arXiv:2603.05809v1 [math.NT] 6 Mar 2026

关于求解 $Ax^4 - By^2 = 1$ 的一种初等方法。

P.G. WALSH

Abstract. 本文从计算和理论两方面研究了 Luo 和 Lin 提出的一种求解四次方程的新方法。由此，本文给出了一种完全直接的初等方法，用于求解 Bumby 方程 $3X^4 - 2Y^2 = 1$；此外还提出了一个猜想，若该猜想得到解决，将能够为一个可能是无限的类似方程族给出类似的证明。

1. Introduction

丢番图方程 $Ax^4 - By^2 = 1$ 有着悠久的历史，许多人都曾对此作出贡献。其中最值得注意的是，Ljunggren [7] 证明了这类方程的整数解的许多基本结果；与此同时，其他人也作出了重要贡献，例如 Cohn [5], 、Akhtari [1],、Chen 和 Voutier [4], 、Bennett、Togb´e 以及作者本人 [2] 。该主题的大部分内容都收录在综述文章 [9] 中。

本文的灵感源于 Richard Bumby 的一项非凡成果 [3]。1967年，Bumby 解决了 J.H.E. Cohn 在 [5] 提出的一个猜想，确定四次方程 $3x^4 - 2y^2 = 1$ 的所有正整数解为（x， y）=(1，1) 和（x， y）=(3，11)。Bumby 给出的证明运用了巧妙的洞见，并构造了涉及环 $\mathbb{Z}[\sqrt{-2}]$中整数的一些方法。

我们在此指出，利用 [6]中给出的、涉及雅可比符号的论证，求解形如 $Ax^4 - By^2 = 1$ 的方程可以归结为求解形如（$t + 1$）$X^4 - tY^2 = 1$的方程。此外，Bumby 的结果后来在 [2] 中通过超几何方法推广到了任意形如（$t + 1$）$x^4 - ty^2 = 1$的四次方程，其中 t 形如 $t = u^2 + u$；按照猜想，只有当 t 取这些特定值时，此类方程才恰有一个正整数解不同于（x， y）=(1， 1)。换言之，对于不具有 $u^2 + u$形式的 t，猜想其唯一的正整数解就是这个显然的解。

最近，林和罗 [8] 发现了一种求解 $(t + 1)X^4 - tY^2 = 1$ （其中 $t = 1$）的初等方法。本质上，该方法利用因子基和模数，排除模数所确定的等差数列中除一个以外的所有等差数列，然后通过一种非凡的构造证明，在剩下的等差数列中，每一项在某个相应整数处取值的雅可比符号始终等于 -1。

Date: 2026年3月9日。
2020 *Mathematics Subject Classification.* 11D25。
Key words and phrases. 丢番图方程。

本文旨在探究 [8] 的思想在多大程度上能够用于求解一般方程 $(t+1)$ $X^4 - tY^2 = 1$。尽管 [8] 的方法极其巧妙，但似乎存在一些复杂之处和局限性。特别是，对于 $t = 1$， [8] 中用于计算相关雅可比符号的论证乍看之下相当令人望而生畏，而且论证中没有任何迹象表明该方法有望推广。尽管如此，我们仍将努力发展这些思想。在第2节中，我们考虑 $t = 2$的情形。正如我们将看到的，该方法的效果出奇地好，其中关于雅可比符号的论证远比 [8]中的简单。

2. Solving Bumby's equation $3X^4 - 2Y^2 = 1$

2.1. **因子基**。

设 $\alpha = \sqrt{3} + \sqrt{2}$，并对 $k \geq 1$ 定义数列 $\{P_k\}$ 与 $\{Q_k\}$ 如下

$$P_k\sqrt{3} + Q_k\sqrt{2} = \alpha^k \quad (k \text{ odd})$$

and

$$P_k + Q_k\sqrt{6} = \alpha^k \quad (k \text{ even}).$$

$3x^2 - 2y^2 = 1$ 在正整数 (x, y) 中的所有正整数解由 $(x, y) = (P_k, Q_k)$ 给出，其中 k 为奇正整数。数列 $\{P_k\}$ 可通过取α的相应负幂而延拓到负指标，并注意到 $P_{-k} = P_k$。

