

丢番图方程的计算方法

郭永东 薛国芬 李 由 编著

$$\left| \sum_{i=1}^l C_i \cdot \prod_{j=1}^{s_j} \alpha_{ij}^{n_{ij}} \right| < \min_i \left| C_i \cdot \prod_{j=1}^{s_j} \alpha_{ij}^{n_{ij}} \right|^{\delta}$$

新疆大学出版社

丢番图方程的计算方法

郭永东 薛国芬 李 由

新疆大学出版社

(新)新登字 08 号

责任编辑:王少杰

封面设计:子 辛

丢番图方程的计算方法

郭永东

薛国芬 编著

李 由

出版发行:新疆大学出版社

(乌鲁木齐市胜利路 14 号 邮编:830046)

经 销:新华书店

印 刷:湛江恒辉彩色印刷有限公司

开 本:850×1168 毫米 1/32

印 张:8.875

字 数:191.3 千字

版 次:1995 年 12 月第一版 1995 年 12 月第 1 次印刷

印 数:1-1000 册

ISBN7-5631-0508-5/O·5

定价:18.70 元

序

丢番图方程的求解问题是数论研究中非常重要内容之一。近些年来,由于超越数论等出现了许多重要进展,为丢番图方程求解提供了重要和有效的工具,并形成了求解丢番图方程的近代方法,从而使得一大批丢番图方程获得有效的解决。

本书首先介绍了超越数论和丢番图逼近论中近年出现的著名 Gelfond-Baker 方法, L^3 -算法等基本原理和方法。然后讲述这些方法在一些重要丢番图方程,如 Thue 方程, Thue-Mahler 方程, S -单位方程, S -单位不等式等方面求解问题中的应用。该书既有有关理论的详细论述,又特别着重讲述这些理论如何具体实现几种类型方程的求解问题。这自然包括作者多年从事这一领域的研究成果和总结,同时本书提供的研究方法,可以应用到很多同类型的方程和逼近问题的解决,这对从事本领域研究和工作的同志有重要参考价值。本书也是国内首次介绍这一重要研究方向并有重要价值的一本书。

中国科学院
教学研究所
徐广善

内 容 简 介

丢番图方程是数论中的一个相当活跃的研究领域,本书系统地介绍了以 Baker 方法和 L^3 -算法为基础的计算方法及其在丢番图方程中的应用.本书可供从事计算数论及其相关领域研究的数学工作者以及对此感兴趣的数学系大学生、研究生,中学数学教师和数论爱好者参考.

引 言

在数论中,通常将未知数个数多于方程或不等式个数,并且对未知数的取值加以某些限制(例如限制为整数、正整数等)的方程、方程组和不等式统称为丢番图方程.早在公元三世纪初,古希腊数学家 Diophantus 就已经对此类方程进行了比较系统的研究.我国最早的数学文献《周髀算经》也曾有过此类方程正整数解的记载.因此,丢番图方程是数论中最古老的分支.由于丢番图方程与数论、代数、组合数学等数学分支有着密切的联系,所以它一直是基础数学中的一个相当活跃的研究领域.

如果暂且不考虑不等式的情况,一般的丢番图方程都可以表成以下形式:

$$f(x_1, x_2, \dots, x_m) = 0, \quad x_1, x_2, \dots, x_m \in S,$$

其中 $f(x_1, x_2, \dots, x_m)$ 是未知数 $x_1, x_2, \dots, x_m$ 的函数, S 是未知数取值的集合,该方程的求解就是要找出集合 S 中所有可使 $f(x_1, x_2, \dots, x_m) = 0$ 成立的元素组 $(x_1, x_2, \dots, x_m)$. 具体来说,丢番图方程的种类异常繁多. Dickson 在他的名著《History of the Theory of Numbers》第二卷中,用了八百多页的篇幅也只能对本世纪初以前的工作给出了简要的介绍.但是从总体而言,迄今为止人们讨论较多的主要是以下两类方程.

