Introduction to Diophantine Equations

HIT

数论经典著作系列

丢番图方程引论

曹珍富 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

数论经典著作系列

丢番图方程引论

Introduction to Diophantine Equations

曹珍富 著

由黑龙江省精品图书出版工程专项资金资助出版

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

丢番图方程(Diophantine equations)是数论的一个重要分支,国内外很多著名数学家都从事过它的研究。其中尤以 Roth、Baker 和 Faltings 等人的工作最为突出(他们分别获得了国际数学家大会的 Fields 奖)。本书力求全面详细地介绍这一数学分支的研究成果和创造的方法(有些方法产生了新的数学分支)。

本书共分十章,分别为:引言、解丢番图方程的初等方法、解丢番图方程的高等方法、一次丢番图方程、二次丢番图方程、三次丢番图方程、四次丢番图方程、高次丢番图方程、指数丢番图方程和单位分数问题。其中有一些是作者本人的研究成果。

本书可供从事这一数学分支或相关学科(组合论、群论和编码理论等)的数学工作者、研究生以及有兴趣的大学生和中学生阅读、学习和参考。

图书在版编目(CIP)数据

丢番图方程引论/曹珍富著. —哈尔滨:哈尔滨工业大学出版社,2012.3

ISBN 978-7-5603-3517-9

Ⅰ.①丢… Ⅱ.①曹… Ⅲ.①丢番图方程 Ⅳ.①O156.7

中国版本图书馆 CIP 数据核字(2012)第 042755 号

策划编辑 刘培杰 张永芹
责任编辑 王勇钢
封面设计 孙茜艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm×1092mm 1/16 印张 19.25 字数 340 千字
版 次 2012 年 3 月第 1 版 2012 年 3 月第 1 次印刷
书 号 ISBN 978-7-5603-3517-9
定 价 48.00 元

序

数论是数学中的一个重要分支。古今中外许多著名数学家都曾从事过数论的研究。数论往往以它的问题简明易懂吸引了大批青年人和业余数学爱好者。然而,如果不脚踏实地地不断加强数学素养、扩展数学知识面,也是难以取得成功的。

本书作者曹珍富就是哈尔滨工业大学八年前的一位被数论所深深吸引的非数学专业的学生,后来逐渐走上了科学研究的道路,发表了不少论文,成为我国最年轻的一批数学副教授中的一员。这本书是他几年来对数论中的丢番图方程(即不定方程)这一分支学习、研究的一个总结,也是继1969年Mordell的《丢番图方程》一书问世后的又一部著作。

全书共分10章。除引言外,以第2、3两章分别详细介绍解丢番图方程的初等方法和高等方法,这里把借助相应方法所得到的近期成果纳入习题的做法,将有助于增强读者研究问题的能力和信心。第4到第10章,则依次讲述从一次、二次、三次、四次直至高次的丢番图方程以及指数丢番图方程和单位分数问题等不同类型的专题,侧重阐明结果与获得结果的所用方法,这便于读者了解和掌握。因之,本书具有一定特色。

由于丢番图方程的相当部分并不涉及更多的数学基础,加之本书由浅入深、循序渐进,读者只要具备一些初等数论知识即可读懂书中的绝大部分内容。可见该书就是对大学生、乃至部分中学生也都是一种可供阅读、参考的读物。

个人对于丢番图方程完全是门外汉。我国著名数学家柯召教授对此有一系列重要贡献。这本书的作者也得益于孙琦教授的指教甚多。对一个正在成长的年青数学工作者所撰写的专门书籍难免有不成熟之处,甚至还会不少。相信我国数论界的前辈和同行必将继续给予帮助、鼓励和指点。

吴从炘

识于哈尔滨工业大学

1987年10月31日

目录

第 1 章　引言　// 1

1.1　数论的特点　// 1
1.2　丢番图方程及其主要成就　// 2
1.3　解丢番图方程的困难性　// 3
1.4　丢番图方程的内容和求解原则　// 4
1.5　本书的特点　// 5
参考文献　// 6

第 2 章　解丢番图方程的初等方法　// 7

2.1　简单同余法　// 7
2.2　分解因子法　// 12
2.3　无穷递降法　// 18
2.4　比较素数幂法　// 23
2.5　二次剩余法　// 27
2.6　Pell 方程法　// 32
2.7　递推序列法　// 40
2.8　其他的一些初等方法　// 49
参考文献　// 56

