

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 Catalan 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、Catalan 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 Catalan 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, Catalan Conjecture

1. 准备知识.

首先我们列出关于 Pell 方程解的一些基本结论

(1) $x^2 - Dy^2 = 1$ ($D > 0$ 且不含平方因子) 称为正 Pell 方程或标准 Pell 方程, 它总有一组最小正解 (x_1, y_1) , 且所有解 (x_n, y_n) 由 $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$ 决定,

$$\left(\text{或 } x_n = \frac{\lambda^n + \bar{\lambda}^n}{2}, y_n = \frac{\lambda^n - \bar{\lambda}^n}{2\sqrt{D}}, \text{ 其中 } \lambda = x_1 + y_1\sqrt{D}, \bar{\lambda} = x_1 - y_1\sqrt{D}\right)$$

$$\text{并有递推公式 } \begin{cases} x_n = x_{n-1}x_1 + Dy_{n-1}y_1 \\ y_n = x_{n-1}y_1 + y_{n-1}x_1 \end{cases} (n \geq 2)$$

$$\text{以及衍生公式 } \begin{cases} x_{m+n} = x_m x_n + Dy_m y_n \\ y_{m+n} = x_m y_n + y_m x_n \end{cases} (m, n \in \mathbb{N}^*).$$

若定义 $x_0 = 1, y_0 = 0, x_{-n} = x_n, y_{-n} = -y_n$, 则以上两个递推公式的下标范围可推广到整个 \mathbb{Z} .

(2) $x^2 - Dy^2 = -1$, 称为负 Pell 方程. 它如果有解, 则必有无穷多解. 设 (a_1, b_1) 是其最小正解, 则通解 (a_n, b_n) 由 $a_n + b_n\sqrt{D} = (a_1 + b_1\sqrt{D})^{2n-1}$ 决定, (或

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

且有 $(a_1 + b_1\sqrt{D})^2 = x_1 + y_1\sqrt{D}$ (依记号, x_1, y_1 为正 Pell 方程的基本解).

(3) $x^2 - Dy^2 = K, |K| > 1$, 称为类 Pell 方程. 它如果有解, 就一定有无穷多解. 特别当 $|K|=2$ 时, 若记最小解为 (u_1, v_1) 则通解 (u_n, v_n) 由

$$u_n + v_n\sqrt{D} = \frac{(u_1 + v_1\sqrt{D})^{2n-1}}{2^{n-1}} \text{ 决定 (或 } u_n = \frac{\xi^{2n-1} + \bar{\xi}^{2n-1}}{2^n}, v_n = \frac{\xi^{2n-1} - \bar{\xi}^{2n-1}}{2^n\sqrt{D}}, \text{ 其中}$$

$$\xi = u_1 + v_1\sqrt{D}, \bar{\xi} = u_1 - v_1\sqrt{D})$$

$$(4) \text{ 无论何种 Pell 方程, 递推式 } \begin{cases} x_{m+n} = x_m x_n^* + Dy_m y_n^* \\ y_{m+n} = x_m y_n^* + y_m x_n^* \end{cases} \text{ 总成立.}$$

其中 (x_n, y_n) 与 (x_n^*, y_n^*) 分别表示 $x^2 - Dy^2 = K$ 和 $x^2 - Dy^2 = 1$ 的第 n 组正解.

2. 主定理

本文将得到这样的两个主要定理

定理 1 (1)对标准 Pell 方程 $x^2 - Dy^2 = 1$, 设 d 为 D 的大于 3 的因子

且 $(y_1, d) = 1$, 则 $d^k \square y_n \Leftrightarrow d^k \square n$ ($n \in N^*$, $k \in N$. 记号“ \square ”表示: 若 $b^a \mid a$, 且 $b^{a+1} \nmid a$, 则称 b^a 恰整除 a , 记为 $b^a \square a$.)

(2) 对 (I) 负 Pell 方程 $x^2 - Dy^2 = -1$,

(II) 类 Pell 方程 $x^2 - Dy^2 = \pm 2, -4$,

(III) 类 Pell 方程 $x^2 - Dy^2 = 4$.

有类似的结论成立, 即:

(I) 型方程中, 若 $d \mid D$ 且 $(d, y_1) = 1$, $d > 3$, 则 $d^k \square y_n \Leftrightarrow d^k \square 2n - 1$.

(II) 型方程中, 若 $d \mid D$ 且 $(d, y_1) = 1$, $d > 3$, 且 d 是奇数, 则 $d^k \square y_n \Leftrightarrow d^k \square 2n - 1$.

(III) 型方程中, 若 $d \mid D$ 且 $(d, y_1) = 1$, $d > 3$, 且 d 是奇数, 则 $d^k \square y_n \Leftrightarrow d^k \square n$.

(3)特别地, 对于标准 pell 方程 $x^2 - Dy^2 = 1$, 进一步还有: 设基本解为 (x_1, y_1) ,

$d \mid D$, $d > 3$. 设 $d^\alpha \square y_1$, 那么如果 $(d, \frac{y_1}{d^\alpha}) = 1$, 则 $d^{\alpha+k} \square y_n \Leftrightarrow d^k \square n$.

注: 在(2)中的 (I) 型方程中, $2 \mid d$ 且 $k > 0$ 的情况是不可能出现的, 因为这将有

$2 \mid y_n \Rightarrow 4 \mid Dy_n^2 \Rightarrow x_n^2 \equiv -1 \pmod{4}$, 矛盾. 所以此时 d 一定是奇数.

