Open Access Library Journal
2024, Volume 11, e12011
ISSN Online: 2333-9721
ISSN Print: 2333-9705

The Solution of the Indefinite Equation by the Method of Euclidean Algorithm

Zhongqi Zhou

Hubei Coal Geology Bureau, Wuhan, China
Email: zhouzongqi1058@163.com

How to cite this paper: Zhou, Z.Q. (2024) The Solution of the Indefinite Equation by the Method of Euclidean Algorithm. *Open Access Library Journal*, **11**: e12011.
https://doi.org/10.4236/oalib.1112011

Received: July 26, 2024
Accepted: August 23, 2024
Published: August 26, 2024

Abstract

In this paper, a new mathematical method is used to study the indefinite equations of binary quadratic and binary arbitrary order, the problem of judging and solving these indefinite equations with or without solutions is solved.

Subject Areas

Integral Equation, Number Theory

Keywords

Euclidean Algorithm, Binary Quadratic Indefinite Equation, Indefinite Equation of Higher Order in Binary, Positive Integer Solutions

1. Introduction

On the whole, there is no uniform method to solve the indefinite equations of more than two degrees, but some results have been obtained for some special equations of higher order [1].

If a positive integer can be expressed as the sum of squares of two numbers, it is generally difficult to give a formula to express its solution in detail [2].

The study of indefinite equation $m = qx^n + py^n \left(n \geq 3\right)$ is very rare, and there is no general determination method for this kind of indefinite equation with and without solutions, and there is no general method for solving it.

In this paper, the following problems will be solved by using the Euclidean algorithm:

1) A general solution for $m = x^2 + y^2$ is given (its solution is expressed in a formula).

2) Give a determination method for $m = qx^n + py^n \left(n \geq 2\right)$ with or without solutions.

3) A general solution for $m = qx^n + py^n$ is given.

2. Definition

Definition 1

Let $q, p \in N^+$, $m \geq 3$, q, p, m are all given positive integer, if $m \mid qz^n + p$, then

$$qz^n \equiv -p \pmod{m} \tag{1}$$

For the solution of congruence (1), see [3].

Definition 2

Let $m > 3$ is a known positive integer, $qa^n \equiv -p \pmod{m}$, q, p is a known positive integer, $n \geq 2$, $(q, p) = 1$, define the following procedure as m and a Euclidean algorithm.

Denoted by the symbol: $\overrightarrow{(m,a)_{qa^n \equiv -p \pmod{m}}}$.

$$m = q_1 a + r_1 \qquad 0 < r_1 < a \tag{2}$$

$$a = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1, \tag{3}$$

$$r_1 = q_3 r_2 + r_3 \qquad 0 < r_3 < r_2, \tag{4}$$

$$\vdots \qquad \vdots$$

$$r_{i-3} = q_{i-1} r_{i-2} + r_{i-1} \qquad qr_{i-1}^n > m, \quad 0 < r_{i-1} < r_{i-2}, \tag{5}$$

$$r_{i-2} = q_i r_{i-1} + r_i \qquad qr_i^n < m, \quad 0 < r_i < r_{i-1}, \tag{6}$$

$$\vdots \qquad \vdots$$

3. Lemma

Lemma [4] Let m and a be positive integers, and do the Euclidean algorithm:

$$m = q_1 a + r_1, \qquad 0 < r_1 < a$$

$$a = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1$$

$$\vdots \qquad \vdots$$

$$r_{k-2} = q_k r_{k-1} + r_k, \qquad 0 < r_k < r_{k-1}$$

$$\vdots \qquad \vdots$$

record

$$s_0 = 1, s_1 = q_1, s_k = q_k s_{k-1} + s_{k-2}, k \geq 2$$

$$l_0 = 0, l_1 = 1, l_k = q_k l_{k-1} + l_{k-2}, k \geq 2$$

then

$$ml_k - as_k = (-1)^{k-1} r_k. \tag{7}$$

4. Theorems

Theorem 1. Let all positive integer of $m > 3$, $z^2 \equiv -1 \pmod{m}$ less than $\frac{m}{2}$ be solved as: $a_1, a_2, \cdots, a_k$. Then m and a_t Euclidean algorithm, $m = x^2 + y^2$

for all positive integer solution. $t=1,\cdots,k$. $m-a_t$ is the negative integer solution (the same result is obtained with all negative integer solutions).