为了求解 $3x^4 - 2y^2 = 1$，我们看到这等价于确定一组奇正指标 n，使得对某个整数 x有 $P_n = x^2$。注意，对 $n = 1$ 与 $n = 3$ 确实存在解（分别对应于 $x = 1$ 与 $x = 3$），因而对 $n = -1$ 与 $n = -3$也存在解。我们采取的方法是，首先针对某个策略性选取的模数排除一大组同余类。这些同余类由若干素数排除，这些素数见证了当 n 属于某一同余类时P_n 的非平方性。该模数的选取使得数列 $\{P_k\}$ 模因子基中每个素数的阶整除该模数。

要选取有效的模数，需要经过一些试验和摸索。我们不再详细说明这一过程，只指出该模数必须容纳足够多的素数，同时又不能过大。对于所研究的方程，模数 $M = 1680$ 的效果不错，相应的因子基为

$$FB = \{11, 13, 29, 41, 43, 59, 71, 83, 89, 97, 109, 179, 211, 241, 337, 419, 587, 673, 881, 1009, 1901, 3361, 3779, 4549, 5881, 8641, 9601\}。$$

简单计算可知，$\{P_k\}$ 对 FB 中每个素数取模后的阶都整除 1680；并且，除同余类

$$k \in \{1, 3, 837, 839, 841, 843, 1677, 1679\}$$

模 1680 外，都存在一个素数 $p \in FB$，使得勒让德符号 $\left(\frac{P_k}{p}\right) = -1$。 —

因此，我们有如下结论。

命题 1. 若 $P_n = x^2$ 对某个整数 x 成立，则 $n \equiv \pm 1,\ \pm 3 \pmod{840}$。

2.2. 主要情形： $n \equiv 1 \pmod{840}$。我们在上一节已经看到，该问题可归结为四个同余类。其中三个将在证明的最后一步相对容易地处理。证明的主要内容包含在本节中，即构造某个与指标 n（见命题 1）相关的指标 b，以及与数列 $\{P_k\}$ 和 $\{Q_k\}$ 相关的整除性质，并对某些相关的雅可比符号进行求值。

为了继续进行，我们需要对数列 $\{P_k\}$ 和 $\{Q_k\}$ 作若干观察。首先，若 n 为奇数且 k 为偶数，则通过比较 $\sqrt{3}$ 在

$$\alpha^{n+2k} = P_{n+2k}\sqrt{3} + Q_{n+2k}\sqrt{2}$$

与下列式中的

$$\alpha^n \cdot \alpha^{2k} = (P_n\sqrt{3} + Q_n\sqrt{2}) \cdot (P_k + Q_k\sqrt{6})^2,$$

将乘积展开后，我们看到

$$P_{n+2k} \equiv P_n \pmod{Q_k}. \tag{2.1}$$

所需的第二个观察涉及商 Q_{6k}/Q_{2k}，且 k 为奇数。我们将略去细节，仅指出当 k 为奇数时

$$Q_{6k}/Q_{2k} = 3(4P_k^2 - 1)(12P_k^2 - 1). \tag{2.2}$$

将 α^k 提升到六次方即可轻易看出这一点。该恒等式所要使用的主要性质是：对于奇数 k，因子 $2P_k + 1$ 是 Q_{6k} 的因数。

现在假设 $n \equiv 1$（模 840）（$n \neq 1$），并令 t 表示满足 $n = 1 + 840t$ 的非零整数。这一表示将导出一个由四个整数（a、b、c、d）组成的序列，该序列仅取决于 n，并满足非常特殊的性质。需要注意的是，$n \in \mathbb{Z}$，因此它可能为负数。定义 $c = \mathrm{ord}_3(840t)$ 和 $d = 24t/3^c$。注意，整数 d 模 24 同余于 8 或 16。随后我们如下定义 a、b。

$$(a, b) = \begin{cases} (35d, 3^c) & d \equiv 8 \pmod{24} \text{ and } c \text{ is even} \\ (7d, 5 \cdot 3^c) & d \equiv 16 \pmod{24} \text{ and } c \text{ is even} \\ (5d, 7 \cdot 3^c) & d \equiv 8 \pmod{24} \text{ and } c \text{ is odd} \\ (d, 35 \cdot 3^c) & d \equiv 16 \pmod{24} \text{ and } c \text{ is odd.} \end{cases}$$