当 $f(x_1, x_2, \dots, x_m)$ 是 $x_1, x_2, \dots, x_m$ 的整系数多项式时,

称为多项式方程. 如果 $f(x_1, x_2, \dots, x_m)$ 是 n 次多项式, 则称它是 m 元 n 次方程. 例如, 著名的 Fermat 猜想就是要证明: 当 n 是大于 2 的正整数时, 三元 n 次方程

$$x^n + y^n = z^n, \quad x, y, z \in \mathbb{N}$$

无解 (x, y, z) . 在一般情况下, 元数越多, 次数越高, 则相应的多项式方程越不容易解决.

当 $f(x_1, x_2, \dots, x_m)$ 是在指数位置上也有未知数的整系数多项式时, 称为指数型方程. 例如, 至今尚未完全解决的 Catalan 猜想就是要证明: 指数型方程

$$x^m - y^n = 1, \quad x, y, m, n \in \mathbb{N}, \quad x > 1, y > 1, m > 1, n > 1$$

仅有解 $(x, y, m, n) = (3, 2, 2, 3)$.

1900 年, Hilbert 在他的著名演讲中提出了二十三个重要的数学问题, 这些问题直接影响着本世纪数学的发展. Hilbert 的第十问题提出: 对于一般的整系数多项式 $f(x_1, x_2, \dots, x_m)$, 是否存在有限的算法来确定方程

$$f(x_1, x_2, \dots, x_m) = 0, \quad x_1, x_2, \dots, x_m \in \mathbb{Z}$$

的可解性? 1970 年, Davis、Matijasevič 和 Robinson 运用数理逻辑方法否定地解决了这个问题, 即证明了这样的有限算法是不存在的. 上述结果说明了求解丢番图方程的困难程度.

近三十年来, 由于 Baker 和 Lenstra 等人分别在超越数论和丢番图逼近方面的出色工作, 对某些类型的丢番图方程已经有了求解的有限算法. 目前, 这些工作已经形成了数论中最年轻的分支——计算数论的主要内容. 鉴于国内尚未见到这

方面的专门书籍,作者根据近年来学习丢番图方程的计算方法所取得的一点心得编写了本书,以供对此感兴趣的读者参考。

本书的前三章介绍了 Baker 方法、 L^3 -算法等基本方法的原理,后五章分别介绍了这些方法在 Thue 方程、Thue - Mahler 方程、S-单位方程以及 S-单位不等式等丢番图方程求解问题中的应用。

本书第一、二、五章由郭永东编写,第三、四、六章由薛国芬编写,第七、八章由李由编写,全书由薛国芬、郭永东两人总纂。

乐茂华教授审阅了全书并作了一些修改和补充,作者表示感谢。

本书的写作和出版得到了国家自然科学基金和广东省自然科学基金的资助。

吴江先生对本书的出版给予热忱资助,作者深表谢意。

由于作者的水平所限,书中的误谬之处在所难免,切望读者不吝赐教。

作 者

目 录

第一章 绪 论	1
§ 1.1 丢番图方程的解法	1
§ 1.2 Gelfond - Baker 方法	10
§ 1.3 理论的丢番图逼近	13
§ 1.4 计算的丢番图逼近	16
§ 1.5 降低上界的程序	26
第二章 代数数论与超越数论	28
§ 2.1 代数数论	28
§ 2.2 预备引理	30
§ 2.3 p -adic 数及其函数	33
§ 2.4 对数线性型的下界	34
§ 2.5 数值方法	38
第三章 丢番图逼近的计算	43
§ 3.1 导言	43
§ 3.2 实的情形的齐次一维逼近: 连分数	45
§ 3.3 实情形的非齐次一维逼近: Davenport 引理	47
§ 3.4 L^3 -格基简化运算	49
§ 3.5 L^3 -格基简化运算, 实践	54
§ 3.6 寻找所有短格点: Fincke 和 Pohst 运算	62
§ 3.7 实情形的齐次多维逼近: 实逼近格点	64
§ 3.8 实情形的非齐次多维逼近: 对推广的 Davenport 引理的一种取舍	68
§ 3.9 p -adic 情形的非齐次零维逼近	73

