The Study On The Positive Integer Solution To The Indeterminate Equation $x^2 - y^2 = C$

Gao Ming

The College of Mathematics and Information,
China West Normal University,
Nanchong, Sichuan, China 637002

Abstract

The positive integer solution to the indeterminate equation

$x^2 - y^2 = C$ *(1)*

is an important component of Elementary Number Theory. This article studies the conditions for the existence, the form of exceptional circumstances and the number of solution to (1) as well as other aspects.

Key Words: indeterminate equation; existence; form

I. On the existence of positive integer solution to the equation $x^2 - y^2 = C$

The study on the positive integer solution to (1) is primarily sought for *C*. I.e., if x and y are positive integers satisfying (1), then we only need discuss the value of *C*.

Formula: if *C* is a positive integer then *C* can be written as the form of $2^k C_1$ where C_1 is an odd integer and $k \geq 0$.

Theorem1: The indeterminate equation (1) has a solution if and only if $k \geq 0$ and $k \neq 1$.

We may firstly rewrite (1) as

$$(x+y)(x-y) = 2^k C_1 \qquad (2)$$

So that we can discuss the theorem from three aspects.

When $k = 0$, as we can see, $x+y$ and $x-y$ are odd integers with C_1 is an odd integer. Then we shall get $x = \frac{C_1+1}{2}$ and $y = \frac{C_1-1}{2}$ solving $x^2 - y^2 = C_1$ such that (1) has a solution.

When $k=1$, as $2C_1$ is an even integer, $x+y$ and $x-y$ are also even integers. Since the left but not the right side of the equation is divisible by 4, there aren't two integers x and y solving $x^2-y^2=2C_1$.Hence, (1) clearly has no solution.

When $k\geq 2$ (2) can be shown as

$$(x+y)(x-y)=2^{k-1}C_1\times 2 \qquad (3)$$

Similarly, we shall get $x=2^{k-2}C_1+1$ and $y=2^{k-2}C_1-1$satisfying $x^2-y^2=2^kC_1$.

Thus, (1) has a solution.

II. The form of solution of positive integer solution to the equation $x^2-y^2=C$

Having discussed the existence of solutions in the previous section, we will continue to solve the problem about the form of solution to (1).

According to The Unique Factorization Theorem, C_1 can be written as $p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$, where $a_1,a_2,\cdots,a_n$ are positive integers or zero and $p_1,p_2,\cdots,p_n$ are odd prime numbers.

Theorem 2: If $k=0$, the solution to (1) has the form of

$$x=\frac{1}{2}\left(\prod_{i=1}^{n}p_i^{\alpha_i}+\prod_{i=1}^{n}p_i^{\beta_i}\right)\text{and}\ y=\frac{1}{2}\left(\prod_{i=1}^{n}p_i^{\alpha_i}-\prod_{i=1}^{n}p_i^{\beta_i}\right),$$

where

$$\alpha_1+\beta_1=a_1,\alpha_2+\beta_2=a_2,\cdots,\alpha_n+\beta_n=a_n$$

and

$$p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}>p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}.$$

Meanwhile, all number of solutions to (1) is given by

$$\left[\frac{(a_1+1)(a_2+1)\cdots(a_n+1)}{2}\right]\ \text{or}\left[\frac{(a_1+1)(a_2+1)\cdots(a_n+1)-1}{2}\right].$$

From the hypothesis, we know $C_1=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$. If $(a_1+1)(a_2+2)\cdots(a_n+1)$ is an odd integer, then $C_1$is a sequence of an odd integer. In addition, C_1 Can at least be decomposed into the product of C_1 and 1, we shall obtain $x^2-y^2=C_1$be solvable in $x=\frac{C_1+1}{2}$ and $y=\frac{C_1-1}{2}$.We might assume that C_1 is decomposed into the product of C_2 andC_3,C_2 and C_3 can be of the product of $p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ then we

shall obtain $x^2 - y^2 = C_1$ be solvable in $x = \frac{C_2 + C_3}{2}$ and $y = \frac{C_2 - C_3}{2}$ in the same way. As the number of the positive divisor of C_1 which is a sequence of an odd integer is $(a_1+1)(a_2+2)\cdots(a_n+1)$, all number of solutions to (1) is given by $\left[\frac{(a_1+1)(a_2+1)\cdots(a_n+1)-1}{2}\right]$.If $(a_1+1)(a_2+2)\cdots(a_n+1)$ is an even integer, similarly, we shall obtain all number of solution to (1) is given by $\left[\frac{(a_1+1)(a_2+1)\cdots(a_n+1)-1}{2}\right]$.