定理 2 (1) 标准 Pell 方程 $x^2 - Dy^2 = 1$ 的全部解记为 (x_n, y_n) , 则 $\forall t \in N^*$, 以下(i), (ii)情况必有其一发生; (iii), (iv)情况也必有其一发生:

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

(ii) \exists 由 t 唯一决定的 $f(t) \in N^*$, 使 $t \mid x_n \Leftrightarrow \frac{n}{f(t)}$ 为正奇数.

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

(iv) \exists 由 t 唯一决定的 $g(t) \in N^*$, 使 $t \mid y_n \Leftrightarrow g(t) \mid n$.

(2) $x^2 - Dy^2 = -2$, 所有正整数解记为 (x_n, y_n) , 对 \forall 奇数 t , (i) (ii)两种情况必发生其一; (iii)(iv)两种情况也必发生其一.

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

(ii) \exists 由 t 唯一决定的 $f(t) \in N^*$, 使 $t \mid x_n \Leftrightarrow f(t) \mid 2n-1$.

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

(iv) \exists 由 t 唯一决定的 $g(t) \in N^*$, 使 $t \mid y_n \Leftrightarrow g(t) \mid 2n-1$.

(3)更一般地, 我们可以得到:

对给定的 $t \in N^*$, 称结论 (I) 为: 或者不 $\exists x_n$ 使 $t \mid x_n$, 或者 $\exists f(t) \in N^*$ 使 $t \mid x_n \Leftrightarrow n = (2k-1)f(t)$, $k \in N^*$; 或者不 $\exists y_n$ 使 $t \mid y_n$, 或者 $\exists g(t) \in N^*$ 使 $t \mid y_n \Leftrightarrow n = kg(t)$, $k \in N^*$.

称结论 (II) 为: 或者不 $\exists x_n$ 使 $t \mid x_n$, 或者 $\exists f(t) \in N^*$ 使 $t \mid x_n \Leftrightarrow 2n-1 = kf(t)$, $k \in N^*$; 或者不 $\exists y_n$ 使 $t \mid y_n$, 或者 $\exists g(t) \in N^*$ 使 $t \mid y_n \Leftrightarrow 2n-1 = kg(t)$, $k \in N^*$.

则有结论:

(i) 对 $x^2 - Dy^2 = 1$, 满足结论 (I).

(ii) 对 $x^2 - Dy^2 = -1$, 满足结论 (II) .

(iii) 对 $x^2 - Dy^2 = \pm 2$, 满足限定 t 为奇数的结论 (II) .

(iv) 对 $x^2 - Dy^2 = \pm 4$, 满足限定 t 为奇数的结论 (I)

本文将按以下方式编排：第 3 节将证明定理 1，第 4 节则将给出定理 1 的几个应用；第 5 节将证明定理 2，第 6 节则将给出定理 2 的应用。在第 4、6 节的应用中，将得出推广了的 Catlan 猜想的部分情形的讨论结果。

3. 定理 1 的证明

定理 1.(1)显然是 1.(3)的推论，所以先来证明 1.(3)

定理 1.(3)的证明分为三个部分

标准 Pell 方程 $x^2 - Dy^2 = 1$ ，设 d 为 D 的大于 3 的因子且 $d^\alpha \square y_1$ ，

$$(d, \frac{y_1}{d^\alpha}) = 1 (\alpha \in N).$$

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

因为
$$y_n = \frac{(x_1 + \sqrt{D}y_1)^n - (x_1 - \sqrt{D}y_1)^n}{2\sqrt{D}} = C_n^1 \cdot x_1^{n-1} y_1 + C_n^3 \cdot x_1^{n-3} y_1^3 \cdot D + \dots$$

$$\equiv n x_1^{n-1} y_1 \pmod{d^{\alpha+1}}$$

而由原方程知 $(x_1, d) = 1$ ，再由 $(d, y_1) = d^\alpha$ 即得此结论.

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

若不然，设 $d^{\alpha+2} | y_d = d x_1^{d-1} y_1 + C_d^3 x_1^{d-3} y_1^3 D + \dots$

则
$$d^{\alpha+2} | d x_1^{d-1} y_1 + \frac{d(d-1)(d-2)}{6} x_1^{d-3} y_1^3 D + \dots$$

$$d^{\alpha+1} | x_1^{d-1} y_1 + \frac{D(d-1)(d-2)}{6} x_1^{d-3} y_1^3 + \dots$$

若 $3 \nmid d$ ，则 $3 \mid (d-1)(d-2)$ ， $2 \mid (d-1)(d-2)$

所以 $6 \mid (d-1)(d-2)$

所以 $d^{\alpha+1} \mid D \cdot \frac{(d-1)(d-2)}{6} x_1^{d-3} y_1^3 \Rightarrow d^{\alpha+1} \mid x_1^{d-1} y_1$ ，矛盾。

若 $3 \mid d$ ，则设 $d = 3d_1$ ，所以 $d_1 > 1$

所以 $d_1^{\alpha+1} \mid x_1^{d-1} y_1 + \frac{D(d-1)(d-2)}{3} x_1^{d-3} y_1^3 + \dots \Rightarrow d_1^{\alpha+1} \mid x_1^{d-1} y_1$ 但 $(x_1 y_1, d^\alpha) = d^\alpha$

且 $d_1 > 1$ ，矛盾。于是 (ii) 成立。

(iii) 下面直接证明定理

由基本结论 (4)， $\begin{cases} y_{2d} = 2x_d y_d \equiv 2x_d y_d \pmod{d^{2\alpha+3}} \\ x_{2d} = x_d^2 + D y_d^2 \equiv x_d^2 \pmod{d^{2\alpha+3}} \end{cases}$ 一般地，设已证