§ 3.10	p -adic 情形的齐次一维逼近: p -adic 连分数及 p -adic 数的逼近格	75
§ 3.11	p -adic 情形的齐次多维逼近: p -adic 逼近格	78
§ 3.12	p -adic 情形的非齐次一维及多维逼近	80
§ 3.13	p -adic 逼近格的有用子格	82
第四章	双递归序列的 S -整数	86
§ 4.1	导言	86
§ 4.2	双递归序列	88
§ 4.3	递归序列的增长	91
§ 4.4	上界	99
§ 4.5	一个基本引理	102
§ 4.6	平凡的情形	104
§ 4.7	双曲线型情形的简化运算	110
§ 4.8	椭圆型情形的简化运算	115
§ 4.9	广义 Ramanujan - Nagell 方程	118
§ 4.10	混合的平方指数方程	123
第五章	S -整数不等式 $0 < x - y < y^0$	128
§ 5.1	导言	128
§ 5.2	解的上界	129
§ 5.3	在一维情形降低上界	131
§ 5.4	在多维情形降低上界	134
§ 5.5	表	138
第六章	S -整数方程 $x + y = z$	146
§ 6.1	导言	146
§ 6.2	上界	147

§ 6.3	p -adic 逼近格	150
§ 6.4	在一维情形降低上界	152
§ 6.5	在多维情形降低上界	156
§ 6.6	关于 abc-猜想的例	159
§ 6.7	表	161
第七章	两个 S -单位的和是平方数问题	173
§ 7.1	引言	173
§ 7.2	$D=1$ 的情形	175
§ 7.3	对于一般递归	176
§ 7.4	对于对数线性型	181
§ 7.5	解的上界:概述	187
§ 7.6	解的上界:详述	191
§ 7.7	简化方法	202
§ 7.8	范例	202
§ 7.9	表	215
第八章	Thue 方程	230
§ 8.1	引言	230
§ 8.2	从 Thue 方程到对数线性型	231
§ 8.3	上界	237
§ 8.4	简化上界	242
§ 8.5	应用:三角数是三个连续数的积	247
§ 8.6	Thue-Mahler 方程, 简述	262
参考文献		264

第一章 绪 论

1.1 丢番图方程的解法

本节论及丢番图方程的某些类型. 通常将未知数个数多于方程或不等式个数, 并且对未知数的取值加以某些限制(例如限制为整数, 正整数等)的方程、方程组和不等式统称为丢番图方程.

例如本书将要研究的丢番图方程

$$x^2 + 7 = 2^n$$

(Ramanujan - Nagell 方程, 恰有解 $(\pm x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$, 参见第四章);

$$2^x = 3^y + 5^z$$

(纯指数方程, 恰有解 $(x, y, z) = (1, 0, 0), (2, 1, 0), (3, 1, 1), (5, 3, 1), (7, 1, 3)$, 参见第六章);

$$y^2 = x^3 - 4x + 1$$

(椭圆曲线方程, 恰有 22 个解, 其中最大的解是 $(x, y) = (1274, \pm 45473)$, 参见第八章). 这里提及的三个方程仅是丢番图方程的一些例子. 我们将研究更广泛类型的方程, 我们也研究(在第五章)丢番图不等式(一个式子大于另一个式子的表达式, 其解仍然限制为整数). 在下面的讨论中, 关于丢番图

方程的叙述也适用于丢番图不等式。

本书所论述的方程的共同点是它们都能用相同的方法求解。这种方法实质上由三部分组成：变换，Gelfond - Baker 理论的应用以及丢番图逼近。我们简扼地解释这些步骤。

首先，将方程变换成纯指数方程或不等式，即方程或不等式的未知数都出现在指数，例如上面列举的第二个例子。每一种类型的丢番图方程需用一种特别的变换，因此在此意义上更是特别困难。对于某些例子，象上述第二个例子，这种变换是容易的。另一方面的例子，如上面列举的第一个例子或第三个例子，可以运用代数数论的一些理论，这种例子是很多的。

这种纯指数方程的一般形式如下：

$$\sum_{i=1}^t c_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_j} = c_0 \cdot \prod_{j=1}^{s_0} \alpha_{0j}^{n_j} \quad (1.1)$$

