Pell 方程递归解的幂型因子性质及其在不定方程中的应用

华南师范大学附属中学:　赵玉博　　指导教师:　郝保国

摘要

本文的目标是研究 Catlan 猜想($x^m - y^n = 1$ 除 x=3,m=2,y=2,n=3 之外无正整数解)的一个推广，即：不定方程 $x^m - 2y^n = 1$ 都可能有哪些正整数解。为解决这一问题，深入研究了 pell 方程的解的一些数论性质，即：当最小解确定时，方程的递归解的因子性质。并将其结论应用于对这种不定方程的讨论中，在限定 n 为偶数的情况下取得了较为成功的结果。此外，文中还包含了关于 pell 方程解的数论性质的结论在一些其它问题中的应用。

关键词：pell 方程、Catlan 猜想

Some Arithmetic Properties about the Factor of the Solution to Pell Equation and Its Applications in Diophantine Equations

The Affiliated High School of South China Normal University Zhao Yubo
Directed by: Hao Baoguo

Abstract

This Paper is aimed to study a generalization of the Catlan Conjecture (The only nontrivial solution to $x^m - y^n = 1$ is x=3,m=2,y=2,n=3), that is, to determine the nontrivial solutions to $x^m - 2y^n = 1$. To solve this problem, I study some arithmetic properties of the solutions to Pell equation, or more precisely, when the minimum solution is fixed, the properties about factors of the recursive solutions to the equation. Furthermore, I apply these properties into the study of $x^m - 2y^n = 1$, and obtain some successful results when n is restricted to be even. What's more, some applications of these arithmetic properties in other problems are contained in the paper as well.

Key Words and Phrases:

Pell equation, Catlan Conjecture

1. Preliminaries.

We begin with some elementary properties about the solutions of Pell equation.

(1) $x^2 - Dy^2 = 1$ ($D > 0$ and has no divisor of form n^2) is called positive Pell equation(or standard Pell equation). It always has a minimal positive solution (x_1, y_1), and all solutions (x_n, y_n) are fixed by $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$,

(or $x_n = \dfrac{\lambda^n + \bar{\lambda}^n}{2}$, $y_n = \dfrac{\lambda^n - \bar{\lambda}^n}{2\sqrt{D}}$, where $\lambda = x_1 + y_1\sqrt{D}$, $\bar{\lambda} = x_1 - y_1\sqrt{D}$)

Furthermore, the recursion formula $\begin{cases} x_n = x_{n-1}x_1 + Dy_{n-1}y_1 \\ y_n = x_{n-1}y_1 + y_{n-1}x_1 \end{cases} (n \ge 2)$

and $\begin{cases} x_{m+n} = x_m x_n + Dy_m y_n \\ y_{m+n} = x_m y_n + y_m x_n \end{cases} (m, n \in N^*)$ hold.

If we define $x_0 = 1$, $y_0 = 0$, $x_{-n} = x_n$, $y_{-n} = -y_n$, index in the recursion formulas above can be chosen from $\mathbb{Z}$ including negative integers.

(2) $x^2 - Dy^2 = -1$, is called negative Pell equation. If it has solution, it must have infinitely many solutions. Assume (a_1, b_1) is its minimal positive solution, then the general solutions (a_n, b_n) are fixed by $a_n + b_n\sqrt{D} = (a_1 + b_1\sqrt{D})^{2n-1}$, (or

$a_n = \dfrac{\mu^{2n-1} + \bar{\mu}^{2n-1}}{2}$, $b_n = \dfrac{\mu^{2n-1} - \bar{\mu}^{2n-1}}{2\sqrt{D}}$, where $\mu = a_1 + b_1\sqrt{D}$, $\bar{\mu} = a_1 - b_1\sqrt{D}$)

What's more, $(a_1 + b_1\sqrt{D})^2 = x_1 + y_1\sqrt{D}$ (As the symbols above, (x_1, y_1) is the minimal solution of the corresponding positive Pell equation).

(3) $x^2 - Dy^2 = K$, $|K| > 1$, is called quasi-Pell equation. If it has solution, it must have infinitely many solutions. In particular, when $|K| = 2$, if we denote the minimal solution as (u_1, v_1), then the general solutions (u_n, v_n) are fixed by

$u_n + v_n\sqrt{D} = \frac{(u_1 + v_1\sqrt{D})^{2n-1}}{2^{n-1}}$ (or $u_n = \frac{\xi^{2n-1} + \bar{\xi}^{2n-1}}{2^n}$, $v_n = \frac{\xi^{2n-1} - \bar{\xi}^{2n-1}}{2^n\sqrt{D}}$, where $\xi = u_1 + v_1\sqrt{D}$，$\bar{\xi} = u_1 - v_1\sqrt{D}$)

（4）No matter what kind of Pell equation it is, the recursion formula always holds. Where (x_n, y_n) and (x_n^*, y_n^*) stand for the nth positive solution of $x^2 - Dy^2 = K$ and $x^2 - Dy^2 = 1$.

2. Main Theorems

In this paper, we will obtain the following two main theorems

Theorem 1 (1) For standard Pell equation $x^2 - Dy^2 = 1$，assume d is a divisor of D, d is greater than 3, and $(y_1, d) = 1$，then $d^k \parallel y_n \Leftrightarrow d^k \parallel n$ $(n \in N^*$, $k \in N$. The symbol "$\parallel$" means: $b^a \parallel a \Leftrightarrow b^a \mid a$, $b^{a+1} \nmid a$)

(2) For（I）negative Pell equation $x^2 - Dy^2 = -1$,

（II）quasi-Pell equation $x^2 - Dy^2 = \pm 2, -4$,

（III）quasi-Pell equation $x^2 - Dy^2 = 4$.

Similar conclusion holds, that is：

In equation of type （I）, if $d \mid D$ and (d, y_1) =1 , $d > 3$, then $d^k \parallel y_n \Leftrightarrow d^k \parallel 2n-1$.

In equation of type （II）, if $d \mid D$, (d, y_1) =1，$d > 3$，and d is odd integer，then $d^k \parallel y_n \Leftrightarrow d^k \parallel 2n-1$.

In equation of type （III）, if $d \mid D$, (d, y_1) =1，$d > 3$，and d is odd integer， then $d^k \parallel y_n \Leftrightarrow d^k \parallel n$.