第3章　解丢番图方程的高等方法　// 58

3.1　代数数论方法(Ⅰ)　// 58
3.2　代数数论方法(Ⅱ)　// 67
3.3　p-adic 方法　// 72
3.4　丢番图逼近方法　// 80
3.5　其他的一些高等方法　// 87
参考文献　// 91

第4章　一次丢番图方程　// 93

4.1　二元、三元的一次丢番图方程　// 93
4.2　$s \geqslant 2$ 元一次丢番图方程　// 95
4.3　整系数线性型问题　// 98
参考文献　// 104

第5章　二次丢番图方程　// 105

5.1　一般的二元二次丢番图方程　// 105
5.2　Pell 方程 $x^2 - Dy^2 = 1$　// 106
5.3　方程 $x^2 - Dy^2 = M$　// 110
5.4　方程 $x^2 - Dy^2 = M$ 的应用　// 117
5.5　两个三元二次丢番图方程的公解　// 120
5.6　三元以上的二次丢番图方程　// 127
5.7　一些与二次丢番图方程有关的问题和结果　// 131
参考文献　// 134

第6章　三次丢番图方程　// 135

6.1　方程 $ey^2 = ax^3 + bx^2 + cx + d, a \neq 0$　// 135
6.2　方程 $x^3 + b = Dy^n (n = 2,3)$　// 146
6.3　二元三次型及其相关方程　// 155
6.4　三元三次丢番图方程　// 162
6.5　四元三次丢番图方程　// 173
参考文献　// 176

第7章　四次丢番图方程　// 179

7.1　丢番图方程 $a^2x^4 - Dy^2 = 1 (a = 1,2)$　// 179
7.2　丢番图方程 $x^2 - Da^2y^4 = 1 (a = 1,2)$　// 188
7.3　丢番图方程 $a^2x^4 - Dy^2 = -1$ 和 $x^2 - Dy^4 = -1$　// 195

7.4 丢番图方程 $dy^2 = ax^4 + bx^2 + c$ // 199
7.5 丢番图方程 $x^4 + kx^2y^2 + y^4 = z^2$ // 205
7.6 一些四元四次丢番图方程 // 209
参考文献 // 211

第8章 高次丢番图方程 // 214

8.1 丢番图方程 $x^{2n} - Dy^2 = 1$ 和 $x^2 - Dy^{2n} = 1$ // 214
8.2 丢番图方程 $ax^2 + bx + c = dy^n$ // 219
8.3 丢番图方程 $ax^m - by^n = c$ // 226
8.4 几个连续数问题 // 231
8.5 Fermat 大定理 // 235
参考文献 // 239

第9章 指数丢番图方程 // 243

9.1 两个乘幂之差 // 243
9.2 丢番图方程 $a^x + b^y = c^z$ // 246
9.3 与有限单群相关的指数丢番图方程 // 251
9.4 丢番图方程 $x^2 + D = p^n$ // 253
9.5 方程 $x^x y^y = z^z$ 及其推广 // 258
9.6 其他一些指数丢番图方程 // 263
参考文献 // 268

第10章 单位分数问题 // 272

10.1 方程 $\frac{m}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ // 272
10.2 Mordell 的一个问题 // 275
10.3 方程 $\sum_{i=1}^{s} \frac{1}{x_i} + \frac{1}{x_1 \cdots x_s} = 1$ // 279
10.4 方程 $\sum_{i=1}^{s} \frac{1}{x_i} - \frac{1}{x_1 \cdots x_s} = 1$ // 284
10.5 与单位分数相关的问题 // 287
参考文献 // 289

编辑手记 // 291

引　言

第 1 章

1.1　数论的特点

在如今众多的数学分支中，有些即使你具备了一定的数学基础，要读懂它的基础知识也有一定的困难，甚至要理解它的符号的含义也办不到；而有些却不需要任何数学基础，只要你有耐心地往下读，便可读懂它的绝大部分内容. 数论这门古老的数学分支，它的基本内容便是属于后者. 数论的问题简明易懂，即使是公认的 Fermat 大定理和 Goldbach 猜想等问题也是如此. 正因为这样，历史上几乎所有的数学家都从事过数论的研究，而且许多数学家都是因为数论问题的简明易懂，通过自学获得成功的. 但事情往往是这样，越是简明易懂的问题，解决起来越困难. 也正因为如此，不知道有多少业余数学爱好者迷上了数论，但最终却一事无成.

数论起初只研究整数的一些基本性质，后来从 17 世纪到 19 世纪，大数学家 Fermat，Euler，Legendre，Gauss 等人大大地发展了数论的内容，现在数学界最著名的难题—— Fermat 大定理便是这个时期提出来的.