而对应的纯指数不等式形如

$$\left| \sum_{i=1}^t c_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_j} \right| < \min_i \left| c_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_j} \right|^\delta \quad (1.2)$$

其中， $t, s_i, c_i, \alpha_{ij}, \delta$ 是满足 $t, s_i \in \mathbb{N}, 0 < \delta < 1$ 的常数，且 c_i, α_{ij} 属于 $\mathbb{Q}$ 的某代数扩张， n_j 是 $\mathbb{Z}$ 中的未知数。现在我们假定 (1.1) 或 (1.2) 的左边的项数 t 等于 2。这一限制对于第二个步骤是必不可少的，因为我们要运用所谓代数数对数线性型理论的结果，也称为 Gelfond - Baker 理论 (满足 $t > 2$ 的某些特殊类型的指数方程 (1.1) 也可用 Gelfond - Baker 方法来处理，因为他们可转化为满足 $t = 2$ 的形如 (1.2) 的指数不等式，有关这方面的详细情况可参阅文献 [3]、[4]、[114]、[120])。

赋予满足 $t=2$ 的形如 $(1 \cdot 1)$ 或 $(1 \cdot 2)$ 的指数方程或不等式以对数线性型

$$\Lambda = \log \beta_0 + \sum_{i=1}^m n_i \cdot \log \beta_i$$

其中 β_i 是代数常数, n_i 是未知整数. 这里, 对数在某些情况下是实数或复数, 在其他情况下是 p -adic 数. 方程与对数线性型之间的这一关系使得方程的一个大解的线性型十分接近于零(在实的或复的情况下, 或在 p -adic 情况下). Gelfond - Baker 理论提供了有效计算这种代数数的对数线性型的绝对值(特别是 p -adic 值)的下界的方法. 在许多情形下, 这些界已确切计算出来. 把已找到的上界和下界作比较, 就有可能得到指数丢番图方程或不等式的解的有效上界, 导出原来方程解的上界. 不象第一个步骤, 这第二个步骤是相当一般自然的.

我们注意到, 许多研究者已经应用上面概述的方法, 给出了各种各样的丢番图方程解的有效可计算的上界. 作为综述, 请参看文献[107]. 这些研究者常常满足于知道这些上界的存在, 而不实际求出这些上界. 如果他们求出这些上界, 他们也不总是确定方程所有的解. 在本书中, 解丢番图方程总是意味着: 确切地求出方程所有的解.

在第二个步骤之后, 解丢番图的问题就转化为一个有限问题, 这由上述方法的第三个步骤来处理. 换句话说, 因为我们已找到了未知数的绝对值的有效上界, 我们就能检验未知数仅有的有限多种可能. 然而 Gelfond - Baker 理论提供的关于代数数对数线性型的下界中出现的常数相当大. 因此, 实际

上用这种方法能得到的纯指数方程解的上界可以大得象常数 10^{40} 这么大. 上界太大以致不容许将所有可能完全列举, 甚至用现今最快的计算机也做不到.

证明解的绝对值上界存在使得确定所有的解从无限问题归化为有限问题. 因此, Gelfond - Baker 理论的应用(第二个步骤)在一定意义上使无限多次的困难工作归化为进行有限多次的检验(第三个步骤). 而且, 这个检验几乎仅是技术问题而不是数学问题. 尽管如此, 我们认为解决这个比较小的技术问题不仅是非平凡的, 而且包含着重要和有趣的数学问题. 本书期待着举例证明这一见解.

尽管第二个步骤中 Gelfond - Baker 理论的应用实际上产生很大的上界, 一般假定这些上界远非实际上的最大解. 因此, 寻找将这些上界降低到容易处理的大小的方法是很值得研究的. 直接应用原来丢番图方程的某些性质来找出这种方法常常是可能的. 例如大数解必须满足多模或大数模的一定同余式(参见文献[26]、[45]、[96]), 或满足某可逆性条件(参见文献[90]). 这种方法的缺点是仅能用于特殊类型的丢番图方程, 因此, 一般情况下, 对每一种类型的方程必须想出一种新的变换方法. 因此, 对于对数线性型不等式的解降低上界的方法将是有趣的. 导出这样的不等式将可用于解每一类型的丢番图问题.