(3) In particular, for standard Pell equation $x^2 - Dy^2 = 1$, we have: assume the minimal solution is (x_1, y_1), $d \mid D$, $d > 3$, and $d^\alpha \parallel y_1$, then if $(d, \frac{y_1}{d^\alpha}) = 1$, we have $d^{\alpha+k} \parallel y_n \Leftrightarrow d^k \parallel n$.

Remark: In (2), among the equations of type (I), the situation that $2 \mid d$ and $k > 0$ will never occurat all, since this will yield $2 \mid y_n \Rightarrow 4 \mid Dy_n^2 \Rightarrow x_n^2 \equiv -1 (\mathrm{mod}\, 4)$, which leads to a contradiction. So in this case d must be odd.

Theorem 2 (1) Denote the general solutions of standard Pell equation $x^2 - Dy^2 = 1$ as (x_n, y_n), then $\forall t \in N^*$ among the following propositions either (i) or (ii) will hold; and either (iii) or (iv) will hold:

(i) $\forall n, t \nmid x_n$.

(ii) $\exists\ f(t) \in N^*$ which is uniquely determined by t, such that $t \mid x_n \Leftrightarrow \frac{n}{f(t)}$ is a positive odd integer.

(iii) $\forall n, t \nmid y_n$.

(iv) $\exists\ g(t) \in N^*$ which is uniquely determined by t, such that $t \mid y_n \Leftrightarrow g(t) \mid n$.

(2) $x^2 - Dy^2 = -2$, denote its general solutions as (x_n, y_n), for $\forall$ odd integer t, among the following propositions either (i) or (ii) will hold; and either (iii) or (iv) will hold:

(i) $\forall n \in N^*, t \nmid x_n$.

(ii) $\exists\ f(t) \in N^*$ which is uniquely determined by t, such that $t \mid x_n \Leftrightarrow f(t) \mid 2n-1$.

(iii) $\forall n \in N^*, t \nmid y_n$.

(iv) $\exists\ g(t) \in N^*$ which is uniquely determined by t, such that $t \mid y_n \Leftrightarrow g(t) \mid 2n-1$.

(3)More generally, we can obtain：

For fixed $t \in N^*$，we denote the following statement as proposition （I）：either we cannot find an x_n such that $t \mid x_n$，or $\exists f(t) \in N^*$ such that $t \mid x_n \Leftrightarrow n = (2k-1) f(t)$，$k \in N^*$；either we cannot find an y_n such that $t \mid y_n$，or $\exists g(t) \in N^*$ such that $t \mid y_n \Leftrightarrow n = kg(t)$，$k \in N^*$.

In parallel, we denote the following statement as proposition （II）：either we cannot find an x_n such that $t \mid x_n$，or $\exists f(t) \in N^*$ such that $t \mid x_n \Leftrightarrow 2n-1 = kf(t)$，$k \in N^*$；either we cannot find an y_n such that $t \mid y_n$，or $\exists g(t) \in N^*$ such that $t \mid y_n \Leftrightarrow 2n-1 = kg(t)$，$k \in N^*$.

Then we have：

（i）For $x^2 - Dy^2 = 1$，proposition （I） holds.

（ii）For $x^2 - Dy^2 = -1$，proposition（II） holds.

（iii）For $x^2 - Dy^2 = \pm 2$，proposition（II）holds if we require in which t is odd.

（iv）对 $x^2 - Dy^2 = \pm 4$，proposition（I）holds if we require in which t is odd.

This paper will be organized as follows：in section 3 we will prove theorem 1，and several applications of theorem 1 will be given in section 4；in section 5 we will prove theorem 2，and several applications of theorem 2 will be given in section 6. In the applications in section 4 and 6，we will obtain parts of the results of the generalized Catlan’s Conjecture.

3. Proof of Theorem 1

Obviously, theorem 1.(1) is the corollary of 1.(3), so we prove 1.(3) first.

The proof of 1.(3) is divided into three parts:

In standard Pell equation $x^2 - Dy^2 = 1$, assume d is divisor of D, d is greater than 3, and $d^{\alpha} \| y_1$, $(d, \frac{y_1}{d^{\alpha}}) = 1$ ($\alpha \in N$).

(i) $d^{\alpha+1} \mid y_n \Leftrightarrow d \mid n$

since
$$y_n = \frac{(x_1 + \sqrt{D} y_1)^n - (x_1 - \sqrt{D} y_1)^n}{2\sqrt{D}} = C_n^1 \cdot x_1^{n-1} y_1 + C_n^3 \cdot x_1^{n-3} y_1^3 \cdot D + \ldots$$
$$\equiv n x_1^{n-1} y_1 (\bmod d^{\alpha+1})$$

and by the original equation we have $(x_1, d) = 1$, then by $(d, y_1) = d^{\alpha}$ the conclusion follows.

(ii) $d^{\alpha+1} \nmid y_d$

If not, assume $d^{\alpha+2} \mid y_d = d x_1^{d-1} y_1 + C_d^3 x_1^{d-3} y_1^3 D + \ldots$

Then
$$d^{\alpha+2} \mid d x_1^{d-1} y_1 + \frac{d(d-1)(d-2)}{6} x_1^{d-3} y_1^3 D + \ldots$$
$$d^{\alpha+1} \mid x_1^{d-1} y_1 + \frac{D(d-1)(d-2)}{6} x_1^{d-3} y_1^3 + \ldots$$

If $3 \nmid d$, then $3 \mid (d-1)(d-2)$, $2 \mid (d-1)(d-2)$

so $6 \mid (d-1)(d-2)$

then $d^{\alpha+1} \mid D \cdot \frac{(d-1)(d-2)}{6} x_1^{d-3} y_1^3 \Rightarrow d^{\alpha+1} \mid x_1^{d-1} y_1$, which leads to a contradiction.

If $3 \mid d$, then assume $d = 3d_1$, then $d_1 > 1$

so $d_1^{\alpha+1} \mid x_1^{d-1} y_1 + \frac{D}{3} \frac{(d-1)(d-2)}{2} x_1^{d-3} y_1^3 + \ldots \Rightarrow d_1^{\alpha+1} \mid x_1^{d-1} y_1$ however $(x_1 y_1, d^{\alpha}) = d^{\alpha}$ and $d_1 > 1$, which leads to a contradiction. So (ii) holds.