今天的数论已经发展为十多个数论分支，诸如代数数论、解析数论、丢番图方程、丢番图逼近和丢番图几何等，许多内容

已经发展到相当深刻的程度，以至于搞不同分支的数论同行间也无法相互交流. 可以举一个例子，你如果想读懂丢番图几何方面的研究论文，在不具有相当好的代数、拓扑等基础时，即使你在其他某个数论分支中做出过很好的工作，但也几乎是不可能的.

1.2 丢番图方程及其主要成就

这本书将专门研究数论的一个分支——丢番图方程的各种基本类型. 什么叫丢番图方程呢？众所周知，Fermat 大定理是 Fermat 于 1637 年左右在古希腊数学家丢番图(Diophantus) 所著《算术》一书的空白处写下的注释，用如今的语言叙述，就是：不定方程

$$x^n + y^n = z^n \quad n > 2$$

没有正整数解. 这就明显告诉我们，Fermat 大定理是属于不定方程的. 所谓不定方程，是指未知数的个数多于方程个数的方程(或方程组). 数论中的不定方程，通常对解的范围有一定的限制，例如解限制在有理数、整数等范围内. 这种带限制的不定方程早在公元 3 世纪初古希腊数学家丢番图就研究过，人们为了与其他分支中的不定方程区别，也称数论中的不定方程为丢番图方程(Diophantine equations). 正如丢番图几何一样，它是代数几何中曲线上的“点”带限制的部分.

在丢番图方程中，各种形式的不定方程是无穷无尽的. 但解决问题的方法，从古至今都是不同的问题用不同的方法，其中显示出了人类高度的智慧. 人们自然要问，是否存在一个一般的解不定方程的方法？这个问题的特殊情形是属于 D. Hilbert 第十问题的. 1900 年，D. Hilbert 提出了 23 个著名的数学问题，其中第十个是：

设 $f(x_1,\cdots,x_n)$ 是任给的具有整系数的多项式，那么是否存在一个只有有限步运算的方法来判定丢番图方程 $f(x_1,\cdots,x_n)=0$ 是否有解？

这个问题的一般回答是否定的[1]. 不妨设 $f(x_1,\cdots,x_n)$ 为不可约多项式，则在 $n\geqslant 3$ 时不存在一个只有有限步运算的方法来判定丢番图方程 $f(x_1,\cdots,x_n)=0$ 是否有解. 而在 $n=2$ 时，A. Baker 定出了丢番图方程 $f(x_1,x_2)=0$ 解的上界[2]，因而存在一个有限步运算的方法判定 $f(x_1,x_2)=0$ 是否有解. 但是，A. Baker 定出的上界往往太大，常常用最快的电子计算机也不能计算出方程的全部解来. 因此，即使对于方程 $f(x_1,x_2)=0$，要求出全部解来也不容易.

但是，A. Baker 的工作不失为丢番图方程的重要成就. 包括 A. Baker 在内，还有 K. F. Roth，R. Deligne 和 G. Faltings 都在丢番图方程上作出过杰出的贡献.

1955 年 K. F. Roth 证明了一个著名的定理[3]：设 θ 是一个 $n \geqslant 2$ 次的代数数，则 $\forall \varepsilon > 0$，适合

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{y^{2+\varepsilon}}$$

的整数 $x, y > 0$ 仅有有限组. 这一定理导致了二元 $n \geqslant 3$ 次的不可约多项式方程解的个数有限. 1973 年，R. Deligne 证明了关于有限域上不定方程 $f(x_1, \cdots, x_n) = 0$ 解的个数的猜想，即著名的 A. Weil 猜想[4]. 而 G. Faltings 在 1983 年证明了 L. J. Mordell 猜想，即有理数域里亏格 $\geqslant 2$ 的代数曲线上仅有有限个有理点[5]. 由此可以导出 Fermat 方程 $x^n + y^n = z^n$，$(x, y) = 1$ 在 $n \geqslant 4$ 时最多仅有有限组正整数解. 1985 年 D. R. Heath - Brown 利用 G. Faltings 定理证明了 $\lim\limits_{s\to\infty} \frac{N(s)}{s} = 0$，这里 $N(s)$ 表 $n \leqslant s$ 使 $x^n + y^n = z^n (n > 2)$ 有正整数解的那些 n 的个数[6]. 即对“几乎所有”的正整数 $n > 2$，方程 $x^n + y^n = z^n$ 均没有正整数解.

