Journal of Engineering and Applied Sciences 1 (1) : 69-70, 2006

On Diophantine Equation of Degree Two

Nil Ratan Bhattacharjee, Talky Bhattacharjee and Milan Kanti Dhar
Department of Mathematics, University of Chittagong, Chittagong, Bangladesh

Abstract: Attempt have been made to show that the equation $x^2 – py^2 = -1$ is always solvable for integers if P is a prime of the form 4n+1.

Key words: Diophantine equation, Quadratic equation, quadratic residue

INTRODUCTION

The study of pell's equation $x^2 - dy^2 = N$ using the properties of periodic continued Fractions is an ancient one[1].

An Investigation for numerical solution of the equation $x^2 – py^2 = -1$ has been carried out by BACH, B.D. and Williams H.C.[2]. In their work they presented a table of values of P $(1 \le P \le 10^6)$ for integers x, y with $y \neq 0$.

Here we have used a different and generalized method to show that the equation $x^2 – py^2 = -1$ is always solvable in integers if P is a prime of the form 4n + 1. By a representable number we shall mean a number, which is representable as a sum of two squares.

Theorem: The equation $x^2 – py^2 = -1$ is always solvable in integer if P is a prime of the form 4n+ 1.

To prove this theorem we shall use minimality condition and the identity[3].

$$(A^2+B^2)(C^2+D^2) = (AC - BD)^2 + (AD+BC)^2 \text{ OR } (AC+BB)^2 + (AD - BC)^2.$$

Since P is a prime of the form 4n+1 and –1 is a quadratic residue of P[3,4], there is a positive integer u such that

$$u^2 + 1 \equiv 0 \pmod P \quad (1)$$

Therefore, for some natural number m

$$u^2 + 1 = m P \quad (2)$$

Let R be the set of all positive integers for which mP can be represented as a sum of two squares. Then R is not empty. Suppose m_0 be the smallest of them. If m_0=1, there is nothing to prove.

If $m_0 > 1$, then for certain integers x_0, y_0 we have

$$m_0 P = x_0^2 + y_0^2 \quad (3)$$

Obviously m_0 cannot divide both x_0 and y_0 . Hence we can write

$$x_0 = x_1 \pmod{m_0},\ y_0 = y_1 \pmod{m_0} \quad (4)$$

Now from (3) and (4)

$$x_0^2 + y_0^2 \equiv x_1^2 + y_1^2 \equiv 0 \pmod{m_0}$$

Therefore, there are some m_1 such that

$$x_1^2 + y_1^2 = m_1 m_0 \quad (5)$$

where $0 < m_1 \le m_0$

Using the identity we get from (3) and (4)

$$mm_1P = (x_0x_1 + y_0y_1)^2 + (x_0y_1 – x_1y_0)^2 \quad (6)$$

Now

$$x_0x_1 + y_0y_1 \equiv x_1^2 + y_1^2 \equiv 0 \pmod{m_0}$$
$$x_{0y1} – x_1y_0 \equiv x_1y_1 – x_1y_1 \equiv 0 \pmod{m_0}$$

Therefore,

$$m_1P = a^2 + b^2 \quad (7)$$

Where

$$a = (x_0x_1 + y_0y_1)/ m_0$$
$$b = (x_0y_1 – x_1y_0)/ m_0$$

But this contradicts the minimality of m_0 unless $m_0 = m_1$ or $m_0 = 1$.

Hence in both the cases we get an integral number m_1 such that

$$u^2 + 1 = m_1^2 P$$

i.e. $u^2 - m_1^2 P = -1$

Corresponding Auhtor: Talky Bhattacharjee, Department of Mathematics, University of Chittagong, Chittagong, Bangladesh

Now to complete the theorem we shall show that in $mP = u^2 + 1$, m must be a squred number.

If P is not a number of the form $u^2 + 1$, then we must have m>1 such that

$$mP = u^2 + 1$$

And then for some $m_1 < m_0$ equation (6) yeilds.

$$m\, m_1 P = (x_0x_1 + y_0y_1)^2 + (x_0y - x_0y_1)^2$$
$$= a_1^2 + b_1^2$$

if $m_1 = 1$, there is nothing to prove.

But if $m_1>1$ then, since every prime factors of a representable number is also representable proceeding as above we must have a number $m_2 < m_1$ such that

$$m_1^2\, m_2 P = a_2^2 + b_2^2 \text{(say)}$$

if $m_2 \neq 1$ we must have $m_3 < m_2$ and so on.

Continuing the process we shall get $m_1=1$ since P is representable.

Thus it is always possible to have a number

$$m = k^2 = m_1^2 \text{ such that}$$
$$k^2P = x_0^2 + y_0^2, \text{ for some } (x_0, y_0)$$

Hence the theorem.

REFERENCES

1. Mordell, L.J., 1969. Diophantine Equations, Academic press, New York.
2. BACH, B.D. and H.C. WILLIAMS, 1972. A numerical investigation of the Diophantine equation x2-dy2=-1, Florida Atlantic Univ. Boca Raton, Fia, 37.
3. Telang, S.G., 1996. Number Throry, Tata McGraw-Hill Publishing Co. Ltd., New Delhi.
4. Ivan Niven, H.S. Zuckerman and H.L. Montgomery, 2004. John Wiley and Sons, Inc.