(iii) Now we prove the theorem directly

By the preliminary proposition（4）, $\begin{cases} y_{2d} = 2x_d y_d \equiv 2x_d y_d \pmod{d^{2\alpha+3}} \\ x_{2d} = x_d^2 + Dy_d^2 \equiv x_d^2 \pmod{d^{2\alpha+3}} \end{cases}$. Generally，

if we have proven $\begin{cases} y_{kd} \equiv kx_d^{k-1} y_d \pmod{d^{2\alpha+3}} \\ x_{kd} \equiv x_d^k \pmod{d^{2\alpha+3}} \end{cases}$ then

$$y_{(k+1)d} = y_{kd} x_d + x_{kd} y_d \equiv kx_d^{k-1} y_d \cdot x_d + x_d^k y_d \equiv (k+1) x_d^k y_d \pmod{d^{2\alpha+3}}$$

$$x_{(k+1)d} = x_{kd} x_d + D y_{kd} y_d \equiv x_d^k \cdot x_d + D \cdot kx_d^{k-1} y_d \cdot y_d \equiv x_d^{k+1} \pmod{d^{2\alpha+3}}$$

so $\begin{cases} x_{nd} \equiv x_d^n \pmod{d^{2\alpha+3}} \\ y_{nd} \equiv nx_d^{n-1} y_d \pmod{d^{2\alpha+3}} \end{cases}$

so whe $d \nmid n$ we have $d^{\alpha+2} \nmid y_{nd}$， otherwise $d^{\alpha+2} \mid nx_d^{n-1} y_d \Rightarrow d \mid nx_d^{n-1}$.

by $(d, x_n) = 1 \Rightarrow d \mid n$， this is a contradiction. This deduction also proves when $d \mid n$,

$d^{\alpha+2} \mid y_{nd}$. $d^{\alpha+2} \nmid y_{d^2}$.

so $d^{\alpha+2} \mid y_n \Leftrightarrow d^2 \mid n$， $d^{\alpha+2} \nmid y_{d^2}$.

Generally, assume that we have proven $d^{\alpha+s} \mid y_n \Leftrightarrow d^s \mid n$， and $d^{\alpha+s} \nmid y_{d^s}$, $s \in N^*$.

then $\begin{cases} x_{2d^s} = x_{d^s}^2 + Dy_{d^s}^2 \equiv x_{d^s}^2 \pmod{d^{2\alpha+2s+1}} \\ y_{2d^s} = 2x_{d^s} y_{d^s} \equiv 2x_{d^s} y_{d^s} \pmod{d^{2\alpha+2s+1}} \end{cases}$.

If we have proven $\begin{cases} x_{k \cdot d^s} \equiv x_{d^s}^k \pmod{d^{2\alpha+2s+1}} \\ y_{k \cdot d^s} \equiv kx_{d^s}^{k-1} y_{d^s} \pmod{d^{2\alpha+2s+1}} \end{cases}$.

then
$$x_{(k+1)d^s} = x_{kd^s} \cdot x_{d^s} + D \cdot y_{kd^s} \cdot y_{d^s} \equiv x_{d^s}^k \cdot x_d^s + Dx_{d^s}^k y_{d^s}^2 \equiv x_{d^s}^{k+1} \pmod{d^{2\alpha+2s+1}}.$$

$$y_{(k+1)d^s} = x_{kd^s} y_{d^s} + y_{kd^s} x_{d^s} \equiv x_{d^s}^k y_{d^s} + kx_{d^s}^{k-1} x_{d^s} \equiv (k+1) x_{d^s}^k y_{d^s} \pmod{d^{2\alpha+2s+2}}$$

so $\forall n, \begin{cases} x_{nd^s} \equiv x_{d^s}^n \pmod{d^{2\alpha+2s+2}} \\ y_{nd^s} \equiv nx_{d^s}^{n-1} y_{d^s} \pmod{d^{2\alpha+2s+2}} \end{cases}$.

So naturally we have $d^{\alpha+s+1} \mid y_n \Leftrightarrow s^{s+1} \mid n$, $d^{\alpha+s+1} \parallel y_{d^{s+1}}$.

By induction we have $\forall k \in N^*$, $d^{\alpha+k} \parallel y_n \Leftrightarrow d^k \parallel n.$ $\square$

Proof of 1．(2)：

Firstly，the minimal solution of $x^2 - Dy^2 = h$ is (x_1, y_1)，then the general solution (x_n, y_n) is given by $x_n + y_n\sqrt{D} = \dfrac{(x_1 + y_1\sqrt{D})^{a_n}}{b_n}$.

Where when $h = -1$，$a_n = 2n - 1$，$b_n = 1$；

when $h = 4$ ，$a_n = n$，$b_n = 2^{n-1}$；

when $h = -4$，$a_n = 2n - 1$，$b_n = 2^{2n-2}$；

when $h = \pm 2$，$a_n = 2n - 1$，$b_n = 2^{n-1}$.

The proof will still be divided into three parts：

（i） $d \mid y_n \Leftrightarrow d \mid a_n$

since
$$y_n = \frac{(x_1 + \sqrt{D}y_1)^{a_n} - (x_1 - \sqrt{D}y_1)^{a_n}}{2b_n\sqrt{D}} = \frac{C_{a_n}^1 \cdot x_1^{a_n-1} y_1 + C_{a_n}^3 \cdot x_1^{a_n-3} y_1^3 \cdot D + \ldots}{b_n}$$
$$\equiv a_n x_1^{a_n-1} y_1 \pmod d$$

By the original equation we have $(x_1, d) = 1$，then by $(d, y_1) = 1$ the conclusion holds.

（ii） $d \parallel y_{c_d}$

Where when $h = -1, -4, \pm 2$, $c_d = \dfrac{d+1}{2}$, when $h = 4$, $c_d = d$. Then we have $a_{c_d} = d$.

If not，assume $d^2 \mid y_{c_d} = \dfrac{a_{c_d} x_1^{a_{c_d}-1} y_1 + C_{a_{c_d}}^3 x_1^{a_{c_d}-3} y_1^3 D + \ldots}{b_{c_d}}$

Then
$$d^2 \mid d x_1^{d-1} y_1 + \frac{d(d-1)(d-2)}{6} \cdot x_1^{d-3} y_1^3 D + \ldots$$
$$d \mid x_1^{d-1} y_1 + \frac{D(d-1)(d-2)}{6} \cdot x_1^{d-3} y_1^3 + \ldots$$

If $3 \nmid d$, then $3 \mid (d-1)(d-2)$ ，$2 \mid (d-1)(d-2)$， so $6 \mid (d-1)(d-2)$

and $$d \mid D\cdot\frac{(d-1)(d-2)}{6} \Rightarrow d \mid x_1^{d-1}y_1,$$ which is a contradiction.