因为 K. F. Roth，A. Baker，R. Deligne 和 G. Faltings 的出色工作，他们分别于 1958 年、1970 年、1978 年和 1986 年获得了国际数学家大会的菲尔兹(Fields)奖.

1.3 解丢番图方程的困难性

解丢番图方程由于没有一个一般的方法，因而它向人类的智慧提出了挑战. 有一些看上去简单的方程，但解决起来却相当困难，例如求不定方程

$$1 + x^2 = 2y^4 \tag{1}$$

的正整数解 x, y 问题，在很长时间内数学家们只知道它有两组解 $(x, y) = (1, 1), (239, 13)$，但要回答它是否存在另外的解却不容易. 直到 1942 年 W. Ljunggren 在认真研究四次域的单位数后，用了大量的现代数论的成果才最终证明：方程(1) 最多有两组正整数解[7]. 后来，人们感到 W. Ljunggren 的证明复杂又不初等，且方法上的技巧又太特殊，故大数学家 L. J. Mordell 向全世界提出了一个公开性的问题[8]：是否能找到一个简单的或初等的证明？这个问题直到现在仍未解决.

对于不定方程

$$x^x y^y = z^z \quad x > 1, y > 1 \tag{2}$$

著名数学家 P. Erdös 曾经猜想它没有正整数解. 1940 年我国著名数学家柯召否定了这一猜想，证明了方程(2) 有无穷多组解[9]：

$$x = 2^{2^{n+1}(2^n-n-1)+2n}(2^n-1)^{2(2^n-1)}$$
$$y = 2^{2^{n+1}(2^n-n-1)}(2^n-1)^{2(2^n-1)+2}$$
$$z = 2^{2^{n+1}(2^n-n-1)+n+1}(2^n-1)^{2(2^n-1)+1}$$

其中 $n > 1$. 1959 年 W. H. Mills 发现柯召得到的解均满足 $4xy = z^2$ 的条件，从而证明了[10]：1) 如果 $4xy > z^2$，则方程(2) 没有正整数解；2) 如果 $4xy = z^2$，则柯召找到的解是(2) 的全部正整数解. 1984 年，S. Uchiyama 证明了：如果 $4xy < z^2$，则方程(2) 最多只有有限组正整数解[11]. 这提醒我们，很可能方程(2) 的全部正整数解都已包含在柯召得到的解中. 但是，要证明这件事或者找到另外的解都很困难.

对于 $n!$ 和组合数 $\binom{n}{m} = \frac{n!}{m!\ (n-m)!}$ 也曾有过一些猜想和问题. 例如方程

$$\binom{n}{m} = y^k \quad n > m > 1, k > 2 \tag{3}$$

没有正整数解. 这是 1939 年 P. Erdös 提出的一个猜想，直到 1984 年，才由本书作者解决了 k 为偶数的情形[12]；而 k 为奇数时，除了在 1951 年由 P. Erdös 本人解决了 $m > 3$(此时方程(3) 无正整数解) 外，目前只有一些零碎的结果. 要彻底证明 P. Erdös 的这个猜想还有一定的困难. 另一个问题是，方程

$$n! + 1 = x^2$$

仅有正整数解 $(n,x) = (4,5), (5,11)$ 和 $(7,71)$ 吗？P. Erdös 和 R. Obláth 曾经解决了方程 $n! = x^p \pm y^p$，$(x,y) = 1$ 且 $p > 2$，但对 $p = 2$ 无能为力[8]. G. J. Simmons 还提出，方程 $n! = (m-1)m(m+1)$ 仅有正整数解 $(m,n) = (2,3), (3,4), (5,5)$ 和 $(9,6)$ 吗？这个问题也没有得到解决.

通常，解一个丢番图方程很大程度上由人们的数学基础和研究经验决定的. 这常常导致初学者望而生畏. 但也有些初学者不了解丢番图方程的内容，以为丢番图方程是从属于初等数论的，就是初等数论中的几个小玩艺儿. 因此，许多初学者在不具备一定数学基础的同时，就不切实际地去试图证明 Fermat 大定理.

1.4 丢番图方程的内容和求解原则

丢番图方程的内容异常丰富，它的分类基本上是由方程的形式决定的. 例如，可分为一次方程、二次方程、三次方程、高次方程、指数方程和一些特殊的类型. 很多基本类型都是历史遗留下来的. 当然近代也提出了许多新的类型，这是

由于许多学科的交叉渗透产生的. 例如,在代数数论、组合论和群论等数学分支中都提出了一些丢番图方程问题.