这种方法的研究是我们所述的解丢番图方程方法的第三个步骤. 在第三个步骤中, 已发表的新的进展是主要的. 我们在第一、第二个步骤的讨论中应用的主要是经典的, 我们将其应用于以前已研究过的各类型的方程, 也用于一些新类型的方程.

第三个步骤需要提供的丢番图逼近理论的方法牵涉到研究如何能使给出变量的值的线性型接近零.在这方面近来已获得重要进展.惊人的进展是1981年L·Lovász创造了所谓 L^3 -格基缩减运算.我们将阐明怎样由 L^3 -运算导出实际有效的丢番图逼近运算,这种方法能用于证明许多丢番图方程在某个区间 $[x_1, x_0]$ 上没有解存在.通常 x_1 是 $\log x_0$ 的数量级.当解被置换为理论的上界 x_0 时,通常一个新的更好的上界 x_1 就可以找到.对许多方程,这种运算的实际应用,仅在几分钟的计算机时之内便可得到初始上界 x_0 .对于那些未找到变换的方法或变换未获成功的方程来说,上述导出了寻找许多类型的丢番图方程所有解的实际方法.

在本书中用于解许多例各种各样的丢番图方程的上述列举的方法,是一种“运算”特征.在一定意义上,它处于“特定的”方法与“理论的”方法之间.这一点我们将在下面解释.设给出带未指定参数的一个丢番图方程集合.作为这样的集合的一个例子,考虑广义Ramanujan-Nagell方程 $x^2 + D = 2^n$,其中 D 是一个参数, x, n 是未知数.

特定的方法是仅对参数的特殊值解方程的方法.它对这些特殊值以外的参数值不适用.解形如 $x^2 + D = 2^n$ 的方程的第一个例子出现在Nagell 1948年的著作中,其中取 $D = 7$.他使用的方法是特定的特征,因为这种方法对参数 D 选取了特殊的固定值7.

理论的方法可以对于参数值是某个大集合导出结果.Gelfond-Baker理论是理论的特征,因为它对许多方程关于它们的参数导出解的上界.另一例子是平方互反性理论的应用,证明了若 D 是任意不小于5的奇数,则方程 $x^2 + D = 2^n$ 没

有解,且关于7不同余(mod 8),而且,1981年Beukers[14]运用超几何函数理论证明了方程 $x^2 + D = 2^n$ 的解 (x, n) 满足 $n < 435 + 10^2 \cdot \log |D|$,而且若 $|D| < 2^{96}$,则又有 $n < 18 + 2^2 \cdot \log |D|$.理论的方法常常太一般以致不能导出给定方程的全部解.

计算的方法是保证对参数值的任一个集合都能进行的方法,但为了导出所有解,这是分别对参数值的每一个特殊集合来进行的.在本书中应用的方法意味着这样一种计算的特征.我们将在第4章中对方程 $x^2 + D = 2^n$ (实际上是对更一般的方程)给出计算的方法.事实上,由于Beukers的上述结果产生解的一个小上界,就能通过枚举所有解的简单方法来降低上界,但是这一方法的计算部分是微不足道的,因此我们宁可将Beukers的方法归为理论上的一类.为了进行Gelfond-Baker理论计算,枚举所有可能是不实用的.因此,确定所有解的更巧妙方法是找到降低大上界的方法.我们注意到Beukers方法对更一般方程 $x^2 + D = p^n$ 也有其特定的方面,因为它仅对某一特殊的值 p 来考虑.我们在第4章中的方法就没有这一缺点.

关于解丢番图方程的想法,可以努力的是设计一种计算机计算程序,一种“丢番图计算机”,仅需将方程的参数输入,短时间之后,所有解就列示出来.我们理应保证(从严格的数学证明的意义说来)没有解被遗漏.

上述列举的方法乍看起来,在本书中叙述这样一种一般适用的解法似乎是较好的选择.换句话说,在第二个步骤中,证明参数已确定的指数丢番图方程的上界,是一种十分一般的特征.第三个步骤,计算丢番图逼近部分,就原理而论也可