If $d^2 \mid nu_d^{n-1}v_d \Rightarrow d \mid nu_d^{n-1}$. $3 \mid d$, then assume $d = 3d_1$, $d_1 > 1$

so $$d_1 \mid x_1^{d-1}y_1 + \frac{D}{3}\cdot\frac{(d-1)(d-2)}{2}x_1^{d-3}y_1^3 + \ldots \Rightarrow d_1 \mid x_1^{d-1}y_1$$

but $(x_1y_1, d) = 1$ and $d_1 > 1$, which is a contradiction. So (ii) holds.

(iii) Now we prove the theorem directly

Let $u_n + \sqrt{D}v_n = (x_1 + \sqrt{D}y_1)^n$, then actually we have $x_n = \dfrac{u_{a_n}}{b_n}$, $y_n = \dfrac{v_{a_n}}{b_n}$ u_n, v_n satisfy $\begin{cases} u_{m+n} = u_m u_n + Dv_m v_n \\ v_{m+n} = u_m v_n + u_n v_m \end{cases}$ Thus what we have got in the previous two steps is exactly $d \mid v_n \Leftrightarrow d \mid n$, $d \,\|\, v_d$.

Then we have $$\begin{cases} v_{2d} = 2u_d v_d \equiv 2u_d v_d \pmod{d^3} \\ u_{2d} = u_d^2 + Dv_d^2 \equiv u_d^2 \pmod{d^3} \end{cases}$$

Generally, assume we have proven $$\begin{cases} v_{kd} \equiv ku_d^{k-1}v_d \pmod{d^3} \\ u_{kd} \equiv u_d^k \pmod{d^3} \end{cases}$$

Then $$v_{(k+1)d} = v_{kd}u_d + u_{kd}v_d \equiv ku_d^{k-1}v_d\cdot u_d + u_d^k v_d \equiv (k+1)u_d^k v_d \pmod{d^3}$$

$$u_{(k+1)d} = u_{kd}u_d + Dv_{kd}v_d \equiv u_d^k\cdot u_d + D\cdot ku_d^{k-1}v_d\cdot v_d \equiv u_d^{k+1} \pmod{d^3}$$

So we have $$\begin{cases} u_{nd} \equiv u_d^n \pmod{d^3} \\ v_{nd} \equiv nu_d^{n-1}v_d \pmod{d^3} \end{cases}$$

So when $d \nmid n$ we have $d^2 \nmid v_{nd}$, otherwise $d^2 \mid nu_d^{n-1}v_d \Rightarrow d \mid nu_d^{n-1}$.

By $(d, u_n) = 1 \Rightarrow d \mid n$, which is a contradiction. This also proves when $d \mid n$ we have $d^2 \mid v_{nd}$. $d^2 \,\|\, v_{d^2}$

So $$d^2 \mid v_n \Leftrightarrow d^2 \mid n, \quad d^2 \,\|\, v_{d^2}.$$

Generally, assume we have proven $d^s \mid v_n \Leftrightarrow d^s \mid n$, and $d^s \,\|\, v_{d^s}$,

then $$\begin{cases} u_{2d^s} = u_{d^s}^2 + Dv_{d^s}^2 \equiv u_{d^s}^2 \pmod{d^{s+2}} \\ v_{2d^s} = 2u_{d^s}v_{d^s} \equiv 2u_{d^s}v_{d^s} \pmod{d^{s+2}}. \end{cases}$$

If we have proven $\begin{cases} u_{k\cdot d^s} \equiv u_{d^s}^k \pmod{d^{s+2}} \\ v_{k\cdot d^s} \equiv k u_{d^s}^{k-1} v_{d^s} \pmod{d^{s+2}}. \end{cases}$

Then $u_{(k+1)d^s} = u_{kd^s} \cdot u_{d^s} + D \cdot v_{kd^s} \cdot v_{d^s} \equiv u_{d^s}^k \cdot u_d^s + D u_{d^s}^k v_{d^s}^2$

$$\equiv u_{d^s}^{k+1} \pmod{d^{s+2}}.$$

$$v_{(k+1)d^s} = u_{kd^s} v_{d^s} + v_{kd^s} u_{d^s} \equiv u_{d^s}^k v_{d^s} + k u_{d^s}^{k-1} u_{d^s}$$

$$\equiv (k+1) u_{d^s}^k v_{d^s} \pmod{d^{s+2}}$$

so $\forall n, \begin{cases} u_{nd^s} \equiv u_{d^s}^n \pmod{d^{s+2}} \\ v_{nd^s} \equiv n u_{d^s}^{n-1} v_{d^s} \pmod{d^{s+2}}. \end{cases}$

so naturally we have $d^{s+1} \mid v_n \Leftrightarrow d^{s+1} \mid n$, $d^{s+1} \parallel v_{d^{s+1}}$

Then by induction we have $\forall k \in N^*$, $d^k \parallel v_n \Leftrightarrow d^k \parallel n.$

That is exactly $d^k \parallel y_n \Leftrightarrow d^k \parallel a_n$ $\square$

4. Applications of Theorem 1

Example 1 $x^2 - 24^{2n+1} = 1$ x, $n \in N.$

This equation has an obvious solution $x = 5$, $n = 0$. Assume (x, n) is a non-negative solution of $x^2 - 24^{2n+1} = 1$ such that $n > 0$, then in the Pell equation

$x^2-24y^2=1$, assume $y_m=24^n, n>0$, then $24^n \mid y_m \Leftrightarrow 24^n \mid m$. So $y_m \geq y_{24^n}$.

Notice that $y_{24^n}=C_{24^n}^1\cdot 5+C_{24^n}^3\cdot 5^3\cdot 24+...$

$$\geq 5\cdot 24^n > 24^n = y_m$$

This is a contradiction.

So this equation has no non-negative integral solution other than $(x,n)=(5,0)$.

This example can be directly generalized into the following result:

$x^2-(a^2-1)^{2n-1}=1$ （$a>2$ is fixed, x, n are variables）has no non-negative solutions.

A more general question is: Besides $n=0$, is there any non-negative integral solution of $x^2-y^{2n+1}=1$? We can only obtain parts of answer to this question here.