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

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

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

所以 $d \nmid n$ 时自然有 $d^{\alpha+2} \nmid y_{nd}$ ，否则 $d^{\alpha+2} \mid nx_d^{n-1} y_d \Rightarrow d \mid nx_d^{n-1}$ 。

由 $(d, x_n) = 1 \Rightarrow d \mid n$ ，矛盾。这也顺便证明了 $d \mid n$ 时 $d^{\alpha+2} \mid y_{nd} \cdot d^{\alpha+2} \square y_{d^2}$ 。

所以 $d^{\alpha+2} \mid y_n \Leftrightarrow d^2 \mid n$ ， $d^{\alpha+2} \square y_{d^2}$ 。

一般地，设已证明 $d^{\alpha+s} \mid y_n \Leftrightarrow d^s \mid n$ ，且 $d^{\alpha+s} \square y_{d^s}$ ， $s \in \mathbb{N}^*$ 。

$$\text{则 } \begin{cases} x_{2d^s} = x_{d^s}^2 + D y_{d^s}^2 \equiv x_{d^s}^2 \pmod{d^{2\alpha+2s+1}} \\ y_{2d^s} = 2x_{d^s} y_{d^s} \equiv 2x_{d^s} y_{d^s} \pmod{d^{2\alpha+2s+1}} \end{cases} \cdot$$

$$\text{且若已证 } \begin{cases} x_{k \cdot d^s} \equiv x_{d^s}^k \pmod{d^{2\alpha+2s+1}} \\ y_{k \cdot d^s} \equiv kx_{d^s}^{k-1} y_{d^s} \pmod{d^{2\alpha+2s+1}} \end{cases} \cdot$$

$$\begin{aligned} \text{则 } x_{(k+1)d^s} &= x_{kd^s} \cdot x_{d^s} + D \cdot y_{kd^s} \cdot y_{d^s} \equiv x_{d^s}^k \cdot x_{d^s}^s + Dx_{d^s}^k y_{d^s}^2 \\ &\equiv x_{d^s}^{k+1} \pmod{d^{2\alpha+2s+1}}. \end{aligned}$$

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

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

所以自然也有 $d^{\alpha+s+1} | y_n \Leftrightarrow s^{s+1} | n$, $d^{\alpha+s+1} \nmid y_{d^{s+1}}$.

从而由归纳原理知 $\forall k \in N^*$, $d^{\alpha+k} \nmid y_n \Leftrightarrow d^k \nmid n$. \square

定理 1. (2)的证明:

首先, $x^2 - Dy^2 = h$ 的基本解为 (x_1, y_1) , 则通解 (x_n, y_n) 由

$$x_n + y_n \sqrt{D} = \frac{(x_1 + y_1 \sqrt{D})^{a_n}}{b_n} \text{ 给出.}$$

其中当 $h = -1$ 时, $a_n = 2n - 1$, $b_n = 1$;

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

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

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

证明仍分为三个部分:

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

$$\begin{aligned} \text{因为 } y_n &= \frac{(x_1 + \sqrt{D}y_1)^{a_n} - (x_1 - \sqrt{D}y_1)^{a_n}}{2b_n \sqrt{D}} = \frac{C_{a_n}^1 \cdot x_1^{a_n-1} y_1 + C_{a_n}^3 \cdot x_1^{a_n-3} y_1^3 \cdot D + \dots}{b_n} \\ &\equiv a_n x_1^{a_n-1} y_1 \pmod{d} \end{aligned}$$

而由原方程知 $(x_1, d) = 1$, 再由 $(d, y_1) = 1$ 即得此结论.

(ii) $d \nmid y_{c_d}$

其中当 $h = -1, -4, \pm 2$ 时, $c_d = \frac{d+1}{2}$, 当 $h = 4$ 时, $c_d = d$. 则有 $a_{c_d} = d$.

若不然, 设 $d^2 \mid y_{c_d} = \frac{a_{c_d} x_1^{a_{c_d}-1} y_1 + C_{a_{c_d}}^3 x_1^{a_{c_d}-3} y_1^3 D + \dots}{b_{c_d}}$

则 $d^2 \mid dx_1^{d-1} y_1 + \frac{d(d-1)(d-2)}{6} \cdot x_1^{d-3} y_1^3 D + \dots$
 $d \mid x_1^{d-1} y_1 + \frac{D(d-1)(d-2)}{6} \cdot x_1^{d-3} y_1^3 + \dots$

若 $3 \nmid d$, 则 $3 \mid (d-1)(d-2)$, $2 \mid (d-1)(d-2)$ 所以 $6 \mid (d-1)(d-2)$

所以 $d \mid D \cdot \frac{(d-1)(d-2)}{6} \Rightarrow d \mid x_1^{d-1} y_1$, 矛盾.

若 $d^2 \mid nu_d^{n-1} v_d \Rightarrow d \mid nu_d^{n-1} \cdot 3 \mid d$, 则设 $d = 3d_1$, 所以 $d_1 > 1$

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

但 $(x_1, y_1, d) = 1$ 且 $d_1 > 1$, 矛盾. 于是 (ii) 成立.

(iii) 下面直接证明定理

记 $u_n + \sqrt{D}v_n = (x_1 + \sqrt{D}y_1)^n$, 则实际上有 $x_n = \frac{u_n}{b_n}$, $y_n = \frac{v_n}{b_n}$ u_n, v_n 满足

$\begin{cases} u_{m+n} = u_m u_n + D v_m v_n \\ v_{m+n} = u_m v_n + u_n v_m \end{cases}$ 这样, 我们由一、二步所得即 $d \mid v_n \Leftrightarrow d \mid n$, $d \nmid v_d$.

