On the Number of Solutions of the Diophantine Equation $x^2 - y^2 = N$

J.F.T. Rabago

***Abstract*—In this short note we show that the number of solutions of the Diophantine equation $x^2 - y^2 = N$ depends entirely on its prime factorization. We also derived a formula to determine the number of integral solutions satisfying the given equation. Finally, we find a relation between the number of solutions of the Diophantine equation $x^2 - y^2 = N$ and $\tau(N)$, where $\tau(N)$ denotes the number of positive divisors of N, for N odd.**

***Index Terms*—Diophantine equation, prime factorization, number of solutions, number-of-divisor function.**

***MSC 2010 Codes* – 11D61**

I. Introduction

In a letter to Father Marin Mersenne in 1643, Fermat describe a method of his own for factoring large numbers. His technique of finding an odd factor of a positive integer N is equivalent to solving for integral solutions x and y of the equation

$$x^2 - y^2 = N.$$

Such equation is called Diophantine equation. Intuitively, a Diophantine equation is defined as an equation whose numerical coefficients are integers and for which the solution we seek is restricted only in the set of integers. On the otherhand, it is known that the Diophantine equation

$$x^2 + y^2 = N$$

has no solution for $N \equiv 3 \mod 4$ (*see* for example [2, Lemma 1.12, pg. 9] for the proof). In a more general sense, the solvability of the Diophantine equation $x^2 + y^2 = N$ is given in the following theorem.

Theorem I.1. [*2, Theorem 1.25, pg. 14*] *Let $N \in \mathbb{N}$ with $N \geq 2$ and let $N = \prod_{i=1}^{k} p_i^{\alpha_i}$ be the prime factorization of N. Then N is the sum of two squares if and only if for $i = 1, 2, ..., k$, we have that α_i is even if $p_i \equiv 3$ mod 4.*

In this short note we study the solutions of simple Diophantine equations of the form $x^2 - y^2 = N$. We also provide formulas to determine the number of solutions satisfying the given Diophantine equation. Finally, we present a theorem relating the number of solutions of the Diophantine equation $x^2 - y^2 = N$ to $\tau(N)$, where $\tau(N)$ denotes the number of positive divisors of N, for N odd.

Julius Fergy T. Rabago is with the Department of Mathematics and Physics, Central Luzon State University, Science City of Muñoz, Nueva Ecija Philippines (e-mail: julius_fergy.rabago@up.edu.ph).

II. The Diophantine equation $x^2 - y^2 = N$

In this section we study the solutions of the Diophantine equation of the form $x^2 - y^2 = N$. First we let N be a positive integer and suppose that for some natural number n, N can be factored as $N = p_1^{\alpha_1}\ p_2^{\alpha_2}\ p_3^{\alpha_3}\ \cdots\ p_n^{\alpha_n}$. Hence, we have two possible cases.

If N is prime, then $N = p_i^{\alpha_i}$ for some $i = 1, 2, \ldots, n$ with $\alpha_i = 1$. So,

$$x^2 - y^2 = (x + y)(x - y) = p_i. \tag{1}$$

If $p_i = 2$ then (1) has no solution, otherwise, if p_i is an odd prime we have

$$\begin{cases} x + y = p_i \\ x - y = 1 \end{cases}$$

which implies that

$$(x, y) = \left(\frac{p_i + 1}{2}, \frac{p_i - 1}{2} \right).$$

On the otherhand, if N is not a prime then we have the following subcases.

If N is even then,

$$x^2 - y^2 = (x + y)(x - y) = p_1^{\alpha_1}\ p_2^{\alpha_2}\ p_3^{\alpha_3}\ \cdots\ p_n^{\alpha_n}$$

where $p_i = 2$ and $\alpha_i \geq 1$ for some $i = 1, 2, \ldots, n$. For simplicity, we set $i = 1$, so we have

$$\begin{cases} x + y = 2^{\beta_1}\ p_2^{\beta_2}\ p_3^{\beta_3}\ \cdots\ p_n^{\beta_n} \\ \\ x - y = 2^{\delta_1}\ p_2^{\delta_2}\ p_3^{\delta_3}\ \cdots\ p_n^{\delta_n} \end{cases}$$

where $\delta_j = \alpha_j - \beta_j$ for all $j = 2, 3 \ldots, n$. Solving for x, we obtain

$$x = 2^{\beta_1 - 1}\ p_2^{\beta_2}\ p_3^{\beta_3}\ \cdots\ p_n^{\beta_n} + 2^{\delta_1 - 1}\ p_2^{\delta_2}\ p_3^{\delta_3}\ \cdots\ p_n^{\delta_n}.$$