Example 2 $x^2-y^{2n+1}=1\ (n>0)$ when $2n+1=p$ is prime, we must have $2\mid y$, $p\mid x$.

Proof: First we prove $2\mid y$. Otherwise $2\nmid y$, then $2\mid x$. So $x+1$, $x-1$ are both odd.

By $(x+1)(x-1)=y^{2n+1}$, and $(x+1)(x-1)=y^{2n+1}$

So $\begin{matrix} x+1=u^{2n+1} \\ x-1=v^{2n+1} \end{matrix} \Rightarrow u^{2n+1}-v^{2n+1}=2$. So $u-v \mid u^{2n+1}-v^{2n+1}=2$.

Since u, v are either both odd or both even, we must have $u=v+2$. So $(v+2)^{2n+1}-v^{2n+1}\geq 2^{2n+1}>2$. This is a contradiction.

So $2\mid y$.

By the original equation, we have $x^2=(y+1)(y^{p-1}-y^{p-2}+...+1)$.

$y^{p-1}-y^{p-2}+...+1\equiv 1-(-1)+...+1=p(\mathrm{mod}\ y+1)$.

If $p\mid y+1$ then $p\mid x^2 \Rightarrow p\mid x$, and the conclusion follows.

Next we assume $p\nmid y+1$ so $(y+1, y^{p-1}-y^{p-2}+...+1)=1$.

So $\begin{cases} y+1=a^2 \\ y^{p-1}-y^{p-2}+...+1=b^2 \end{cases}$ since $y\geq 2$ and $2\mid y$ so $y\geq 8$， $a>2$.

Now the original equation turns into $x^2-(a^2-1)^{2n+1}=1 \quad (a>2)$

By the generalization of example 1 we know this equation has no non-negative integral solutions such that $n>0$. □

In fact $x^2-y^{2n+1}=1$ is a special case of Catalan's Conjecture：the Diophantine equation $x^a-y^b=1$ has only one solution $x=3$，$y=2$，$a=2$，$b=3$ if we require the positive integers x，y，a，b are greater than 1. This conjecture has been solved by Preda Mihăilescu in 2002.

Now we deal with the generalized Catlan's conjecture： the Diophantine euqation $x^m-2y^n=1$.

When m=n=2, it is just the standard Pell equation $x^2-2y^2=1$，we have known it has infinitely many solutions with minimal solution (3,2)，general solutions can be given by $x_n+\sqrt{2}y_n=(3+2\sqrt{2})^n$.

When m=p or 2p，p is odd prime，the following several examples show some necessary conditions of the solutions of this equation.

Example 3 $x^p-2y^2=1\ (x>3)$ (p is odd prime), its any positive integral solution must satisfy $p\mid y$.

Proof： $(x^p-1)(x^{p-1}+...+1)=2y^2$

$x^{p-1}+...+1\equiv p(\text{mod}(x-1))$

If $p \mid x-1$, then obviously $p \mid y$.

If $p \nmid x-1$, then $(x-1, x^{p-1}+\ldots+1)=1$.

Since x is odd, $x^{p-1}+\ldots+1$ is odd, too.

so $x^{p-1}+\ldots+1=a^2$, $x-1=2b^2$.

The equation turns to $(2b^2+1)^p-2y^2=1$, so $(2y,(2b^2+1)^{\frac{p-1}{2}})$ is solution of quasi-Pell equation $X^2-2(2b^2+1)Y^2=-2$.

The minimal solution of this equation is $(X_1,Y_1)=(2b,1)$, assume

$$(2y,(2b^2+1)^{\frac{p-1}{2}})=(X_n,Y_n),$$

Then by theorem 1.(2) we have $(2b^2+1)^{\frac{p-1}{2}} \mid n$, thus $n \ge (2b^2+1)^{\frac{p-1}{2}}$

Now $X_n+\sqrt{2(2b^2+1)}Y_n=\dfrac{\left(2b+\sqrt{2(2b^2+1)}\right)^{2n-1}}{2^{n-1}}$,

So $Y_n \ge \dfrac{(2n-1)(2b)^{2n-2}}{2^{n-1}} > 2n-1 \ge n \ge (2b^2+1)^{\frac{p-1}{2}} = Y_n$, this is a contradiction.

So $p \mid x-1$, $p \mid y$. □

Completely in parallel, we can prove any positive integral solution of $x^p-2y^2=-1\ (x>3)$ (p is odd prime) must satisfy $p \mid y$.

Example 4 $x^{2p}-2y^2=1$ $(x>3)$ (p is odd prime), its any positive integral solution must satisfy $p \mid y$.

Proof: $x^{2p}+y^4=(y^2+1)^2$, and x is odd $\Rightarrow x^{2p}\equiv 1 \pmod 8$, so y is even.

By results from Pythagoras equation, $\exists a,b$ with one odd and the other even, $a>b$,

such that $x^p=a^2-b^2$, $y^2=2ab$, $y^2+1=a^2+b^2$.

so $a^2+b^2=1+2ab$ $a-b=1$.

so $x^p = 2b+1$， $y^2 = 2b(b+1)$.

When b is odd， $(2(b+1), b) = 1$， so $2(b+1) = u^2$， $b = v^2$， $y = uv$，

$x^p - 2v^2 = 1$，by Example 3， $p \mid v$ so $p \mid y$.

When b is even， $(2b, (b+1)) = 1$， so $2b = u^2$， $(b+1) = v^2$， $y = uv$，

$x^p - 2v^2 = -1$，by the remark after Example 3， $p \mid v$ so $p \mid y$. □

Example 5 The Diophantine equation $3^{2n+1} - 2y^2 = 1$ has no positive integral solution when $2n+1$ is a composite number.

Lemma： a， m， $n \in N^*$， 则 $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Proof of lemma：For $m > n$, by Euclidean algorithm we have，

$$m = q_1 n + r_1$$

$$n = q_2 r_1 + r_2$$

$$\cdots$$

$$r_k = q_{k+2} r_{k+1} + r_{k+2}$$

$$\cdots$$

$$r_s = q_{s+2} r_{s+1}$$

thus $r_{s+1} = (m, n)$.

