 \end{pmatrix}$, then, $r_n=\alpha a+\beta b$. Next, $r_n|c$, $c=kr_n$, for all k constant. So, $c=(\alpha k)a+(\beta k)b$, then, $x_0=\alpha k$ and $y_0=\beta k$ are specific solutions for this linear Diophantine equation (T. Koshy, 1996).

THEOREM 2

Consider $r_{i-1}=q_ir_i+r_{i+1}$, for $0\leq i\leq n$ in the Eukledean algorithm to get FSTB (a,b), where $a\geq b$. Consider $Q_i=\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$, and $Q=\prod_{i=0}^{n}Qi$. Then, (T. Koshy. 1996)

$$Qi=\begin{pmatrix} \alpha & \beta \\ \frac{(-1)^n b}{r_n} & \frac{(-1)^{n+1}a}{r_n} \end{pmatrix},$$

Verification
Generally, it has been identified that the top row of Q_i are $[\alpha,\beta]$, so we just have to focus on the second line of Q_i. This can be proven by using induction method *n,* which includes equation $n+1$ (T. Koshy, 1996).

$$a=q_0r_0+r_1, \qquad 0\leq r_1<r_0$$
$$r_0=q_1r_1+r_2, \qquad 0\leq r_2<r_1$$
$$.$$

$$\begin{aligned} &\vdots \\ &r_{n-2} = q_{n-1}r_{n-1} + r_n, \qquad 0 \le r_n < r_{n-1} \\ &r_{n-1} = q_n r_n + 0 \end{aligned}$$

When $n = 0$, this alkhawarizmi has the equation of $a = q_0 r_0 + 0$ where $r_0 = b$. Therefore, $Q = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}$, and $Q^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ \frac{b}{r_0} & \frac{-a}{r_0} \end{pmatrix}$. So, the solution is true when $n = 0$.

Now, suppose that the solution of the equation is satisfied for $k \ge 0$. Take the value of $n = k+1$. Then, alkhawarizmi involves equation $k+2$. Put it on top of the equation. Then, equation $k+1$. These equations will form alkhawarizmi to find FSTB (r_0, r_1).

Consider $Q' = \prod_{i=0}^{k} Q_i'$, when $Q_i' = Q_{i+1}$. By using hypothesis $(Q')^{-1} = \begin{pmatrix} ? & ? \\ (-1)^k \frac{r_1}{r_{k+1}} & (-1)^{k+1} \frac{r_0}{r_{k+1}} \end{pmatrix}$, where '?' states that the solution for the top of the matrix is not involved.

So,

$$\begin{aligned} Q^{-1} = (Q')^{-1} &= \begin{pmatrix} ? & ? \\ (-1)^k \frac{r_1}{r_{k+1}} & (-1)^{k+1} \frac{r_0}{r_{k+1}} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_0 \end{pmatrix}, \\ &= \begin{pmatrix} ? & ? \\ (-1)^{k+1} \frac{r_1}{r_{k+1}} & (-1)^{k+2} \frac{r_{(1+q_0 r_0)}}{r_{k+1}} \end{pmatrix}, \\ &= \begin{pmatrix} ? & ? \\ (-1)^{k+1} \frac{b}{r_{k+1}} & (-1)^{k+2} \frac{a}{r_{k+1}} \end{pmatrix}, \end{aligned}$$

By using induction method, this solution is satisfied for each integer $n \ge 0$. It has been stated previously that

$$\begin{aligned} Q^{-1}\begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} a & b \\ (-1)^n \frac{b}{r_n} & (-1)^{n+1} \frac{a}{r_n} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \\ &= \begin{pmatrix} r_n \\ 0 \end{pmatrix}, \end{aligned}$$

COROLLARY 1:

Suppose that r_n is the final divider in alkhawarizmi Eukledean to find FSTB (a,b) and $Q^{-1} = \begin{pmatrix} \alpha & \beta \\ (-1)^n \dfrac{b}{r_n} & (-1)^{n+1} \dfrac{a}{r_n} \end{pmatrix}$. The solution for this linear Diophantine equation is $ax+by+c=0$ where $r_n | c$ is derived from $x = x_0 + \dfrac{(-1)^n b}{r_n} t$, and $y = y_0 + \dfrac{(-1)^{n+1} a}{r_n} t$.