For $\alpha_1 = 1$, we obtain

$$x = 2^{\beta_1 - 1}\ p_2^{\beta_2}\ p_3^{\beta_3}\ \cdots\ p_n^{\beta_n} + 2^{-\beta_1}\ p_2^{\delta_2}\ p_3^{\delta_3}\ \cdots\ p_n^{\delta_n},$$

in which we see that there is no possible value for β_1 so that x is an integer.

For $\alpha > 1$, we have

$$x = 2^{\beta_1 - 1}\ p_2^{\beta_2}\ p_3^{\beta_3}\ \cdots\ p_n^{\beta_n} + 2^{\delta_1 - 1}\ p_2^{\delta_2}\ p_3^{\delta_3}\ \cdots\ p_n^{\delta_n}.$$

Now, if N is odd, then $N = p_1^{\alpha_1}\ p_2^{\alpha_2}\ p_3^{\alpha_3}\ \cdots\ p_n^{\alpha_n}$ where $p_i \neq 2$ for all $i = 1, 2, \ldots, n$ and $\alpha_i \geq 1$ for some $i = 1, 2, \ldots, n$. This implies that

$$x = \frac{1}{2}\left(p_1^{\beta_1}\ p_2^{\beta_2}\ p_3^{\beta_3}\ \cdots\ p_n^{\beta_n} + p_1^{\delta_1}\ p_2^{\delta_2}\ p_3^{\delta_3}\ \cdots\ p_n^{\delta_n}\right).$$

It is clear that, from the above equation, x is surely an integer since p_i are all odd integers for all $i = 1, 2, \ldots, n$.

It can be observed easily from the above discussion that the number of solutions of the Diophantine equation $x^2 - y^2 = N$ depends on the prime factorization of N. We formalized our results in the following section.

III. Main Results

We have the following theorems:

Theorem III.1. *For any odd integer m, the Diophantine equation*

$$x^2 - y^2 = 2m$$

has no solution. In particular, $x^2 - y^2 = 2$ has no integral solution.

Proof: Since m is odd, then $m = 2k + 1$ for some $k \in \mathbb{Z}$. So,

$$\begin{cases} x + y = 2 \\ x - y = 2k + 1 \end{cases}$$

This implies that, $x = \frac{1}{2}(2k + 3)$. In which no value of $k \in \mathbb{Z}$ for x to be an integer.

Theorem III.2. *Let p_i be odd primes for all $i = 1, 2, \ldots, n$, $q = \prod_{i=1}^{n} p_i^{\alpha_i}$ with $\alpha_i \geq 1$ for all $i \leq n$ and suppose r is the number of solutions of the Diophantine equation $x^2 - y^2 = q$ then*

$$r = 2\prod_{i=1}^{n}(\alpha_i + 1).$$

Proof: Let $\delta_i = \alpha_i - \beta_i$ for all $i = 1, 2, \ldots, n$. Since $x^2 - y^2 = \prod_{i=1}^{n} p_i^{\alpha_i}$ then

$$\begin{cases} x + y = \prod_{i=1}^{n} p_i^{\beta_i} \\ x - y = \prod_{i=1}^{n} p_i^{\delta_i} \end{cases}$$

So, $x = \frac{1}{2}\prod_{i=1}^{n} p_i^{\beta_i} + \frac{1}{2}\prod_{i=1}^{n} p_i^{\delta_i}$. Then we have $\beta_i + 1$ possible exponents for p_i. If we assume that $(x, -y)$ is different from (x, y) then, conclusion follows.