Then we have $(a^m - 1, a^n - 1)$

$$= ((a^m - 1) - (a^n - 1), a^n - 1)$$

$$= (a^m - a^n, a^n - 1)$$

$$= (a^n (a^{m-n} - 1), a^n - 1)$$

$$= (a^{m-n} - 1, a^n - 1)$$

$$= \dots = (a^{m-q_1 n} - 1, a^n - 1) = (a^n - 1, a^{r_1} - 1)$$

$= \ldots = (a^{r_1}-1, a^{r_2}-1) = \ldots = (a^{r_s}-1, a^{r_{s+1}}-1) = a^{r_{s+1}}-1 = a^{(m,n)}-1$.

The lemma is proven.

Now return to Example 5. Denote prime divisors of $2n+1$ as p_1, p_2, …, p_k.

since $2n+1$ is a composite number,

So for $\forall 1 \le i \le k$,

$p_i < 2n+1$. Now we have $\left(3^{\frac{2n+1}{p_i}}\right)^{p_i} - 2y^2 = 1$, since $3^{\frac{2n+1}{p_i}} > 3$, by conclusion of

Example 3 we know for $\forall 1 \le i \le k$, $p_i \mid y$.

So $3^{2n+1} \equiv 1 \pmod{p_i}$, $\forall 1 \le i \le k$.

Without losing generality, we can assume p_1 is the minimal prime divisor of

$2n+1$, then p_1 is an odd integer that is greater than 1, and we have

$p_1 \mid 3^{2n+1}-1$, $p_1 \mid 3^{p_1-1}-1$

By the lemma, $p_1 \mid 3^{(2n+1, p_1-1)}-1$.

Notice that all the prime divisors of p_1-1 is smaller than p_1, by our assumption of p_1, $2n+1$ cannot divided by them. So p_1-1 is relative prime to $2n+1$.

Thus $(2n+1, p_1-1) = 1$, $p_1 \mid 3-1 = 2$, this is a contradiction.

Thus we have proven when $2n+1$ is a composite number, $3^{2n+1} - 2y^2 = 1$ has no positive integral solutions. □

5. Proof of Theorem 2

Theorem 2.(1) We denote the general solutions of standard Pell equation $x^2 - Dy^2 = 1$ as (x_n, y_n), then $\forall t \in N^*$,

among the following propositions either (i) or (ii) will hold; and either (iii) or (iv) will hold:

(i) $\forall n, t \nmid x_n$.

(ii) $\exists\ f(t) \in N^*$ that is uniquely determined by t, such that $t \mid x_n \Leftrightarrow \dfrac{n}{f(t)}$ is a positive odd integer.

(iii) $\forall n, t \nmid y_n$.

(iv) $\exists\ g(t) \in N^*$ that is uniquely determined by t, such that $t \mid y_n \Leftrightarrow g(t) \mid n$.

Proof: First, we enlarge the domain of index of (x_n, y_n) from N^* to $\mathbb{Z}$. Define

$$x_n = \frac{(x_1 + \sqrt{D}y_1)^n + (x_1 - \sqrt{D}y_1)^n}{2}, \quad y_n = \frac{(x_1 + \sqrt{D}y_1)^n - (x_1 - \sqrt{D}y_1)^n}{2\sqrt{D}}, \quad \forall n \in \mathrm{Z}.$$

Check directly from the definition we have $\begin{cases} x_{m+n} = x_m x_n + D y_m y_n \\ y_{m+n} = x_m y_n + y_m x_n \end{cases} (\forall m, n \in Z)$.

If we let $\lambda = x_1 + \sqrt{D}y_1$, $\bar{\lambda} = x_1 - \sqrt{D}y_1$, then

$$x_n = \frac{\lambda^n + \bar{\lambda}^n}{2} = \frac{\lambda^n + \bar{\lambda}^n}{2(\lambda \cdot \bar{\lambda})^n} = \frac{\lambda^{-n} + \bar{\lambda}^{-n}}{2} = x_{-n}$$

$$y_n = \frac{\lambda^n - \bar{\lambda}^n}{2\sqrt{D}} = \frac{\lambda^n - \bar{\lambda}^n}{2(\lambda \cdot \bar{\lambda})^n \sqrt{D}} = \frac{\bar{\lambda}^{-n} - \lambda^{-n}}{2\sqrt{D}} = -y_{-n}.$$

Or equivalently, $(x_{-n}, y_{-n}) = (x_n, -y_n) \quad \forall n \in \mathrm{Z}$.

With these preparations we can enter the proof of the theorem now.

For $\forall r \in N^*$, $\begin{cases} y_{n+r} = x_n y_r + x_r y_n \equiv x_n y_r \pmod{x_r} \\ x_{n+r} = x_n x_r + D y_n y_r \equiv D y_n y_r \pmod{x_r} \end{cases}$.

so $$x_{n+r} \equiv Dy_n y_r \equiv D\cdot(x_{n-r}y_r)y_r = Dy_r^2 x_{n-r} \pmod{x_r}$$

For fixed $r \in N^*$, assume $n = 2kr + r_0$, $-r < r_0 \le r$.

Then we have $x_n \equiv \left(Dy_r^2\right)^k x_{r_0} \pmod{x_r} \equiv \left(Dy_r^2\right)^k x_{|r_0|} \pmod{x_r}$. $0 \le |r_0| \le r$.

（since $x_{r_0} = x_{-r_0} = x_{|r_0|}$ ）

Thus, for $\forall t \in N^*$ such that there is some x_n that can be divided by t, assume $x_{f(t)}$ is the minimal term with positive index such that its index is dividable by t and itself is dividable by t as well, then $(t, Dy_{f(t)}^2) = 1$. In the congruence equation above we let $r = f(t)$, then $t \mid x_n \Leftrightarrow t \mid x_{|r_0|}$. Since $0 \le |r_0| \le f(t)$, and $x_0 = 1$ cannot be divided by p, then by our requirement of $f(t)$ we must have $|r_0| = f(t)$, or equivalently, $n = (2k \pm 1) f(t)$. So $\frac{n}{f(t)}$ is a positive odd number.

The other direction of the sufficient and necessary condition is easy to shown in the same manner.

As for the corresponding conclusion about y_n: either $\forall n \in N^*$, $t \nmid y_n$; or $\exists g(t) \in N^*$, such that $t \mid y_n \Leftrightarrow g(t) \mid n$.

By $y_{n+r} = y_n x_r + x_n y_r \equiv x_r y_n \pmod{y_r}$ immediately we have:

If $n = kr + r_0$, $0 \le r_0 < r$,

then $y_n \equiv \left(x_r\right)^k y_{r_0} \pmod{y_r}$. Thus we still take $y_{g(t)}$ as the term with minimal positive integral index among those terms that are dividable by t. In the congruence equation above let $r = g(t)$ we have $t \mid y_n \Leftrightarrow t \mid y_{r_0}$, by our requirement of $g(t)$, we must have $r_0 = 0$, that just means $g(t) \mid n$.