Proof: Let's prove that $m=x^2+y^2$ has a positive integer solution:

From $a_t^2\equiv -1\pmod{m}$, we know: $a_t^2+1=lm$, l is a positive integer, m is a factor of a_t^2+1, and a_t^2+1 has only prime factor of 2 and $4n+1$, so m also has only prime factors of 2 and $4s+1$, therefore, $m=x^2+y^2$ has positive integer solutions [5].

$\overleftrightarrow{(m,a_t)}_{a_t^2\equiv -1(\bmod m)}$ and according to (7) obtain:

$$ml_j-a_ts_j=(-1)^{j-1}r_j. \tag{8}$$

Modulo m to (8) to obtain the congruence:

$$(-1)^{j-1}\times r_j\equiv -s_ja_t\pmod{m} \tag{9}$$

Let square both sides of (9):

$$r_j^2\equiv s_j^2\times a_t^2\pmod{m} \tag{10}$$

Since $a_t^2\equiv -1\pmod{m}$, the congruence (10) morphs into:

$$r_j^2+s_j^2\equiv 0\pmod{m}.$$

$$\text{Or}\quad r_j^2+s_j^2=l_jm \tag{11}$$

l_j is a positive integer.

From $a_t^2\equiv -1\pmod{m}$ we know that: $(a,m)=1$, take $\overleftrightarrow{(m,a_t)}_{a_t^2\equiv -1(\bmod m)}$, always get the following result:

$$\begin{array}{ll}
m=q_1a_t+r_1 & 0<r_1<r_0=a_t,\\
a=q_2r_1+r_2 & 0<r_2<r_1,\\
r_1=q_3r_2+r_3 & 0<r_3<r_2,\\
\vdots & \vdots\\
r_{i-3}=q_{i-1}r_{i-2}+r_{i-1} & r_{i-1}^2>m,\ 0<r_{i-1}<r_{i-2},\\
r_{i-2}=q_ir_{i-1}+r_i & r_i^2<m,\ 0<r_i<r_{i-1},\\
\vdots & \vdots\\
r_{k-2}=q_kr_{k-1}+r_k & r_k=1.
\end{array}$$

According to the above result and (7), a further result can be obtained:

When k is even:

$$s_1=r_{k-(1-1)}=r_k, s_2=r_{k-(2-1)}=r_{k-1},\cdots,s_k=r_{k-(k-1)}=r_1.$$

$$r_{\frac{k}{2}}=r_i\left(r_i^2<m,r_{i-1}^2>m\right),s_i=s_{\frac{k}{2}}=r_{k-\left(\frac{k}{2}-1\right)}=r_{\frac{k}{2}+1}=r_{i+1}.$$

When k is odd:

$$s_1=r_{k-1},s_2=r_{k-2},\cdots,s_j=r_{k-j},\cdots,s_k=r_{k-k}=r_0=a_t.$$

$$r_{\frac{k-1}{2}}=r_i\left(r_i^2<m,r_{i-1}^2>m\right),s_i=s_{\frac{k-1}{2}}=r_{k-\frac{k-1}{2}}=r_{\frac{k+1}{2}}=r_{i+1}.$$

According to the above result:

$$s_i = r_{i+1}.$$

Since $r_{i+1} < r_i$, according to (6) of definition 2: $r_i^2 < m$, so the $r_{i+1}^2 = s_i^2 < r_i^2 < m$.

According to (11) we get $r_i^2 + s_i^2 = l_i m$, since l_i is a positive integer, therefore

$$l_i = 1.$$

Resulting in: $m = r_i^2 + s_i^2 = r_i^2 + r_{i+1}^2$. That is $x = r_i, y = r_{i+1}$.