Corollary III.3. *For any prime p, the Diophantine equation $x^2 - y^2 = p$ has the solutions $(x, y) = \left(\pm\frac{p+1}{2}, \pm\frac{p-1}{2}\right)$.*

Theorem III.4. *Let p_i be primes for all $i = 1, 2, 3 \ldots, n$, $q = 4\prod_{i=1}^{n} p_i^{\alpha_i}$ with $\alpha_i \geq 1$ for all $i \leq n$ and suppose t is the number of solutions of the Diophantine equation $x^2 - y^2 = q$ then*

$$t = 2\prod_{i=1}^{n}(\alpha_i + 1).$$

Proof: The proof is similar to Theorem III.2 ∎

Remark III.5. *If we restrict x and y to be non-negative integers in Theorem III.2 then the number of solutions of the Diophantine equation $x^2 - y^2 = N$ would reduce to*

$$r = \left\lceil \frac{1}{2}\prod_{i=1}^{n}(\alpha_i + 1) \right\rceil,$$

where $\lceil\cdot\rceil$ denotes the least integer function. Similarly, in Theorem III.4, the number of solutions would reduce to

$$s = \left\lceil \frac{1}{4}\prod_{i=1}^{n}(\alpha_i + 1) \right\rceil$$

if we apply the same restriction to x and y.

The presence of the least integer function is due to the possibility that the product $\prod_{i=1}^{n}(\alpha_i + 1)$ is odd.

We provide some examples and applications of the above results in the following section.

IV. Some Examples

Here we used the results we obtained from the previous section to support our answers for the following problems.

Example IV.1. *Find all integral solutions of $x^2 - y^2 = 108$.*

Solution: We begin by expressing each side of the above equation into product of power of primes, that is, we have

$$(x + y)(x - y) = 2^2\ 3^3.$$

Then,

$$\begin{cases} x + y = 2^m\ 3^n \\ x - y = 2^{2-m}\ 3^{3-n} \end{cases}$$

Solving for x we obtain

$$x = 2^{m-1}\ 3^n + 2^{1-m}\ 3^{3-n}.$$

In which we see that $m = 1$. Similarly,

$$y = 2^{m-1}\ 3^n - 2^{1-m}\ 3^{3-n}.$$

Letting $m = 1$, we have

$$\begin{cases} x + y = 2 \cdot 3^n \\ x - y = 2 \cdot 3^{3-n} \end{cases}$$

It follows that we have the following set of solutions

$$\{(x, y) : x^2 - y^2 = 108\} = \{(\pm 28, \pm 26), (\pm 12, \pm 6)\}.$$

Example IV.2. *Find all integral solutions of $x^2 - y^2 = 600$.*

Solution: We write the given equation into its prime factorization. Hence,

$$(x + y)(x - y) = 2^3 \cdot 3 \cdot 5^2,$$

and so,

$$\begin{cases} x + y = 2^m\ 3^n\ 5^r \\ x - y = 2^{3-m}\ 3^{1-n}\ 5^{2-r} \end{cases}$$

Solving for the values of x and y we have,

$$x = 2^{m-1}\ 3^n\ 5^r + 2^{2-m}\ 3^{1-n}\ 5^{2-r}.$$

and

$$y = 2^{m-1}\ 3^n\ 5^r - 2^{2-m}\ 3^{1-n}\ 5^{2-r}.$$

Thus, from Theorem III.4, we have 24 pairs of solutions (x, y). In particular, we have the following

$$\begin{aligned}\{(x,y) : x^2 - y^2 = 600\} \quad &= \quad \{(\pm 151, \pm 149), (\pm 77, \pm 73),\\ &\quad (\pm 53, \pm 47), (\pm 35, \pm 25),\\ &\quad (\pm 31, \pm 19), (\pm 25, \pm 5)\}.\end{aligned}$$

Example IV.3. *Find all integral solutions of* $x^2 - y^2 = 294$.

Solution: Again we express the given equation into product of power of primes.

$$(x + y)(x - y) = 2 \cdot 3 \cdot 7^2.$$

Then,

$$\begin{cases} x + y = 2^m\ 3^n\ 7^r \\ \\ x - y = 2^{1-m}\ 3^{1-n}\ 7^{2-r} \end{cases}$$

Solving for x we have,

$$x = 2^{m-1}\ 3^n\ 7^r + 2^{-m}\ 3^{1-n}\ 7^{2-r}.$$

Which gives us no possible value for m for x to be an integer. Therefore, $x^2 - y^2 = 294$ has no integral solution. This can be verified easily by Theorem III.1 since it is obvious that $x^2 - y^2 = 294 = 2(147)$.