The other direction of the sufficient and necessary condition is easy to shown in the same manner. □

Theorem 2.(1) actually shows such a fact: among the solutions (x_n, y_n) of $x^2 - Dy^2 = 1$, if we select out the terms that can be dividable by a given positive integer t, we will see that their indexes are generated by a positive integer $f(t)$ that is determined by t.

Theorem 2.(2) $x^2 - Dy^2 = -2$, denote its general positive integral solutions as (x_n, y_n), for $\forall$ odd integer t, among the following propositions either (i) or (ii) will hold; and either (iii) or (iv) will hold:

(i) $\forall n \in N^*, t \nmid x_n$.

(ii) $\exists$ $f(t) \in N^*$ that is uniquely determined by t, such that $t \mid x_n \Leftrightarrow f(t) \mid 2n-1$.

(iii) $\forall n \in N^*, t \nmid y_n$.

(iv) $\exists$ $g(t) \in N^*$ that is uniquely determined by t, such that $t \mid y_n \Leftrightarrow g(t) \mid 2n-1$.

Proof: Denote the minimal solution as (x_1, y_1), $\mu = x_1 + \sqrt{D}y_1$,

$$x_n = \frac{\mu^{2n-1} + \overline{\mu}^{2n-1}}{2^n}, \quad y_n = \frac{\mu^{2n-1} - \overline{\mu}^{2n-1}}{2^n\sqrt{D}}, \quad n \in Z .$$

then
$$x_{-n} = \frac{\mu^{-2n-1} + \overline{\mu}^{-2n-1}}{2^{-n}} = -\frac{\mu^{-2n-1} + \overline{\mu}^{-2n-1}}{2^{n+1}(\mu\overline{\mu})^{-2n-1}}$$

$$= -\frac{\mu^{2n+1} + \overline{\mu}^{2n+1}}{2^{n+1}} = -x_{n+1},$$

$$y_{-n} = \frac{\mu^{-2n-1} - \overline{\mu}^{-2n-1}}{2^{-n}\sqrt{D}} = -\frac{\mu^{-2n-1} - \overline{\mu}^{-2n-1}}{2^{n+1}(\mu\overline{\mu})^{-2n-1}\sqrt{D}}$$

$$= \frac{\mu^{2n+1} - \overline{\mu}^{2n+1}}{2^{n+1}\sqrt{D}} = y_{n+1}.$$

By the preliminary proposition (3) about Pell equation, such defined (x_n, y_n) are all positive integers when $n > 0$.

So such defined (x_n, y_n) are all integers when $n \in Z$.

Define again

$a_n = \frac{\mu^n + \bar{\mu}^n}{2}$, $b_n = \frac{\mu^n - \bar{\mu}^n}{2\sqrt{D}}$, $\forall n \in Z$. It is easy to verify this definition satisfies the recursion formula $\begin{cases} a_{m+n} = a_m a_n + D b_m b_n \\ b_{m+n} = a_m b_n + a_n b_m \end{cases}$, $\forall m, n \in Z$.

Here a_n, b_n do not need to be integers.

But a_n, b_n must be an integral power of 2 times by a integer, this is because:

Obviously, when $n \geq 0$, a_n, $b_n \in Z$,

But
$$a_{-n} = \frac{\mu^{-n} + \bar{\mu}^{-n}}{2} = \frac{\mu^{-n} + \bar{\mu}^{-n}}{2(\text{-}2)^n (\mu\bar{\mu})^{-n}} = \frac{\mu^n + \bar{\mu}^n}{(\text{-}1)^n 2^{n+1}} = 2^{-n}\left[(\text{-}1)^n a_n\right],$$
$$b_{-n} = \frac{\mu^{-n} - \bar{\mu}^{-n}}{2\sqrt{D}} = \frac{\mu^{-n} - \bar{\mu}^{-n}}{2(\text{-}2)^n (\mu\bar{\mu})^{-n}\sqrt{D}} = \frac{\mu^n - \bar{\mu}^n}{(\text{-}2)^{n+1}\sqrt{D}} = 2^{-n}\left[(\text{-}1)^{n+1} b_n\right],$$

So for $\forall n \in Z$, a_n, b_n can be represented as an integral power of 2 times by a integer.

Without losing generality, we can assume $a_n = 2^{k_n} \cdot c_n$, $b_n = 2^{l_n} \cdot d_n$, c_n, $d_n \in Z$ and they are both odd, k_n, $l_n \in Z$.

For a fixed odd integer t, we define $t \mid a_n$ if $t \mid c_n$, $t \mid b_n$ if $t \mid d_n$.

Since $b_{n+r} = a_n b_r + a_r b_n$, and $\exists\ N$ that is large enough such that $2^N \cdot b_{n+r}$, $2^N \cdot a_n b_r$, $2^N \cdot a_r b_n$ are all integers.

Thus, when $t \mid a_r$, by $2^N \cdot b_{n+r} = 2^N a_n b_r + 2^N a_r b_n$, $t \mid c_r$ and $2^N \cdot 2^{k_r} \cdot b_n \in Z$,

$2^N a_r b_n = (2^N \cdot 2^{k_r} \cdot b_n) c_r$

So we have $2^N b_{n+r} \equiv 2^N a_n b_r \pmod{t}$

So $t \mid b_{n+r} \Leftrightarrow t \mid a_n b_r$.