则 $\begin{cases} v_{2d} = 2u_d v_d \equiv 2u_d v_d \pmod{d^3} \\ u_{2d} = u_d^2 + D v_d^2 \equiv u_d^2 \pmod{d^3} \end{cases}$

一般地, 设已证 $\begin{cases} v_{kd} \equiv k u_d^{k-1} v_d \pmod{d^3} \\ u_{kd} \equiv u_d^k \pmod{d^3} \end{cases}$

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

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

所以有 $\begin{cases} u_{nd} \equiv u_d^n \pmod{d^3} \\ v_{nd} \equiv n u_d^{n-1} v_d \pmod{d^3} \end{cases}$

所以 $d \nmid n$ 时自然有 $d^2 \nmid v_{nd}$, 否则 $d^2 \mid nu_d^{n-1} v_d \Rightarrow d \mid nu_d^{n-1}$.

由 $(d, u_n) = 1 \Rightarrow d \mid n$, 矛盾. 这也顺便证明了 $d \mid n$ 时 $d^2 \mid v_{nd} \cdot d^2 \nmid v_{d^2}$

所以 $d^2 | v_n \Leftrightarrow d^2 | n$, $d^2 \square v_{d^2}$.

一般地, 设已证明 $d^s | v_n \Leftrightarrow d^s | n$, 且 $d^s \square v_{d^s}$,

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

$$\text{且若已证} \quad \begin{cases} u_{k \cdot d^s} \equiv u_{d^s}^k \pmod{d^{s+2}} \\ v_{k \cdot d^s} \equiv ku_{d^s}^{k-1}v_{d^s} \pmod{d^{s+2}}. \end{cases}$$

$$\begin{aligned} \text{则 } u_{(k+1)d^s} &= u_{kd^s} \cdot u_{d^s} + D \cdot v_{kd^s} \cdot v_{d^s} \equiv u_{d^s}^k \cdot u_{d^s} + Du_{d^s}^k v_{d^s}^2 \\ &\equiv u_{d^s}^{k+1} \pmod{d^{s+2}}. \end{aligned}$$

$$\begin{aligned} v_{(k+1)d^s} &= u_{kd^s} v_{d^s} + v_{kd^s} u_{d^s} \equiv u_{d^s}^k v_{d^s} + ku_{d^s}^{k-1} u_{d^s} \\ &\equiv (k+1)u_{d^s}^k v_{d^s} \pmod{d^{s+2}} \end{aligned}$$

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

所以自然也有 $d^{s+1} | v_n \Leftrightarrow d^{s+1} | n$, $d^{s+1} \square v_{d^{s+1}}$

从而由归纳原理知 $\forall k \in \mathbb{N}^*$, $d^k \square v_n \Leftrightarrow d^k \square n$.

$$\text{即 } d^k \square y_n \Leftrightarrow d^k \square a_n \quad \square$$

4. 定理 1 的应用

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

这个方程有一组显然的解 $x=5$, $n=0$. 假设 (x, n) 是一组使 $n > 0$ 的适合 $x^2 - 24^{2n+1} = 1$ 的非负整数解, 则在 Pell 方程 $x^2 - 24y^2 = 1$ 中, 设 $y_m = 24^n, n > 0$, 则 $24^n \square y_m \Leftrightarrow 24^n \square m$. 所以 $y_m \geq y_{24^n}$.

$$\begin{aligned} \text{注意 } y_{24^n} &= C_{24^n}^1 \cdot 5 + C_{24^n}^3 \cdot 5^3 \cdot 24 + \dots \\ &\geq 5 \cdot 24^n > 24^n = y_m \end{aligned}$$

这是一个矛盾.

故此方程除 $(x, n) = (5, 0)$ 外无其它非负整数解.

这个例子可以直接推广到下面的结果:

$$x^2 - (a^2 - 1)^{2n+1} = 1 \quad (a > 2 \text{ 给定}, x, n \text{ 为变量}) \text{ 无非负整数解.}$$

更一般的想法是 $x^2 - y^{2n+1} = 1$ 有无使 $n=0$ 以外的非负整数解, 这里只能得到一个不完整的结果.

例 2 $x^2 - y^{2n+1} = 1$ ($n > 0$) 在 $2n+1 = p$ 为素数的情况下, 必有 $2 \mid y$, $p \mid x$.

证明: 先证 $2 \mid y$. 否则 $2 \nmid y$, 则有 $2 \mid x$. 所以 $x+1$, $x-1$ 均为奇数.

$$\text{移项有 } (x+1)(x-1) = y^{2n+1}, \text{ 且 } (x+1)(x-1) = y^{2n+1}$$

$$\text{所以 } \begin{cases} x+1 = u^{2n+1} \\ x-1 = v^{2n+1} \end{cases} \Rightarrow u^{2n+1} - v^{2n+1} = 2. \text{ 所以 } u-v \mid u^{2n+1} - v^{2n+1} = 2.$$

$$\text{又 } u, v \text{ 同奇偶 所以 } u = v+2. \text{ 所以 } (v+2)^{2n+1} - v^{2n+1} \geq 2^{2n+1} > 2. \text{ 矛盾.}$$

所以 $2 \mid y$.

$$\text{由原方程移项 有 } x^2 = (y+1)(y^{p-1} - y^{p-2} + \dots + 1).$$

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

若 $p|y+1$ 则 $p|x^2 \Rightarrow p|x$ 结论成立.