Inference:

According to theorem 1, for any positive integer *m*, as long as there is a, such that $a^2 \equiv -1(\operatorname{mod} m)$, then a positive integer solution of $m = x^2 + y^2$ can be obtained by Euclidean algorithm, the following indefinite equations can obtained by this method:

$$m = x^2 + y^2, m = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}, p_s \equiv 1(\operatorname{mod} 4), s = 1,2,\cdots,r; \alpha = 0,1.$$

Example 1. Find all positive integer solutions for $28249 = x^2 + y^2$.

Solving the congruence $z^2 \equiv -1(\operatorname{mod} 28249)$ yields the following four positive integer solutions:

$$606, 6118, 11266, 11471.$$

$\overleftrightarrow{(28249, 606)}_{606^2 \equiv -1(\operatorname{mod} 28249)}$ Giving: $r_i = 140, r_{i+1} = 93; x_1 = 140, y_1 = 93$.

$\overleftrightarrow{(28249, 6118)}_{6118^2 \equiv -1(\operatorname{mod} 28249)}$ Giving: $r_i = 157, r_{i+1} = 60; x_2 = 157, y_2 = 60$.

$\overleftrightarrow{(28249, 11266)}_{11266^2 \equiv -1(\operatorname{mod} 28249)}$ Giving: $r_i = 168, r_{i+1} = 5; x_3 = 168, y_3 = 5$.

$\overleftrightarrow{(28249, 11471)}_{11471^2 \equiv -1(\operatorname{mod} 28249)}$ Giving: $r_i = 165, r_{i+1} = 32; x_4 = 165, y_4 = 32$.

Theorem 2. Set the $q, p \geq 1$, for a given positive integer, $(qx, py) = 1$, $n \geq 2$, if $qz^n \equiv -p(\operatorname{mod} m)$ no positive integer solutions, then

$$m = qx^n + py^n$$

No positive integer solution.

Proof: If $m = qx^n + py^n$ has a positive integer solution, set it as: (x_0, y_0), that is:

$$m = qx_0^n + py_0^n,\ qx_0^n \equiv -py_0^n (\operatorname{mod} m),\ q\left(\frac{x_0}{y_0}\right)^n \equiv -p(\operatorname{mod} m).$$

When the $\frac{x_0}{y_0} \equiv a(\operatorname{mod} m)$, then $qa^n \equiv -p(\operatorname{mod} m)$, with the $qz^n \equiv -p(\operatorname{mod} m)$ unsolved contradictions.

Theorem 3. Set the $q, p \geq 1$, $m > 1$, for a given positive integer, $(qx, py) = 1$, $n \geq 2$, if $qz^n \equiv (p \operatorname{mod} m)(\operatorname{mod} m)$ no positive integer solutions, then

$$m = qx^n - py^n$$

No positive integer solution.

Proof: If $m = qx^n - py^n$ has a positive integer solution, set it as: (x_0, y_0), that is:

$$m = qx_0^n - py_0^n,\ qx_0^n \equiv (p \bmod m) y_0^n (\bmod m),\ q\left(\frac{x_0}{y_0}\right)^n \equiv (p \bmod m)(\bmod m).$$

When the $\frac{x_0}{y_0} \equiv a(\bmod m)$, then $qa^n \equiv (p \bmod m)(\bmod m)$, with the $qz^n \equiv (p \bmod m)(\bmod m)$ unsolved contradictions.

Theorem 4. m is a given positive integer no nth power factor, $n \geq 2$. $q, p \geq 1$ are all given positive integer, without nth power factors. $(q, p) = 1$, $qz^n \equiv -p(\bmod m)$ for all positive integers less than m are solved as: $a_1, a_2, \cdots, a_k$. $t = 1, \cdots, k$. (when n is even, only take all positive integer solutions less than $\frac{m}{2}$, since $m - a_t$ and a_t yield the same result).

Respectively $\overleftrightarrow{(m,a_t)}_{qa_t^n \equiv -p(\bmod m)}$ and according to (7), respectively

$$(-1)^{i-1} \times r_i = l_i m - s_i a \tag{12}$$

When n is even, if for some a_t, when $qr_{i-1}^n > m$, $qr_i^n < m$, $ps_i^n < m$, then $m = qx^n + py^n$ there are positive integer solutions.