Example IV.4. *Find all integral solutions of* $x^2 - y^2 = 189$.

Solution: Note that $x^2 - y^2 = 189$ can be express as $(x + y)(x - y) = 3^3 \cdot 7$ which has, by Theorem III.2, 16 solutions. Then,

$$\begin{cases} x + y = 3^m\ 7^n \\ \\ x - y = 3^{3-m}\ 7^{1-n} \end{cases}$$

Solving for x and y we have,

$$x = \frac{3^m\ 7^n + 3^{3-m}\ 7^{1-n}}{2}$$

and

$$y = \frac{3^m\ 7^n - 3^{3-m}\ 7^{1-n}}{2}.$$

Thus, we have the following set of solutions

$$\begin{aligned}\{(x,y) : x^2 - y^2 = 189\} \quad &= \quad \{(\pm 95, \pm 94), (\pm 33, \pm 30),\\ &\quad (\pm 17, \pm 10), (\pm 15, \pm 6)\}.\end{aligned}$$

Remark IV.5. *If we restrict our solutions to be in the set of positive integers in Example IV.1 then we'll have only two solutions, specifically (28,26) and (12,6). Take note that the number of solutions in Example IV.1 agrees with Remark III.5. Similarly, if we apply the same argument to Example IV.2, the number of solutions would reduce from 24 to six. In particular, we'll only have the following set of solutions:* $\{(151, 149), (77, 73), (53, 47), (35, 25), (31, 19), (25, 5)\}$ *for Example IV.2.*

Now, we will see in the following last two examples the use of least integer function in Remark III.5.

Example IV.6. *In how many ways the number 9 can be expressed as a difference of squares of two integers?*

Solution: It can be observed that $(3, 0)$ and $(5, 4)$ are the only solutions of the Diophantine equation $x^2 - y^2 = 9$. Hence, we see that we have 2 solutions. This can be verified easily using Remark III.5. Note that $9 = 3^2$, then $r = \left\lceil \frac{1}{2}(3) \right\rceil = 2$.

Example IV.7. *Let* x *and* y *be positive integers. Determine the number of solutions of the Diophantine equation* $x^2 - y^2 = 400$*?*

Solution: It could be verified that the solution to the Diophantine equation $x^2 - y^2 = 400$ is the set $\{(20, 0), (25, 15), (29, 21), (52, 48), (101, 91)\}$. Then, we have 5 solutions. This result agrees with Remark III.5, since $s = \left\lceil \frac{1}{2} \prod_{i=1}^{2} (\alpha_i + 1) \right\rceil = \left\lceil \frac{9}{2} \right\rceil = 5$.

As a final remark, we present the following theorem expressing the number-of-divisor function $\tau(N)$ in terms of the number of solutions of the Diophantine equation $x^2 - y^2 = N$, for N odd.

Theorem IV.8. *Let* p_i *be odd primes for all* $i = 1, 2, \ldots, n$, $N = \prod_{i=1}^{n} p_i^{\alpha_i}$ *with* $\alpha_i \geq 1$ *for all* $i \leq n$ *and suppose* r *is the number of solutions of the Diophantine equation* $x^2 - y^2 = N$, *then*

$$\tau(N) = \frac{1}{2} r,$$

where $\tau(N)$ *denotes the number of positive divisors of* N.

V. Conclusion

Formulas for the number of solutions of the Diophantine equation $x^2 - y^2 = N$ were obtained and an expression relating the number of solutions of the given Diophantine equation and the number of positive divisors of N for N odd was developed. For future study, it might be interesting to find a formula expressing the number of solutions of the given Diophantine equation and the number of positive divisors of N for $N \equiv 0 \bmod 4$.

VI. Acknowledgement

I am grateful to the anonymous referee for his valuable suggestion and comment for the preparation of this manuscript.

References

[1] D. Burton, *Elementary Number Theory,* Allyn and Bacon, Inc., USA, 1980.

[2] S. Delcroix, *Topics in Number Theory,* California State University, Fresno, 2008.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 4th ed., Oxford University Press, Great Britain, 1959.