注意，$a \equiv 16 \equiv -8$（模 24），因此我们令 m 表示满足 $a = 24m - 8$ 的整数。还要注意，$3 \nmid b$，且 $b \equiv 1$（模 4）。我们将使用上面的（2.1）将 P_n 对 Q_{6b} 取模，具体如下。

$$P_n = P_{1+ab} = P_{1+(24m-8)b} \equiv P_{1-8b} = P_{8b-1} \pmod{Q_{6b}}.$$

由 (2.2) 可知，$2P_b + 1$ 整除 Q_{6b}，因此我们证明了

$$P_n \equiv P_{8b-1} \pmod{(2P_b + 1)}. \tag{2.3}$$

量 P_{8b-1} 可先利用恒等式$P_{8b-1} = P_{8b} - 2Q_{8b}$，再展开 $(\alpha^b)^8$，从而将 P_{8b-1} 写成关于 P_b 的多项式，进而模 $2P_b + 1$ 约化。我们略去这一计算的展示，仅说明在这样做之后，得到同余式

$$P_n \equiv P_b - 2Q_b \pmod{(2P_b + 1)}. \tag{2.4}$$

由于对所有奇数 k 均有 $P_k \equiv 1 \pmod 8$，故有 $2P_b+1 \equiv 3 \pmod 8$，从而得到如下一列雅可比符号等式

$$\left(\frac{P_n}{2P_b+1}\right) = \left(\frac{P_b-2Q_b}{2P_b+1}\right) = -\left(\frac{2P_b-4Q_b}{2P_b+1}\right) = -\left(\frac{-1-4Q_b}{2P_b+1}\right) = \left(\frac{4Q_b+1}{2P_b+1}\right).$$

现在回想一下 $b \equiv 1 \pmod 4$，这意味着 $b = 2r+1$，其中 r 为偶数。在这种情况下，展开 $\alpha \cdot (\alpha^r)^2$，后，很容易看出 $P_{2r+1} = P_{2r} + 2Q_{2r} = (2P_r^2-1) + 4P_rQ_r$，且 $Q_{2r+1} = P_{2r} + 3Q_{2r} = (2P_r^2-1) + 6P_rQ_r$。因此，

$$\left(\frac{P_n}{2P_b+1}\right) = \left(\frac{4Q_b+1}{2P_b+1}\right) = \left(\frac{8P_r^2+24P_rQ_r-3}{4P_r^2+8P_rQ_r-1}\right) = \left(\frac{8P_rQ_r-1}{4P_r^2+8P_rQ_r-1}\right)$$
$$= -\left(\frac{4P_r^2+8P_rQ_r-1}{8P_rQ_r-1}\right) = -\left(\frac{4P_r^2}{8P_rQ_r-1}\right) = -1.$$

2.3. 证明的完成。 还需处理模 840 的同余类 $-3, -1$ 和 3。我们先考虑对应于 3 的同余类，然后处理负数情形，以完成证明。

假设存在一个整数 $n \equiv 3 \pmod{840}$（$n \neq 3$），使得 $P_n = x^2$。令 $n = 3k$。由于 $P_{3k} = P_k(3P_k^2 + 6Q_k^2)$，且能同时整除这两个因子的素数只有 3，因此必存在整数 u, v，使得要么 $P_k = u^2, 3P_k^2+6Q_k^2 = v^2$，要么 $P_k = 3u^2$，$3P_k^2 + 6Q_k^2 = 3v^2$。后一种情况去掉因子 3 后显然不可能模 8 成立，因此只剩前一种情况。关于 n 的同余条件迫使 k 满足 $k \equiv 1 \pmod{280}$。然而，根据目前已证明的结果，方程 $P_k = u^2$ 意味着 $k \pmod{840} \in \{-3, -1, 3\}$，这是不可能的。