In parallel, from $a_{n+r} = a_n a_r + D b_n b_r$ we can also obtain

when $t \mid a_r$, $t \mid a_{n+r} \Leftrightarrow t \mid D b_n b_r$.

thus， when $t \mid a_r$, $t \mid a_{n+r} \Leftrightarrow t \mid D b_n b_r \Leftrightarrow t \mid D b_r^2 a_{n-r} \Leftrightarrow t \mid a_{n-r}$. （The last equivalence is because $a_r^2 - D b_r^2 = (-2)^r$,so $t \mid a_r$, $(t,(-2)^r) = 1 \Rightarrow (t, D b_r^2) = 1$.）

Assume $a_{f(t)}$ is the term with minimal positive integral index among the terms dividable by t , for $\forall n$ such that $t \mid a_n$, denote $n = 2kf(t) + r_0$, $-f(t) < r_0 \le f(t)$. By the discussion above we know that $t \mid a_n \Leftrightarrow t \mid a_{r_0}$.

when $r_0 > 0$, by the requirement of $f(t)$ we must have $r_0 = f(t)$.

when $r_0 = 0$, $a_{r_0} = a_0 = 1$, it is impossible.

when $r_0 < 0$, $a_{r_0} = 2^{r_0}(-1)^{r_0} a_{-r_0}$ so $t \mid a_{r_0} \Leftrightarrow t \mid a_{-r_0}$. and $0 < -r_0 < f(t)$, this will lead to a contradiction to the requirement of $f(t)$.

so $t \mid a_n \Leftrightarrow r_0 = f(t) \Leftrightarrow \dfrac{n}{f(t)} = 2k+1$ is a positive odd integer. Thus we have proven, either odd integers t cannot divide any a_n , or $\exists$ $f(t) \in N^*$ such that $t \mid a_n \Leftrightarrow \dfrac{n}{f(t)}$ is a positive odd integer. Now notice that $x_n = 2^{-(n-1)} a_{2n-1}$, so $t \mid x_n \Leftrightarrow t \mid a_{2n-1}$.

Thus we have proven either the odd integer t cannot divide any x_n , or $\exists$ $f(t) \in N^*$ such that

$t \mid x_n \Leftrightarrow f(t) \mid 2n-1$. The proof of corresponding result about y_n is parallel. □

Proof of theorem 2(3) can be obtained with minor changes in proofs of theorem 2.(1) and 2.(2).

6. Applications of Theorem 2

Recall that in Example 5 in section 4 we have proven $3^{2n+1}=2y^2+1$ has no solutions when 2n+1 is a composite number, so the only situation left unsolved is when 2n+1 is prime. Now by theorem 2, let's give a general proof that does not need to discuss whether 2n+1 is composite or prime.

Example 6 The Diophantine equation $3^{2n+1}=2y^2+1$ .has no positive integral solutions other than n=2，y=11.

Proof：We turn the equation into a quasi-Pell equation：$(2y)^2-6\cdot(3^n)^2=-2$. Thus the problem is turned to：among the solutions (x_n,y_n) of $X^2-6Y^2=-2$, how many y_n is 3's power.

We write out the first few terms: $y_1=1$， $y_2=9$， $y_{n+1}=10y_n-y_{n-1}$.

Such we have got $y_n=3^0$， 3^2 are both possible. Now we care about the cases $y_n=3^\alpha$， $\alpha\geq 3$. If such y_n exists, it must be multiples of 27，then by theorem 8，$\exists g(27)\in N^*$ such that $27\mid y_n \Leftrightarrow g(27)\mid 2n-1$.

So now we need to fix $g(27)$， or equivalently, to find the index of the first term in $\{y_n\}$ that is dividable by 27.

Compute $y_3=89$， $y_4=881$， $y_5=8721=27\times17\times19$， so $g(27)=5$.

However, notice that for 17 ， there also $\exists g(17)\in N^*$ such that $17\mid y_n \Leftrightarrow g(17)\mid 2n-1$. So $17\mid y_5 \Rightarrow g(17)\mid 5$.

Thus now for $\forall y_n=3^\alpha$， $\alpha\geq 3$， by $27\mid y_n$ we have $g(27)=5\mid 2n-1$. Since $g(17)\mid 5$， so $g(17)\mid 2n-1 \Rightarrow 17\mid y_n$， this contradicts to $y_n=3^\alpha$.

So we have $y_n=3^\alpha$， $\alpha\geq 3$ is impossible.

Thus among the solutions (x_n, y_n) of $X^2 - 6Y^2 = -2$, there are only two y_n's such that y_n is 3's power: $y_n = 3^0$, 3^2. So all the non-negative solutions of $3^{2n+1} = 2y^2 + 1$ are $(n, y) = (0,1)$, $(2,11)$. □

Example 7 When $n \neq 2^{\alpha}, n \neq 2^{\alpha} \cdot 5$, the Diophantine equation $3^{2n} = 2y^2 + 1$ has no positive integral solutions.

Proof: $3^{2n} + y^4 = (y^2 + 1)^2$, By results of Pythagoras equation, $\exists a, b$ with one odd and one even, $a > b$, such that $3^n = a^2 - b^2$, $y^2 = 2ab$, $y^2 + 1 = a^2 + b^2$.

so $a^2 + b^2 = 1 + 2ab$, $a - b = 1$

so $3^n = 2b + 1$, $y^2 = 2b(b+1)$.

When b is even, $(2b, b+1) = 1$, so $2b = u^2, b+1 = v^2$, $y = uv$, $3^n - u^2 = 1$.

so u is even, by modulo 4 we can see n is even, so we have $\left(3^{\frac{n}{2}}\right)^2 - u^2 = 1$, this equation has no positive integral solution.

When b is odd, $(2(b+1), b) = 1$, so $2(b+1) = u^2$, $b = v^2$, $y = uv$,

$3^n = 2v^2 + 1$. Thus from $3^{2n} = 2y^2 + 1$ we obtain $3^n = 2v^2 + 1$, repeat this procedure for finitely many steps we will get $3^{\frac{2n}{2^{\alpha}}} = w^2 + 1$, such that $\frac{2n}{2^{\alpha}}$ is odd. By the hypothesis, n is neither 2's power nor 2's power times 5, so $\frac{2n}{2^{\alpha}}$ is an odd integer other than 5, then by Example 7, the equation has no positive integral solutions.

Finally, we list results we have got for the Diophantine equation $x^m - 2y^n = 1$ as follows:

1. When m=n=2, it has infinitely many solutions, the minimal solution is (3,2),

general solutions can be given by $x_n + \sqrt{2} y_n = (3 + 2\sqrt{2})^n$.

2. When m=p or 2p, n is even, the positive integral solution (x, y) $(x > 3)$ of the equation must satisfy $p \mid y$.
3. When m is odd; or m is even but not type of $2^{\alpha}, 2^{\alpha} \cdot 5$, n is even, there is not integral solution for the equation such that $x = 3$.

Bibliography

[1]柯召 孙琦 K. Zhao, Q. Sun *谈谈不定方程* 上海：上海教育出版社 1980.8

[2]曹珍富 Z.F. Cao *丢番图方程引论* 哈尔滨：哈尔滨工业大学出版社 1989.2