就丢番图方程的研究目的而言,人们希望尽可能一般性地求解某个类型,以期在另外的许多场合得到更多、更好地应用. 有些问题在整数环上解决了,人们还愿意把它放到代数整环上去研究;有些问题用高深方法解决了,人们还希望 用较为初等的方法去解决. 这些做法的目的,无非是想通过这些研究产生新的结构或新的技巧,而构成这种新结构或新技巧的往往可能是新数学分支的萌芽,也可能对科学技术产生某些特殊的应用.

丢番图方程的内容异常丰富,但又没有一个统一的处理方法,这就决定了研究丢番图方程的困难性. 一般说来,我们只能给出丢番图方程的求解原则,即综合利用各种初等的、高深的方法,将丢番图方程转化为若干容易处理的或有熟知结果的方程. 这就告诉我们,需要有相当熟练的初等和高深的数学基础,才能在丢番图方程研究中取得好的成果. 但是,这也不是绝对的,在初等证明中,具有熟练的初等数论基础同样会做出好的成果.

1.5 本书的特点

本书我们假定读者具有初等数论的知识. 在用到超出初等数论知识时,我们列出主要结果而不加证明. 另外,书中的许多问题和结果在没有注明出处时,均是引自作者的一些未经发表的思想与方法,还有些部分是引自 Mordell 的书《Diophantine equations》书中所有字母在不做特别说明的情况下,均表示整数.

本书的特点是,详细论述了各种类型的丢番图方程的解及其研究的几乎全部成果. 尤其还较系统地介绍了解丢番图方程的方法,其中大量的成果和方法是近几年才得到的.

本书在表达和结构上也作了探索. 为了让读者掌握解丢番图方程的方法,我们在第 2、3 两章里,选择了一些典型的问题(这些问题中,有许多都是数学家们的研究结果,这在后面的专题研究中将有介绍),详细地给出了求解过程. 在让读者领会了这些方法和技巧后,我们除了选择一些基本的习题外,还列出数学家们若干用相应方法得到的近期的研究结果作为习题. 这样做的目的是,能够增强读者(尤其是自学者) 研究问题的信心和能力. 我们在写作时,为了让读者有一个自然的过渡,在讲述解丢番图方程的方法时,对问题(包括例题和习题) 的出处将不加注明(只有少部分例外). 但凡是数学家们的研究结果,都将在后面各章的专题研究中给以介绍. 从第 4 章开始,是各个专题的专门研究. 在

这方面,我们不可能给出每一个定理的详细证明(否则在篇幅上是不允许的).我们采取以介绍结果和取得该结果所使用的方法为主,给出少量技巧性强、方法使用上比较特殊且篇幅比较简短的证明为辅的写作方法. 我们认为,这样做对读者没有什么损失,况且每章末,我们还列出了较为详细的参考文献,便于读者进一步钻研时查阅.

应该指出,虽然本书从收集资料到定稿(1987 年 10 月) 用了许多年的时间,但仍可能有不少重要的成果被遗漏. 又由于作者受水平的限制,书中也可能有不少错误和某些疏忽. 尤其是作者本人的许多论点,可能还不够成熟,敬请前辈和同行们批评指正!

最后,这本书的写作始终是在哈尔滨工业大学校领导和数学系领导的支持、关心下进行的,特别是前校长杨士勤教授和前系主任吴从炘教授对本书的写作和出版帮助甚大. 多年来,作者的业师、四川大学数学系的孙琦教授也给了很多关心和帮助. 在此作者向他们致以诚挚的感谢!

参 考 文 献

[1]Martin,D. ,Amer. Math. Monthly,80(1973),233-269.

[2]Baker,A. ,Phi. Tran. Roy. Soc. Lon. ,A,263(1967),273-291.

[3]Cassels,J. W. S. ,An introduction to Diophantine Approximation,Camb. Univ. Press,1957.

[4]Katz,N. ,Proc. of Symposia in Pure Math. ,28(1976),275-305. (AMS).

[5]Faltings,G. ,Invent. Math. ,73(1983),349-366.

[6]Heath-Brown,D. R. ,Bull. London Math. Soc. ,17(1985),15-16.

[7]Ljunggren,W. ,Avh. Norske Vid. Akad. Oslo,1,5(1942),#5,27pp.

[8]Guy,R. K. ,Unsolved Problems in Number Theory,D6,25,Springer-Verlag,1981.