Lemma 1: If C_1 is an odd prime number, then (1) has only one solution for $x = \frac{C_1+1}{2}$ and $y = \frac{C_1-1}{2}$.

Theorem 3: If $k \geq 2$, the solution to (1) has the form of

$$x = \left(2^m \prod_{i=1}^{n} p_i^{\alpha_i} + 2^t \prod_{i=1}^{n} p_i^{\beta_i}\right) \text{ and } y = \left(2^m \prod_{i=1}^{n} p_i^{\alpha_i} - 2^t \prod_{i=1}^{n} p_i^{\beta_i}\right)$$

Where

$$\alpha_1 + \beta_1 = a_1, \alpha_2 + \beta_2 = a_2, \cdots, \alpha_n + \beta_n = a_n,$$

$$2^m p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} > 2^t p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

in which $m + t = k - 2$. Hence, all number of solutions to (1) is given by

$$\left[\frac{(k-1)(a_1+1)(a_2+1)\cdots(a_n+1)}{2}\right] \text{ or } \left[\frac{(k-1)(a_1+1)(a_2+1)\cdots(a_n+1)-1}{2}\right].$$

III. The development of solution of the indeterminate equation $x^2 - y^2 = C$

From what has been discussed above we know the existence and form of solution to (1), it is quietly worth discussing the normal equation

$$x^2 - Dy^2 = C. \qquad (4)$$

Situation 1: If $D = n^2, (n = 1,2,\cdots)$, then (4) can be converted into the form of (1), which has been discussed.

Situation 2: If $D = -n^2, (n = 1,2,\cdots)$, , then (4) can be converted into the form of

$$x^2 - (ny)^2 = C. \qquad (5)$$

If we let C denote $(5k)^2$, the integer solution to (5) is $x = 3k$, and $y = \frac{4k}{n}$ where n divides $4k$ or $x = 4k$, and $y = \frac{3k}{n}$, in which n divides $3k$.

If C denotes $\left(a^2 + b^2\right)^2$, and $(x, y) = 1$ with x or ny is divisible by 2, then (5) is solvable in $x = 2ab$, and $y = \frac{a^2 - b^2}{n}$ or $x = a^2 - b^2$ and $y = \frac{2ab}{n}$.

If C which is a prime number denotes the sun of two squares, then (5) has four solutions.

In contrast, if (5) has a solution where C is a positive nonsquare integer, and then C denotes the sun of two squares.

Situation 3: Assuming D is an integer, the existence of solution to (4) depends on the value of D and C.

If $-D > C$, (4) has no solution.

If $-D = C$, (4) has two solutions, $x = 0, y = 1$ or $x = 0, y = -1$.

If $D < C$, (4) can be converted into the form of $\frac{x^2}{C} - \frac{y^2}{\frac{C}{D}} = 1$.

If (4) has a solution, then the solution satisfies $0 \le x \le \sqrt{C}, 0 \le y \le \sqrt{-\frac{C}{D}}$;

If (4) has a positive solution, then there are two integer a and b such that $\frac{C}{b^2 - a^2 D}$ is a square.

Situation 4: If $C = 1$ and D isn't a square, then (4) will be converted into Pell's Equation $x^2 - Dy^2 = 1$.

According to the knowledge of Pell's Equation, we know that if x_1 and y_1 make $x + \sqrt{D}y$ be minute, and then all solutions of the equation are given by

$$x_n = \frac{1}{2}\left[\left(x_1 + Dy_1\right)^n + \left(x_1 - Dy_1\right)^n\right], y_n = \frac{1}{2\sqrt{D}}\left[\left(x_1 + \sqrt{D}y_1\right)^n + \left(x_1 - \sqrt{D}y_1\right)^n\right].$$