如果存在一个整数 $n \equiv -1 \pmod{840}$ 使得 $P_n = x^2$，那么由于 $P_n = P_{-n}$，我们可以将上述构造应用于 $-n$，得到一个满足 $\left(\frac{P_{-n}}{2P_b+1}\right) = -1$ 的整数 b，从而看出 P_n 不是平方数。最后，$n \equiv -3 \pmod{840}$ 的情形现在可以完全按照我们处理 $n \equiv 3 \pmod{840}$ 情形的方法来解决。

3. The Extent of the Method

3.1. 与该方法相关的计算结果。 Akhtari 在 [1] 中的结果表明，任意形如 $Ax^4 - By^2 = 1$ 的方程至多有两个正整数解 (x, y)，而且这一上界通常是最佳的。尽管这类方程中存在一个具有两个解的子族 [2],，但据推测，大多数方程只有一个解。因此，这些四次方程中的大多数实际上尚未得到彻底求解。由此看来，理论上，本文的方法可以补充现有的求解方法，成为解决这类方程的工具之一；现有方法大多已在 magma 和 pari 等程序中实现。此外，与 Akhtari 的结果不同，后者给出了所有方程的上界；据我们理解，本文的方法一次只能应用于一个方程。本节将考察该方法的适用程度。

迄今为止，林和罗已成功运用该方法求解 $2x^4 - y^2 = 1$，而且我们在上文第2节展示了该方法如何有效求解$3x^4 - 2y^2 = 1$。在继续研究其他这类方程之前，我们先指出

这一事实：Cohn 首先在 [6], 中证明，具有正整数解的形如 $Ax^4 - By^2 = 1$的方程与形如（$t+1$）$X^4 - tY^2 = 1$的方程一一对应，因此我们可以专注于后一类方程。从计算角度看，化简步骤需要计算类佩尔方程 $Ax^2 - By^2 = 1$的基本解。

如第2节所述，林和罗的方法由两部分组成：首先利用因子基得到的见证元，排除几乎所有的算术级数；然后结合雅可比符号归约及后续论证，排除剩余的算术级数。我们首先描述将该方法的第一部分应用于方程 $(t+1)X^4 - tY^2 = 1$（其中 t 取值至某个相当大的上界）的实践经验。

我们在此提醒读者，对于 $\alpha = \sqrt{t+1} + \sqrt{t}$, 且当 $k \geq 1$时，可以定义数列$\{P_k\}$和 $\{Q_k\}$ 如下：

$$P_k\sqrt{t+1} + Q_k\sqrt{t} = \alpha^k \quad (k \text{ odd})$$

and

$$P_k + Q_k\sqrt{t(t+1)} = \alpha^k \quad (k \text{ even}).$$

如第2.1节所述，我们的方法是同时使用一个主 模数 m和一个工作 模数 M。我们通常使用 $m = 840$，并令 $M = 2^r 3^s m$，其中 r 和 s为非负整数。对于固定的 r 和 s，计算首先尽可能生成满足以下性质的素数 p ：约化数列 P_n （模 p）的阶整除 M。因子基由这组素数组成。计算的第二部分求出所有指标 j，其中 $1 < j < M-1$，使得因子基中不存在满足 $\left(\frac{P_j}{p}\right) = -1$的素数 p。计算的最后一部分将这一步中找到的指标模主模数 m进行约化。预期通过这一过程，当 t 不是 $u^2 + u$的形式时，可以计算出集合 $\{1, 839\}$；而在 $\{1, 3, 837, 839\}$ 时则可以计算出另一种情形。

这项计算的结果完全符合预期，而且几乎总是使 r 和 s 都非常小。奇怪的是，只有当t 取形如 $t = 2u^2$ 的值时，计算才要求 r 和 s 变得稍大一些；尤其是当 t 为 2 的奇数次幂时。

证明的后半部分处理剩下的 2 或 4 个等差数列，具体取决于 t 是否具有 $t = u^2 + u$ 的形式。与第2节一样，大部分工作都在处理情形 $1 + 840i$ $(i \in \mathbb{Z})$。下文中，我们将始终把重点放在这一情形上。