[9]Ko,C. (柯召),J. Chinese Math. Soc. ,2(1940),205-207.

[10] Mills,W. H. ,Report Inst. Theory of Numbers,Boulder,Colo. 1959,258-268.

[11]Uchiyama,S. ,Trudy Mat. Inst. Steklov. ,163(1984),237-243.

[12]Cao,Z. F. (曹珍富),Proc. Amer. Math. Soc. ,98(1986),11-16.

解丢番图方程的初等方法

第2章

本章我们将介绍解丢番图方程的常用初等方法，包括简单同余法、分解因子法、无穷递降法、比较素数幂法、二次剩余法、Pell 方程法和递推序列法等. 这为以后各章的专题研究奠定了必备的基础.

2.1 简单同余法

所谓简单同余法，是指对丢番图方程取某个正整数 $M > 1$ 为模来制造矛盾的方法. 这种方法的要点是根据所给方程的特点，选择模 M. 现举例说明.

1. 选择模 $2^a(a > 1)$. 例如方程

$$x_1^2 + x_2^2 = 4x_3 + 3 \tag{1}$$

没有整数解. 可以取模 4：由于

$$x_1^2 \equiv 0,1 \pmod 4, x_2^2 \equiv 0,1 \pmod 4$$

故 $x_1^2 + x_2^2 \equiv 0,1,2 \pmod 4$. 而方程(1) 给出

$$x_1^2 + x_2^2 \equiv 3 \pmod 4$$

这是矛盾的.

利用方程(1)，可以推出，方程

$$x_1^2 + x_2^2 = (4a + 3)x_3^2 \tag{2}$$

仅有整数解 $x_1=x_2=x_3=0$. 这是因为,除去 $x_1=x_2=x_3=0$ 外,可以假设$(x_1,x_2,x_3)=1$. 由(1) 知 $x_3\not\equiv 1(\bmod 2)$,即$x_3\equiv 0(\bmod 2)$,由(2) 推出 x_1,x_2 同奇同偶. 但$(x_1,x_2,x_3)=1$,故 x_1,x_2 只能是同奇. 所以 $x_1^2\equiv x_2^2\equiv 1(\bmod 4)$,(2) 给出 $2\equiv x_1^2+x_2^2=(4a+3)x_3^2\equiv 0(\bmod 4)$,这不可能.

同样道理,对如下的丢番图方程取模 8 知,均无整数解

$$x_1^2+2x_2^2=8x_3+5\text{ 或 }8x_3+7 \tag{3}$$

$$x_1^2-2x_2^2=8x_3+3\text{ 或 }8x_3+5 \tag{4}$$

和

$$x_1^2+x_2^2+x_3^2=4^a(8x_4+7). \tag{5}$$

例如对方程(3),(4),由于对任一数 x,均有 $x^2\equiv 0,1,4(\bmod 8)$,故 $x_1^2+2x_2^2\not\equiv 5,7(\bmod 8)$,$x_1^2-2x_2^2\not\equiv 3,5(\bmod 8)$,即(3) 和(4) 均无整数解. 对方程(5) 显然 $a\geqslant 0$. 如果 $a\geqslant 1$,则对(5) 取模4 知 $x_1\equiv x_2\equiv x_3\equiv 0(\bmod 2)$. 于是可在(5) 两端除去因子 4. 这样不失一般可设 $a=0$,但 $x_1^2+x_2^2+x_3^2\not\equiv 7(\bmod 8)$,因此(5) 无整数解.

利用 $2^a(a>1)$ 为模解不定方程,主要利用以下的一些事实:

1) 对任意整数 x,有 $x^2\equiv 0,1(\bmod 4)$;如 x 为奇数,则 $x^2\equiv 1(\bmod 8)$;

2) 设 $k\geqslant 4$ 时,对任意的 x,有 $x^{2^{k-2}}\equiv 0,1(\bmod 2^k)$.

2. 选择模 $3^a(a\geqslant 1)$. 例如方程

$$(3a+1)x_1^2+(3b+1)x_2^2=3x_3^2 \tag{6}$$

仅有整数解 $x_1=x_2=x_3=0$. 因为除去 $x_1=x_2=x_3=0$ 的解外,可设$(x_1,x_2,x_3)=1$. 于是取模 3 得 $x_1^2+x_2^2\equiv 0(\bmod 3)$,而 $x_1^2\equiv 0,1(\bmod 3)$,故推出 $x_1\equiv x_2\equiv 0(\bmod 3)$,由(6) 推出 $x_3\equiv 0(\bmod 3)$,与$(x_1,x_2,x_3)=1$ 矛盾.