When n is odd, if for some a_t such that i is even and

$$qr_{i-1}^n > m, qr_i^n < m, ps_i^n < m,$$

Then

$m = qx^n + py^n$ there are positive integer solution.

If for all a_t such that $qr_{i-1}^n > m, qr_i^n < m, ps_i^n > m$ and when n is odd, i is odd, then $m = qx^n + py^n$ there is not positive integer solution.

Proof: take (12) modulo m to get:

$$(-1)^{i-1} \times r_i \equiv -s_i a_t (\bmod m) \tag{13}$$

If n is even, raise both sides of (13) to the power n and multiply q to get:

$$qr_i^n \equiv s_i^n qa_t^n (\bmod m)$$

Since $qa_t^n \equiv -p(\bmod m)$, $qr_i^n + ps_i^n \equiv 0(\bmod m)$, $qr_i^n + ps_i^n = l_i m$.

According to (6) of the definition of $\overleftrightarrow{(m,a_t)}_{qa_t^n \equiv -p(\bmod m)}$: $qr_i^n < m$, if one $ps_i^n < m$.

Then

$$m = qr_i^n + ps_i^n.$$

If n is odd, raise both sides of (13) to the power n and multiply by q:

$$(-1)^{i-1} qr_i^n \equiv -s_i^n qa_t^n (\bmod m) \tag{14}$$

If there is an a_t, such that i is even and $ps_i^n < m$, because $qa_t^n \equiv -p(\bmod m)$,

Then (14) become:

$$qr_i^n + ps_i^n \equiv 0(\bmod m)$$

If there is a a_t such that i is even and $ps_i^n < m$, from the definition of

$\overleftrightarrow{(m,a_t)}_{qa_t^n \equiv -p(\bmod m)}$ We know: $qr_i^n < m$, therefore

$$qr_i^n + ps_i^n = m.$$

If for all a_t such that $ps_i^n > m$ and when *n* is odd, *i* is odd, then $m = qx^n + py^n$.

There are not positive integer solution.

This is because: when *n* is even, there is for any *j*:

$$qr_j^n + ps_j^n = l_j m.$$

When $j > i$, $s_j > s_i$, $ps_j^n > m$, when $j < i$, $qr_j^n > m$, so, for any *j* have:

$$qr_j^n + ps_j^n > m.$$

When *n* is odd and *i* is odd, $qr_i^n - ps_i^n = l_i m$. $qr_i^n + ps_i^n \neq m$.

Example 2. Find the positive integer solution of $14978 = 3x^3 + 5y^3$.

Solving the congruence $3z^3 \equiv -5(\bmod 14978)$ yields the following 3 positive integer.

Solution: 1153,7705,13609.

$\overleftrightarrow{(14978,1153)}_{3\times1153^3 \equiv -5(\bmod 14978)}$ is obtained: $r_i = r_2 = 11$, $s_i = 13$, $5\times13^3 < 14978$.

$\overleftrightarrow{(14978,7705)}_{3\times7705^3 \equiv -5(\bmod 14978)}$ is obtained $r_i = r_5 = 6$, $s_5 = 208$, *n* is odd, *i* is odd.

$\overleftrightarrow{(14978,13609)}_{3\times13609^3 \equiv -5(\bmod 14978)}$ is obtained $r_i = r_5 = 8$, $s_5 = 50$, *n* is odd, *i* is odd.

From the above results we can see: $i = 2$, $3\times r_2^3 = 3993 < 14978$, $5\times13^3 < 14978$.

So the positive integer solution of the indefinite equation is:

$$x = 11,\ y = 13.$$

Example 3. Find the positive integer solution of $20527956 = x^5 + y^5$.

Solving the congruence $z^5 \equiv -1(\bmod 20527956)$ yields the following 5 positive integer solutions:

$$3539303, 6224291, 6284051, 17595395, 20527955.$$

$\overleftrightarrow{(20527956,3539303)}_{3639303^5 \equiv -1(\bmod 20527956)}$ Giving: $r_i = r_4 = 7$, $s_4 = 29$, $29^5 < 20527956$.