现在尝试通过使用一个仅依赖于 t的多项式 $p(x)$，以及一个依赖于 n的输入 b，来证明对于 $n \equiv 1$ （模 840），$P_n = x^2$ 是不可能的（$n \neq 1$）；其中雅可比符号 $\left(\frac{P_n()}{p\ b}\right) = -1$。在上述情形中奏效的 $p(x)$的选取，是 P_{6k}/P_{2k} 或 Q_{6k}/Q_{2k} （k 为奇数）中的一个因子，分别将其写成关于 P_k 或 Q_k 的多项式。更确切地说，计算这些多项式表达式后，我们确定 $p(x)$的选取是以下表达式的一个因子

$$P(x) = (16(t+1)^2x^4 - 16(t+1)x^2 + 1) \cdot (16(t+1)^2x^4 - 16(t+1)x^2 + 3).$$

第2节中描述的 b 的选取，正是 Lin 和 Luo 的工作 [8]中所采用的选取。

我们对 $t \le 1000$ 进行了大量计算，使用的不仅有 $P(x)$ 的因子，还有许多二次多项式以及所述输入的各种变体。只有在非常精确地选取 $p(x)$、b 和 t 时，才能始终如一、可靠地得到雅可比符号的值均为 -1。我们将在下文通过一个猜想阐明我们的发现。

简言之，我们的计算强烈表明，该方法仅适用于一个极其狭窄的集合：

$$t = du^2 - 1 \text{ with } d \in \{2, 3, 4, 6\}.$$

特别是，对于第2节中给出的输入 b，以下多项式总能给出所需的雅可比符号值。

d	t	$p(x)$
2	$2i^2-1$	$8i^2x^2 \pm 4ix - 1$
3	$3i^2-1$	$2ix \pm 1$
4	$4i^2-1$	$4ix \pm 1$
6	$6i^2-1$	$24i^2x^2 \pm 12ix + 1$

要证明 $p(b)$ 的值确如所述，似乎非常困难。迄今为止，我们还无法证明关于 $t > 2$ 的任何结果。因此，我们提出以下猜想，供有意继续这一研究的人参考。

猜想3.1
对于 $d = 3$、$t = 3i^2 - 1$、$p(x) = 2ix + 1$ 且 $i \ge 1$ 为奇数

$$\left(\frac{P_n}{p(P_b)}\right) = (-1)^{(i-1)/2}\left(\frac{2tQ_b + 1}{2iP_b + 1}\right) = -1.$$

请注意，除已在第2节证明的情形 $i = 1$ 外，猜想中给出的两个等式对于所有 $i \ge 2$ 都尚未得到证明。关键在于，如果这一猜想得到证明，就能为无穷多个方程提供这种初等证明。

References

[1] S. Akhtari, *The Diophantine equation $aX^4 - bY^2 = 1$*。《纯粹与应用数学杂志》**630** (2009), 33–57。
[2] M.A. Bennett、A. Togb
´ *A generalization of a theorem of Bumby on quartic* e、P.G. *Diophantine equations.* **2** 2006 195 206
WALSH, 《国际数论杂志》( ) – 。[3] R.T. Bumby, *The Diophantine equation $3x^4 - 2y^2 = 1$*, 《斯堪的纳维亚数学杂志》**21** (1967) 144–148。[4] J. H. Chen 和 P. M. Voutier, *A complete solution of the Diophantine equation $x^2 + 1 = dy^4$ and a related family of quartic Thue equations* **62** 1997 71 99 , 《数论杂志》( ) – 。[5] J.H.E. Cohn, *Eight Diophantine equations*, 《伦敦数学会会刊》**16** (1966), 153–166。[6] J.H.E. Cohn, *The Diophantine equation $x^4 - Dy^2 = 1$ II*, 《算术学报》**78** (1997) 401–403。[7] W. Ljunggren, *On the Diophantine equation $Ax^4 - By^2 = C$ ($C = 1$, 4)*, 《斯堪的纳维亚数学杂志》**21** (1967) 149–158。[8] L. Lin 和 M. Luo, *An elementary solution of the Diophantine equation $x^2 - 2y^4 = -1$*. 即将在《美国数学会会刊》发表，2025年，10页。

[9] P.G. WALSH, *Diophantine equations of the form* $aX^4 - bY^2 = 1$, 载于《代数数论与丢番图分析》，1998年格拉茨国际会议论文集（Walter de Gruyter，柏林，2000年），531–554。

Department of Mathematics, University of Ottawa
Email address: gwalsh@uottawa.ca