对于三次的丢番图方程,常常需要取模 9. 例如,如下的方程

$$x_1^3+x_2^3+x_3^3=9x_4\pm 4 \tag{7}$$

和

$$x_1^3+2x_2^3+4x_3^3=9x_4^3\quad x_1x_2x_3x_4\neq 0 \tag{8}$$

均无整数解. 因为对任意整数 x,有 $x^3\equiv 0,\pm 1(\bmod 9)$,所以对方程(7) 有 $x_1^3+x_2^3+x_3^3\not\equiv\pm 4(\bmod 9)$,即(7) 无整数解. 而对方程(8),除去 $x_1=x_2=x_3=x_4=0$ 外,不失一般可设$(x_1,x_2,x_3,x_4)=1$. 取模 9 知 $x_1^3+2x_2^3+4x_3^3\equiv 0(\bmod 9)$,故 $x_1\equiv x_2\equiv x_3\equiv 0(\bmod 3)$,由(8) 推出 $x_4\equiv 0(\bmod 3)$,与$(x_1,x_2,x_3,x_4)=1$ 矛盾.

我们还可证方程

$$x_1^3+3x_1^2x_2+x_2^3=9x_3+2 \tag{9}$$

无整数解. 这是因为对(9) 取模 3 知 $x_1+x_2\equiv 2(\bmod 3)$,故有三种情形:

1) $x_1 \equiv x_2 \equiv 1 \pmod 3$;2) $x_1 \equiv 0 \pmod 3$, $x_2 \equiv 2 \pmod 3$;3) $x_1 \equiv 2 \pmod 3$, $x_2 \equiv 0 \pmod 3$. 在1) 时 $x_1^3 \equiv x_2^3 \equiv 1 \pmod 9$,故对(9) 取模9得:$2 + 3x_1^2x_2 \equiv 2 \pmod 9$,此推出 $x_1^2x_2 \equiv 0 \pmod 3$ 与 $x_1 \equiv x_2 \equiv 1 \pmod 3$ 矛盾;在2) 时 $x_1^3 \equiv 0 \pmod 9$, $x_2^3 \equiv 8 \equiv -1 \pmod 9$ 和 $3x_1^2x_2 \equiv 0 \pmod 9$,故(9) 给出 $-1 \equiv 2 \pmod 9$,此也不可能;在3) 时,与2) 类似,(9) 仍无整数解.

由(9) 可知方程

$$x_1^3 + 3x_1^2x_2 + x_2^3 = 9x_3 - 2 \tag{10}$$

也无整数解. 这是因为(10) 可化为

$$(-x_1)^3 + 3(-x_1)^2(-x_2) + (-x_2)^3 = 9(-x_3) + 2.$$

利用方程(9) 和(10) 的结果可以推出,方程

$$x_1^3 + 3x_1^2x_2 + x_2^3 = (9a + 2)x_3^3 \tag{11}$$

仅有整数解 $x_1 = x_2 = x_3 = 0$. 这个结果的证明不难,例如,除开 $x_1 = x_2 = x_3 = 0$,对方程(11) 可不失一般地设 $(x_1, x_2, x_3) = 1$. 当 $x_3 \equiv 0 \pmod 3$ 时,方程(11) 推出 $x_1 \equiv x_2 \equiv 0 \pmod 3$,与 $(x_1, x_2, x_3) = 1$ 矛盾;而当 $x_3 \equiv \pm 1 \pmod 3$ 时,(11) 的右端 $\equiv \pm 2 \pmod 9$,故由(9) 和(10) 的结果知,(11) 不可能.

有些三次丢番图方程还需要取模7,例如方程

$$x_1^3 + 2 = 7x_2 \tag{12}$$

没有整数解. 这是因为 $x_1^3 \equiv 0, \pm 1 \pmod 7$. 利用(12) 的结果,可以证明方程

$$x_1^3 + 2x_2^3 = 7(x_3^3 + 2x_4^3) \tag{13}$$

仅有整数解 $x_1 = x_2 = x_3 = x_4 = 0$. 因为除 $x_1 = x_2 = x_3 = x_4 = 0$ 外,可设方程(13) 的解满足 $(x_1, x_2, x_3, x_4) = 1$. 如果 $7 \nmid x_2$,则 $x_2^3 \equiv \pm 1 \pmod 7$,所以(13) 推出 $(\pm x_1)^3 + 2 \equiv 0 \pmod 7$,由(12) 的结果知,这是不可能的. 如果 $7 \mid x_2$,由(13) 推出 $7 \mid x_1$,可设 $x_1 = 7y_1, x_2 = 7y_2$ 代入(13) 式得出

$$7^2(y_1^3 + 2y_2^3) = x_3^3 + 2x_4^3$$

由前类似可知,上式给出 $7 \mid x_4, 7 \mid x_3$,这与 $(x_1, x_2, x_3, x_4) = 1$ 矛盾.