下设 $p \nmid y+1$ 所以 $(y+1, y^{p-1} - y^{p-2} + \dots + 1) = 1$.

所以 $\begin{cases} y+1 = a^2 \\ y^{p-1} - y^{p-2} + \dots + 1 = b^2 \end{cases}$ 因为 $y \geq 2$ 且 $2|y$ 所以 $y \geq 8, a > 2$.

原方程化为 $x^2 - (a^2 - 1)^{2n+1} = 1 \quad (a > 2)$

由例 1 的推广知其无 $n > 0$ 的非负整数解. 矛盾. \square

事实上 $x^2 - y^{2n+1} = 1$ 这个方程是 Catalan 猜想的特例: 不定方程 $x^a - y^b = 1$ 对于大于 1 的正整数 x, y, a, b 只有唯一解 $x=3, y=2, a=2, b=3$. 这已在 2002 年被 Preda Mihăilescu 证明.

下面进一步用定理 1 处理 Catalan 猜想的推广: 不定方程 $x^m - 2y^n = 1$. 当 $m=n=2$ 时就是标准 Pell 方程 $x^2 - 2y^2 = 1$, 已经知道有无穷多解, 最小解为 $(3, 2)$, 通解可以由 $x_n + \sqrt{2}y_n = (3 + 2\sqrt{2})^n$ 给出.

当 $m=p$ 或 $2p, p$ 为奇素数的时候, 下面的几个例子给出了这个方程的解的一些必要条件.

例 3 $x^p - 2y^2 = 1 \quad (x > 3)$ (p 为奇素数) 的任何一组正整数解必满足 $p|y$.

证明: $(x^p - 1)(x^{p-1} + \dots + 1) = 2y^2$

$$x^{p-1} + \dots + 1 \equiv p \pmod{(x-1)}$$

若 $p|x-1$, 则显然 $p|y$.

若 $p \nmid x-1$, 则 $(x-1, x^{p-1} + \dots + 1) = 1$.

又 x 为奇数, 故 $x^{p-1} + \dots + 1$ 也为奇数,

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

方程化为 $(2b^2 + 1)^p - 2y^2 = 1$, 即 $(2y, (2b^2 + 1)^{\frac{p-1}{2}})$ 是类 Pell 方程 $X^2 - 2(2b^2 + 1)Y^2 = -2$ 的解.

此方程的最小解为 $(X_1, Y_1) = (2b, 1)$, 设 $(2y, (2b^2 + 1)^{\frac{p-1}{2}}) = (X_n, Y_n)$,

则由定理 1.(2) 知 $(2b^2 + 1)^{\frac{p-1}{2}} \square n$, 于是 $n \geq (2b^2 + 1)^{\frac{p-1}{2}}$

$$\text{而 } X_n + \sqrt{2(2b^2 + 1)}Y_n = \frac{(2b + \sqrt{2(2b^2 + 1)})^{2n-1}}{2^{n-1}},$$

从而 $Y_n \geq \frac{(2n-1)(2b)^{2n-2}}{2^{n-1}} > 2n-1 \geq n \geq (2b^2 + 1)^{\frac{p-1}{2}} = Y_n$, 矛盾.

所以 $p \mid x-1$, 所以 $p \mid y$. \square

完全类似地可以证明, 不定方程 $x^p - 2y^2 = -1$ ($x > 3$) (p 为奇素数) 的任何一组正整数解也必满足 $p \mid y$.

例 4 $x^{2p} - 2y^2 = 1$ ($x > 3$) (p 为奇素数) 的任何一组正整数解必满足 $p \mid y$.

证明: $x^{2p} + y^4 = (y^2 + 1)^2$, 且 x 奇 $\Rightarrow x^{2p} \equiv 1 \pmod{8}$, 所以 y 为偶数.

由勾股方程的结果, $\exists a, b$ 一奇数一偶数, $a > b$, 满足 $x^p = a^2 - b^2$, $y^2 = 2ab$, $y^2 + 1 = a^2 + b^2$.

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

所以 $x^p = 2b + 1$, $y^2 = 2b(b + 1)$.

当 b 为奇数时, $(2(b+1), b) = 1$, 所以 $2(b+1) = u^2$, $b = v^2$, $y = uv$,

$x^p - 2v^2 = 1$, 由例 3, $p \mid v$ 所以 $p \mid y$.

当 b 为偶数时, $(2b, (b+1)) = 1$, 所以 $2b = u^2$, $(b+1) = v^2$, $y = uv$,

$x^p - 2v^2 = -1$, 由例 3 后的注, $p \mid v$ 所以 $p \mid y$. \square

例 5 不定方程 $3^{2n+1} - 2y^2 = 1$ 在 $2n+1$ 为合数时无正整数解.

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

引理的证明: 对 $m > n$ 作辗转相除法, $m = q_1 n + r_1$

$$n = q_2 r_1 + r_2$$

...

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

...

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

则 $r_{s+1} = (m, n)$.

$$\begin{aligned} \text{有} \quad & (a^m - 1, a^n - 1) \\ &= ((a^m - 1) - (a^n - 1), a^n - 1) \\ &= (a^m - a^n, a^n - 1) \\ &= (a^n (a^{m-n} - 1), a^n - 1) \\ &= (a^{m-n} - 1, a^n - 1) \\ &= \dots = (a^{m-q_1 n} - 1, a^n - 1) = (a^n - 1, a^{r_1} - 1) \end{aligned}$$

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

引理证毕.