$\overleftrightarrow{(20527956,6224291)}_{6224291^5 \equiv -1(\bmod 20527956)}$ Giving $r_i = r_9 = 13$, $s_9 > 60$, *n* is odd, *i* is odd.

$\overleftrightarrow{(20527956,6284051)}_{62840515 \equiv -1(\bmod 20527956)}$ Giving $r_i = r_9 = 23$, $s_9 > 60$, *n* is odd, *i* is odd.

$\overleftrightarrow{(20527956,17595395)}_{17595395^5 \equiv -1(\bmod 20527956)}$ Giving $r_i = r_2 = 29$, $s_2 = 7$, $7^5 < 20527956$.

$\overleftrightarrow{(20527956,20527955)}_{20527955 \equiv -1(\bmod 20527956)}$ Giving $r_i = r_1 = 1$, $s_1 = 1$, *n* is odd,

i is odd.

From the above results we can see: $i=4$, $s_4^5 = 29^5 < 20527956$.

So the positive integer solution of the indefinite equation is:

$$x = 7,\ y = 29.$$

From the above results we can see: $i=2$, $s_2^5 = 7^5 < 20527956$.

So the positive integer solution of the indefinite equation is:

$$x = 29,\ y = 7.$$

Example 4. Find the positive integer solution of $26067 = x^3 + 7y^3$.

Solving the congruence $7z^3 \equiv -1 \pmod{26067}$ yields the following 3 positive integer solutions: 6890,19208,26036.

$\overleftrightarrow{(26067, 6890)}_{7\times 6890^3 \equiv -1 \pmod{26067}}$ is obtained $r_i = r_8 = 10$, $s_8 = 227$, $227^3 > 26067$.

$\overleftrightarrow{(26067, 19208)}_{7\times 19208^3 \equiv -1 \pmod{26067}}$ is obtained $r_i = r_4 = 14$, $r_i = r_4 = 14$, $19^3 < 26067$.

$\overleftrightarrow{(26067, 26036)}_{7\times 26036^3 \equiv -1 \pmod{26067}}$ is obtained $r_i = r_3 = 4$, $s_3 = 841$, n is odd, i is odd.

From the above results we can see: $i=4$, $7\times r_4^3 = 7\times 14^3 < 26067$, $19^3 < 26067$.

So the positive integer solution of the indefinite equation is:

$$x = 19,\ y = 14.$$

Example 5.

Example 5. Find the positive integer solution of $59783703 = 5x^4 + 11y^4$.

Solving the congruence $5z^3 \equiv -11 \pmod{59783703}$ has no positive integer solution.

According to theorem 2: indefinite equations have no positive integer solution.

5. Conclusions

For the indefinite equation $m = x^2 + y^2$ (m is a given positive integer), as long as $z^2 \equiv -1 \pmod{m}$ has a solution, the positive integer solution can be obtained by the Euclidean algorithm.

For the indefinite equation $m = qx^n + py^n$ ($n \ge 2, m, q, p$ are all given positive integer, $(q, p) = 1$), it can be solve by solving the congruence $qz^n \equiv -p \pmod{m}$ method to judge whether the equation has a positive integer solution, if $qz^n \equiv -p \pmod{m}$ has no positive integer solution, then the equation has no positive Integer solution; if the congruence formula has solutions, it can be judged and solved according to the Euclidean algorithm given in this paper.

The above method is a general and effective method.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Ke, Z. and Sun, Q. (2011) Talk about Indefinite Equations. Harbin Institute of Technology Press.

[2] Pan, C.D. and Pan, C.B. (2009) Elementary Number Theory. Beijing University Press, 279-280.

[3] Vinogradov (2014) Fundamentals of Number Theory and Vinogradov. Harbin Institute of Technology Press, 43-45.

[4] Ji, J. (2013) Number Theory and Application. Tsinghua University Press, 23.

[5] Silverman, J.H. (2008) Introduction to Number Theory. Ministry of Machinery Industry Press, 127.