From corollary shown above, the matrix method might be influenced by calculation from calculator like TI-85. It has four main benefits which are:

1. It calculates constant α and β only in the linear equation $r_n = \alpha a + \beta b$
2. When the value of r_n, α and β are known, specific solutions for Diophantine linear equation will be more easy which are: $x_0 = \alpha k$, $y_0 = \beta k$, and $k = \dfrac{c}{r_n}$.
3. Any value in the second row is constant for parameter t in general solution of this Diophantine linear equation.
4. It does not show how difficult each calculation is.

When linear congruent is from this linear Diophantine equation, corollary 1 is satisfied. It is said that using the matrix solution is suitable for solving linear congruent.

COROLLARY 2:

Linear congruent equation $ax \equiv c (\operatorname{mod} b)$, can be solved if and only if $rn | c$ and the solution is $x = x_0 + \dfrac{(-1)^n b}{r_n} t$, where $r_n = FSTB(a,b)$.

IV. Conclusion

This study shows that one of the mathematical solutions is through linear Diophantine equation or Diophantine equation of the form $x^2 - Dy^2 = 2z^2$. Actually, there are many forms of Diophantine equation. One of the interesting topics in number theory is Diophantine equation which states that

"a linear Diophantine equation $ax+by=c$, when *a, b* and *c* are whole number have the whole number solution if and only if FSTB (a,b) divide c totally".

It can be concluded that Diophantine equation in general is an equation which states that its variables are from the elements of a whole number. Actually, the solutions for Diophantine equation are many. The more the number of variables used, the longer the calculation. Linear Diophantine equation can be solved in different ways. If we prefer integer solution, we can use this Diophantine equation. Diophantine equation also can be used if we prefer results that are not negative. To further facilitate the Diophantine equation, Eukledean alkhawarizmi can be used. One thing to keep in mind in solving Diophantine equation is, one should be careful in solving every problem especially when writing the initial answers obtained from the parameters used because during the end of the process, one should re-enter each answer that is previously obtained into the original equation.

References

[1]. P. Novikov. 1948. A new solution of the indeterminate equation $ax^2 + by^2 + cz^2 = 0$.

[2]. *Doklady Akad Nauk SSSR (N.S.)* 61:205-206.

[3]. Barnes, E. S. 1953. On the Diophantine equation $x^2 + y^2 + c = xyz$. *J. London Math.*

[4]. *Soc.* 28:242-244.

[5]. Georgikopoulos. 1948. On the equation $ax^2 + by^2 + cz^2 = 0$. *Bul. Soc. Math. Grece* 24:20-25.

[6]. Edward L. Cohen. 1982. *The Mathematics Student,* Vol. 50:106-11.

[7]. Goldberg, K., Newman, M., Straus, E. G. & Swift, J. D. 1954. The representation of integers by binary quadratic rational form. *Arch. Math*. 5:12-18.

[8]. Joseph H. Silverman. 1997. Mersenne prime. *A friendly introduction to number theory.*80-83.

[9]. K. H. Rosen. 1993. *Elementary number theory and its applications, 3rd edition,*

[10]. Addison-Wesley, Reading, Massachusetts.

[11]. Le Veqeu, W. J. 1969. A brief survey of diophantine equation. *MAA studies in Mathematic*. 6:4-23.

[12]. L. J. Mordell. 1969. Diophantine Equation. *Pure and Applied Mathematics, Vol 30, Academic Press.*

[13]. Mills, W. H. 1954. A method for solving certain Diophantine equation. *Proc. Amer. Math. Soc*. 5:473-475.

[14]. T. N. Sinha dan Venkatramaiah. 1978. The equation $x^2 - Py^2 = 2z^2$: *P*, a Mersenne prime. *Indian J. Mech. Math*. 16:45-47.T. Koshy. November 1996. The Euclidean Algorithm via matrices and a calculator,*Math. Gaz*. 80:570-574.

[15]. Wikipedia, the free encyclopedia, Diophantine equation (dalam talian). http://en.wikipedia.org/wiki/Diophantine_equation [3 Mac 2010].

[16]. Wikipedia, the free encyclopedia, Diophantine equation of second powers (dalam talian). http://mathworld.wolfram.com/DiophantineEquation2ndPowers.html [10 Mac 2010].