回到例 5. 记 $2n+1$ 的素因子为 p_1, p_2, \dots, p_k . 因为 $2n+1$ 为合数,

所以 $\forall 1 \leq i \leq k$,

$$p_i < 2n+1. \text{ 而 } \left(3^{\frac{2n+1}{p_i}} - 2y^2 = 1 \right)^{p_i}. \text{ 由于 } 3^{\frac{2n+1}{p_i}} > 3, \text{ 及例 3 结论知 } \forall 1 \leq i \leq k,$$

$$p_i \mid y.$$

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

不妨设 p_1 为 $2n+1$ 的最小素因子, 则 p_1 为大于 1 的奇数, 且有

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

由引理, $p_1 \mid 3^{(2n+1, p_1-1)} - 1.$

注意到 $p_1 - 1$ 的每个素因子都小于 p_1 , 不能整除 $2n+1$, 所以 $p_1 - 1$ 与 $2n+1$ 互素.

所以 $(2n+1, p_1-1) = 1, \quad p_1 \mid 3-1 = 2,$ 矛盾.

这就证明了 $2n+1$ 为合数时 $3^{2n+1} - 2y^2 = 1$ 无正整数解. \square

5. 定理 2 的证明

定理 2.(1)标准 Pell 方程 $x^2 - Dy^2 = 1$ 的全部解记为 (x_n, y_n) , 则 $\forall t \in N^*$,

以下(i), (ii)情况必有其一发生; (iii), (iv)情况也必有其一发生:

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

(ii) \exists 由 t 唯一决定的 $f(t) \in N^*$, 使 $t \mid x_n \Leftrightarrow \frac{n}{f(t)}$ 为正奇数.

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

(iv) \exists 由 t 唯一决定的 $g(t) \in N^*$, 使 $t \mid y_n \Leftrightarrow g(t) \mid n$.

证明: 首先, 将 (x_n, y_n) 补全, 把下标由 N^* 扩充到 Z . 定义

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

直接由定义验证知 $\begin{cases} x_{m+n} = x_m x_n + D y_m y_n \\ y_{m+n} = x_m y_n + y_m x_n \end{cases} (\forall m, n \in Z).$

而且若记 $\lambda = x_1 + \sqrt{D}y_1$, $\bar{\lambda} = x_1 - \sqrt{D}y_1$, 则

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

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

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

有了这些准备后进入定理的证明.

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

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

对取定的 $r \in N^*$, 设 $n = 2kr + r_0$, $-r < r_0 \leq r$.

则有 $x_n \equiv (Dy_r^2)^k x_{r_0} \pmod{x_r} \equiv (Dy_r^2)^k x_{|r_0|} \pmod{x_r}$. $0 \leq r_0 \leq r$.

(因为 $x_{r_0} = x_{-r_0} = x_{|r_0|}$)

这样, 对 $\forall t \in N^*$ 使 $\exists \{x_n\}$ 中某项能被 t 整除, 记其中下标为正整数的被 t 整除的最小项为 $x_{f(t)}$, 则 $(t, Dy_{f(t)}^2) = 1$. 在刚才的同余式中令 $r = f(t)$, 则有 $t | x_n \Leftrightarrow t | x_{|r_0|}$. 而 $0 \leq r_0 \leq f(t)$, $x_0 = 1$ 必不被 p 整除, 由 $f(t)$ 的选取必有 $|r_0| = f(t)$, 即 $n = (2k \pm 1)f(t)$. 即 $\frac{n}{f(t)}$ 为正奇数.

充要性的另一面也容易同样给出证明.

对 y_n 时的结论: 或 $\forall n \in N^*$, $t \nmid y_n$; 或 $\exists g(t) \in N^*$, 使 $t | y_n \Leftrightarrow g(t) | n$.

由 $y_{n+r} = y_n x_r + x_n y_r \equiv x_r y_n \pmod{y_r}$ 可立得若 $n = kr + r_0$, $0 \leq r_0 < r$,

则 $y_n \equiv (x_r)^k y_{r_0} \pmod{y_r}$. 这样仍取 $y_{g(t)}$ 为被 t 整除的项中具有最小正整数下标者, 上式中令 $r = g(t)$ 得 $t | y_n \Leftrightarrow t | y_{r_0}$, 由 $g(t)$ 的选取, 必有 $r_0 = 0$, 即 $g(t) | n$.

充要性的另一面同样容易证明. \square

定理 2.(1) 实际上说明了这样的事实: $x^2 - Dy^2 = 1$ 的解 (x_n, y_n) , $\{x_n\}$, $\{y_n\}$ 中被任何一个给定的正整数 t 整除的项的下标, 都是一个由 t 决定的整数 $f(t)$ “生成的” ..

定理 2.(2) $x^2 - Dy^2 = -2$, 所有正整数解记为 (x_n, y_n) , 对 \forall 奇数 t , (i) (ii) 两种情况必发生其一; (iii)(iv) 两种情况也必发生其一.

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

(ii) \exists 由 t 唯一决定的 $f(t) \in N^*$, 使 $t | x_n \Leftrightarrow f(t) | 2n-1$.

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

(iv) \exists 由 t 唯一决定的 $g(t) \in N^*$, 使 $t | y_n \Leftrightarrow g(t) | 2n-1$.