3. 选择模 p(p 为奇素数). 这种模的选择,主要依据二次剩余、三次剩余和四次剩余的一些熟知结果. 例如,设 a 无平方因子,且 a 含有 $4k + 3$ 形的素因子,则方程

$$x_1^2 + x_2^2 = ax_3^2 \tag{14}$$

仅有 $x_1 = x_2 = x_3 = 0$ 的整数解. 因为除 $x_1 = x_2 = x_3 = 0$ 外,可设方程(14) 的解满足 $(x_1, x_2, x_3) = 1$. 又由 a 含有素因子 $p \equiv 3 \pmod 4$ 知,(14) 给出

$$x_1^2 \equiv -x_2^2 \pmod p$$

由于 $p \mid x_2$ 推出 $p \mid x_1, p^2 \mid ax_3^2$. 又 a 无平方因子,故 $p \mid x_3$ 与 $(x_1, x_2, x_3) = 1$ 矛盾. 故 $p \nmid x_1x_2$,上式给出

$$1=\left(\frac{x_1^2}{p}\right)=\left(\frac{-x_2^2}{p}\right)=\left(\frac{-1}{p}\right)=-1$$

这不可能. 其中$\left(\frac{a}{p}\right)$表勒让德符号.

根据$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$,与上面类似地有方程

$$x_1^2-2x_2^2=a_1x_3^2 \quad a_1 \text{ 无平方因子}$$

和
$$x_1^2+2x_2^2=a_2x_3^2 \quad a_2 \text{ 无平方因子}$$

均仅有整数解$x_1=x_2=x_3=0$. 其中a_1含有素因子$p\equiv\pm3(\mathrm{mod}\ 8)$,$a_2$含有素因子$p\equiv5,7(\mathrm{mod}\ 8)$.

对于三次、四次的丢番图方程,常常需要三次剩余和四次剩余的某些结果. 我们知道,k次剩余符号$\left(\frac{n}{p}\right)_k$定义为设$k>1$,$p-1=kq$,这里$p$是奇素数,则有$\left(\frac{n}{p}\right)_k=(n^q)_p$. 这里$(a)_p$表示$a$模$p$的绝对最小剩余,即$(a)_p\in\left\{-\frac{p-1}{2},\cdots,-1,0,1,\cdots,\frac{p-1}{2}\right\}$. 对于$k=3,4$时有以下几个常用的结果:

1) 设$p\equiv1(\mathrm{mod}\ 6)$,则$\left(\frac{2}{p}\right)_3=1\Longleftrightarrow$存在整数$u,v$使得$p=u^2+27v^2$.

2) 设$p\equiv1(\mathrm{mod}\ 8)$,$p=a^2+b^2$,$4\mid a$,则

$$\left(\frac{2}{p}\right)_4=(-1)^{\frac{a}{4}}$$

3) 设$p\equiv1(\mathrm{mod}\ 4)$,则$\left(\frac{-1}{p}\right)_4=(-1)^{\frac{p-1}{4}}$.

利用1) ~ 3),我们来求解几个丢番图方程.

例1 设p为奇素数,则方程

$$x_1^3=2x_2^3+px_3^3 \quad \left(\frac{2}{p}\right)_3\neq1 \tag{15}$$

仅有$x_1=x_2=x_3=0$的整数解.

证 除去$x_1=x_2=x_3=0$后,可设方程(15)的解满足$(x_1,x_2,x_3)=1$. 于是(15)取模p得

$$x_1^3\equiv2x_2^3(\mathrm{mod}\ p)$$

显然,如$p\mid x_2$,则$p\mid x_1$,推出$p\mid x_3$,与$(x_1,x_2,x_3)=1$矛盾. 所以$p\nmid x_1x_2$,上式给出

$$1=\left(\frac{x_1^3}{p}\right)_3=\left(\frac{2x_2^3}{p}\right)_3=\left(\frac{2}{p}\right)_3\neq1$$

这不可能.