证明：记基本解为 (x_1, y_1) ， $\mu = x_1 + \sqrt{D}y_1$ ，

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

则

$$\begin{aligned} x_{-n} &= \frac{\mu^{-2n-1} + \bar{\mu}^{-2n-1}}{2^{-n}} = -\frac{\mu^{-2n-1} + \bar{\mu}^{-2n-1}}{2^{n+1}(\mu\bar{\mu})^{-2n-1}} \\ &= -\frac{\mu^{2n+1} + \bar{\mu}^{2n+1}}{2^{n+1}} = -x_{n+1}, \\ y_{-n} &= \frac{\mu^{-2n-1} - \bar{\mu}^{-2n-1}}{2^{-n}\sqrt{D}} = -\frac{\mu^{-2n-1} - \bar{\mu}^{-2n-1}}{2^{n+1}(\mu\bar{\mu})^{-2n-1}\sqrt{D}} \\ &= \frac{\mu^{2n+1} - \bar{\mu}^{2n+1}}{2^{n+1}\sqrt{D}} = y_{n+1}. \end{aligned}$$

而由关于 Pell 方程的基本结论(3)，这样定义的 (x_n, y_n) 在 $n > 0$ 时均为正整数，

所以这样定义的 (x_n, y_n) 在 $n \in \mathbb{Z}$ 时就均为整数了.重新另定义

$$a_n = \frac{\mu^n + \bar{\mu}^n}{2}, \quad b_n = \frac{\mu^n - \bar{\mu}^n}{2\sqrt{D}}, \quad \forall n \in \mathbb{Z}. \text{ 容易验证这个定义满足递推式}$$

$$\begin{cases} a_{m+n} = a_m a_n + D b_m b_n, \\ b_{m+n} = a_m b_n + a_n b_m \end{cases}, \quad \forall m, n \in \mathbb{Z}. \quad \text{这里的 } a_n, b_n \text{ 未必是整数.}$$

但是 a_n, b_n 一定是 2 的整数幂乘上一个整数，这是由于：显然， $n \geq 0$ 时 $a_n, b_n \in \mathbb{Z}$ ，

而

$$\begin{aligned} a_{-n} &= \frac{\mu^{-n} + \bar{\mu}^{-n}}{2} = \frac{\mu^{-n} + \bar{\mu}^{-n}}{2(-2)^n(\mu\bar{\mu})^{-n}} = \frac{\mu^n + \bar{\mu}^n}{(-1)^n 2^{n+1}} = 2^{-n} [(-1)^n a_n], \\ b_{-n} &= \frac{\mu^{-n} - \bar{\mu}^{-n}}{2\sqrt{D}} = \frac{\mu^{-n} - \bar{\mu}^{-n}}{2(-2)^n(\mu\bar{\mu})^{-n}\sqrt{D}} = \frac{\mu^n - \bar{\mu}^n}{(-2)^{n+1}\sqrt{D}} = 2^{-n} [(-1)^{n+1} b_n], \end{aligned}$$

所以 $\forall n \in \mathbb{Z}$ ， a_n, b_n 都可表为 2 的整数幂乘上一个整数的形式.

不妨设 $a_n = 2^{k_n} \cdot c_n$ ， $b_n = 2^{l_n} \cdot d_n$ ， $c_n, d_n \in \mathbb{Z}$ 且均为奇数， $k_n, l_n \in \mathbb{Z}$. 我

们对一个奇数 t ，称 $t|a_n \Leftrightarrow t|c_n$ ， $t|b_n \Leftrightarrow t|d_n$. 由 $b_{n+r} = a_n b_r + a_r b_n$ ， \exists 一个足

够大的 N 使 $2^N \cdot b_{n+r}$ ， $2^N \cdot a_n b_r$ ， $2^N \cdot a_r b_n$ 均为整数.

所以 当 $t|a_r$ 时，由 $2^N \cdot b_{n+r} = 2^N a_n b_r + 2^N a_r b_n$

因为 $t \mid c_r$ 而 $2^N \cdot 2^{k_r} \cdot b_n \in Z$, $2^N a_r b_n = (2^N \cdot 2^{k_r} \cdot b_n) c_r$

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

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

同样地, 由 $a_{n+r} = a_n a_r + D b_n b_r$ 出发也可得

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

这样, $t \mid a_r$ 时 $t \mid a_{n+r} \Leftrightarrow t \mid D b_n b_r \Leftrightarrow t \mid D b_r^2 a_{n-r} \Leftrightarrow t \mid a_{n-r}$. (最后一步是由于

$$a_r^2 - D b_r^2 = (-2)^r, \text{ 故 } t \mid a_r, (t, (-2)^r) = 1 \Rightarrow (t, D b_r^2) = 1.)$$

设被 t 整除的具有最小正整数下标的项为 $a_{f(t)}$, 对 $\forall n$ 使 $t \mid a_n$, 记 $n = 2kf(t) + r_0$,

$-f(t) < r_0 \leq f(t)$. 由刚才的讨论知 $t \mid a_n \Leftrightarrow t \mid a_{r_0}$.

$r_0 > 0$ 时由 $f(t)$ 的选取知必有 $r_0 = f(t)$.

$r_0 = 0$ 时 $a_{r_0} = a_0 = 1$, 这不可能.

$r_0 < 0$ 时, $a_{r_0} = 2^{r_0} (-1)^{r_0} a_{-r_0}$ 所以 $t \mid a_{r_0} \Leftrightarrow t \mid a_{-r_0}$. 且 $0 < -r_0 < f(t)$, 与 $f(t)$ 的选取矛盾.

所以 $t \mid a_n \Leftrightarrow r_0 = f(t) \Leftrightarrow \frac{n}{f(t)} = 2k+1$ 为正奇数. 这就证明了, 或者奇数 t 不

整除 a_n 中任何一项. 或者 $\exists f(t) \in N^*$ 使 $t \mid a_n \Leftrightarrow \frac{n}{f(t)}$ 为正奇数. 而注意

$$x_n = 2^{-(n-1)} a_{2n-1} \text{ 所以 } t \mid x_n \Leftrightarrow t \mid a_{2n-1}.$$

这就证明了, 或者奇数 t 不整除 x_n 中任何一项. 或者 $\exists f(t) \in N^*$ 使

$t \mid x_n \Leftrightarrow f(t) \mid 2n-1$. 对于 y_n 那一方面结论的证明基本同理. \square

把定理 2.(1)和定理 2.(2)的证明略作改动就可以得到定理 2.(3).

6. 定理 2 的应用

回忆在第 4 节的例 5 中我们证明了 $3^{2n+1} = 2y^2 + 1$ 当 $2n+1$ 为合数时无解, 还余下 $2n+1$ 为素数的情况没有解决。现在利用定理 2, 我们来给出一个不用讨论 $2n+1$ 是合数还是素数的统一证明。

例 6 不定方程 $3^{2n+1} = 2y^2 + 1$. 除 $n=2, y=11$ 外无正整数解。

证明: 化为类 Pell 方程: $(2y)^2 - 6 \cdot (3^n)^2 = -2$. 即化为: $X^2 - 6Y^2 = -2$ 的解 (x_n, y_n)

中有多少项 y_n 为 3 的幂. 先写前几项, $y_1 = 1, y_2 = 9, y_{n+1} = 10y_n - y_{n-1}$.

这样已得到 $y_n = 3^0, 3^2$ 均有解, 现在关心的是 $y_n = 3^\alpha, \alpha \geq 3$ 有无解. 若有解,

这个 y_n 必为 27 的倍数, 利用定理 8, $\exists g(27) \in N^*$ 使 $27 | y_n \Leftrightarrow g(27) | 2n-1$.

我们先找 $g(27)$, 也就是要找 $\{y_n\}$ 中第一个被 27 整除的项的下标. 计算

$$y_3 = 89, y_4 = 881, y_5 = 8721 = 27 \times 17 \times 19, \text{ 所以 } g(27) = 5.$$

但注意, 对 17, 也 $\exists g(17) \in N^*$ 使 $17 | y_n \Leftrightarrow g(17) | 2n-1$. 所以 $17 | y_5 \Rightarrow g(17) | 5$.

所以对 $\forall y_n = 3^\alpha, \alpha \geq 3$, 由 $27 | y_n$ 得 $g(27) = 5 | 2n-1$, 而 $g(17) | 5$, 所以

$$g(17) | 2n-1 \Rightarrow 17 | y_n, \text{ 与 } y_n = 3^\alpha \text{ 矛盾.}$$

所以 $y_n = 3^\alpha, \alpha \geq 3$ 均无解.

从而 $X^2 - 6Y^2 = -2$ 的解 (x_n, y_n) 中只有 $y_n = 3^0, 3^2$ 有解. 即 $3^{2n+1} = 2y^2 + 1$ 的

全部非负整数解为 $(n, y) = (0, 1), (2, 11)$. \square

例 7 当 $n \neq 2^\alpha, n \neq 2^\alpha \cdot 5$ 时, 不定方程 $3^{2n} = 2y^2 + 1$ 无正整数解.

证明: $3^{2n} + y^4 = (y^2 + 1)^2$, 由勾股方程的结果, $\exists a, b$ 一奇数一偶数, $a > b$, 满

$$\text{足 } 3^n = a^2 - b^2, y^2 = 2ab, y^2 + 1 = a^2 + b^2.$$

所以 $a^2 + b^2 = 1 + 2ab$ 所以 $a - b = 1$

所以 $3^n = 2b+1, y^2 = 2b(b+1)$.

当 b 为偶数时, $(2b, b+1) = 1$, 所以 $2b = u^2, b+1 = v^2, y = uv, 3^n - u^2 = 1$.

所以 u 为偶数, 模 4 得 n 为偶数, $\left(3^{\frac{n}{2}}\right)^2 - u^2 = 1$, 无正整数解.

当 b 为奇数时, $(2(b+1), b) = 1$, 所以 $2(b+1) = u^2, b = v^2, y = uv$,

$3^n = 2v^2 + 1$. 这样我们从 $3^{2n} = 2y^2 + 1$ 得出了 $3^n = 2v^2 + 1$, 重复有限步后, 得到

$3^{\frac{2n}{2^\alpha}} = w^2 + 1$, 使 $\frac{2n}{2^\alpha}$ 为奇. 由假设, n 不是 2 的方幂, 也不是 2 的方幂乘以 5,

$\frac{2n}{2^\alpha}$ 是不等于 5 的奇数, 由例 7, 无正整数解.

最后, 将关于不定方程 $x^m - 2y^n = 1$ 我们所得到的结果罗列如下:

1. 当 $m=n=2$ 时有无穷多解, 最小解为 $(3, 2)$, 通解可以由 $x_n + \sqrt{2}y_n = (3 + 2\sqrt{2})^n$ 给出.
2. 当 $m=p$ 或 $2p$, n 为偶数时, 方程的正整数解 (x, y) ($x > 3$) 必满足 $p | y$.
3. 当 m 为奇数或 m 为偶且 $m \neq 2^\alpha, m \neq 2^\alpha \cdot 5$, n 为偶数时, 方程没有整数解使 $x = 3$.

参考文献

- [1]柯召 孙琦 谈谈不定方程 上海：上海教育出版社 1980.8
- [2]曹珍富 丢番图方程引论 哈尔滨：哈尔滨工业大学出版社 1989.2