

---

# 谈谈不定方程

TANTAN BUDING FANGCHENG

---

柯 召 孙 琦

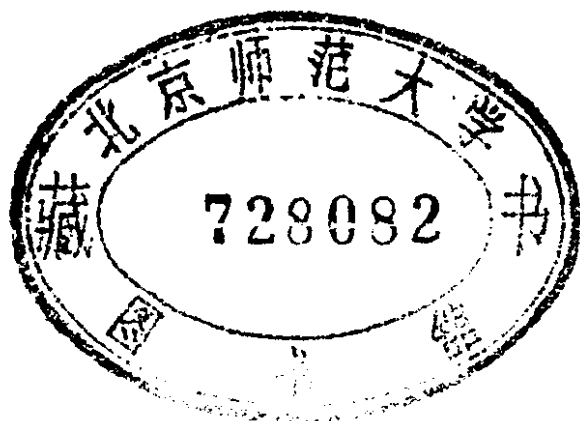


上海教育出版社

# 谈谈不定方程

柯召 孙琦

JY11172/13



上海教育出版社

## 内 容 提 要

不定方程(又称丢番图方程)是数论中一个古老而又有趣的分支。迄今未获彻底解决的费马大定理就是属于不定方程的。由于近年来对不定方程研究有很大进展,这一学科与代数几何、代数数论、组合数学、计算机科学的联系又很密切,因此不定方程仍然引起许多人的兴趣。

本书概括地介绍了不定方程的主要内容。书中谈到了历史上许多著名的问题和猜想,介绍了解决这些问题的方法(大部分是初等方法,少量是代数数论方法),概述了一些近代成果(例如有重大意义的 Baker 的有效方法),等等。可供有志于了解不定方程的中学老师和广大数学爱好者阅读。

### 谈谈不定方程

柯 召 孙 琦

上海教育出版社出版

(上海永福路 123 号)

新华书店上海发行所发行 上海市印刷六厂印刷

开本 787×1092 1/32 印张 5 字数 108,000

1980年8月第1版 1980年8月第1次印刷

印数 1—50,000本

统一书号: 7150·2294 定价: 0.41 元

## 序 言

不定方程是数论中最古老的一个分支。所谓不定方程，简单地讲，就是未知数的个数多于方程的个数，但它们的解受某种限制(如是整数、正整数或有理数等)的方程(组)。例如求  $3x^4 - 2y^2 = 1$  的整数解  $x, y$ ，以及求  $x^2 + 7 = 2^n$  的整数解  $x, n$  等，都是不定方程的求解问题。古希腊数学家丢番图于三世纪初就研究过这样的方程，所以不定方程又称丢番图方程。但实际上，我国古代《周髀算经》就提出了商高定理“勾三股四而弦五”，这表示不定方程  $x^2 + y^2 = z^2$  的一组整数解  $x=3, y=4, z=5$ ，比丢番图早多了。

不定方程的内容极其丰富，与数学的其他分支如代数数论、代数几何、组合数学等也有着密切的联系。近代许多优秀的数学家如费马、欧拉、高斯、拉格朗日、库默(Kummer)、希尔伯特等都从事过不定方程的研究。这些研究大大丰富了数论的内容。近三十年来，这个领域更有重要进展，例如，1968年前后，Baker得到了著名的“有效方法”，定出了一大类不定方程整数解的绝对值的上界。这一结果属于希尔伯特第十问题的特解。所谓希尔伯特第十问题是问能否判定任何整系数多项式  $f(x_1, \dots, x_n) = 0$  有没有整数解，这个问题也在1970年得到了否定的回答。此外，还有一些古老的猜想被解决了。虽然如此，从整个地说，对于高次的多元的不定方程，迄今还只有少数特例被人们搞清楚，还有着广阔的未知领域。这样，就使得不定方程仍然并将继续吸引着许多数学家的注意。

鉴于国内专门介绍不定方程的书较缺，这就促使我们来编写这样一本小册子，其目的是想用初等方法和代数方法比较全面而概括地介绍这一分支，不仅想让读者了解不定方程中有哪些基本的内容、重要的问题和近代的成果，而且希望读者能从中学到一点解决问题的方法。正因为如此，书中的绝大多数定理都给出了证明，这些证明包括了不定方程中一些基本的方法。具有高中和大学一年级数学知识的读者，完全能够读懂书中的绝大多数内容。对于那些希望进一步钻研，有志于在不定方程方面进行研究的读者来说，或许也能从中受到一些启发。最后，这本小册子也写入了我们自己的若干工作。

限于我们的水平，书中的缺点和错误一定不少，我们期待着读者的批评指正。

柯 召 孙 琦

1979年10月于成都

# 目 录

序言	
第一章 一次不定方程	1
§ 1 二元一次不定方程	1
§ 2 $s(s \geq 2)$ 元一次不定方程	4
§ 3 关于一次不定方程的 Frobenius 问题	8
§ 4 联立一次不定方程组	13
第二章 二次不定方程	18
§ 1 Pell 方程 $x^2 - Dy^2 = 1$	18
§ 2 Pell 方程 $x^2 - Dy^2 = -1$	24
§ 3 不定方程 $x^2 - Dy^2 = c$	28
§ 4 高斯关于二元二次方程的一个结果	35
§ 5 不定方程 $x^2 + y^2 = z^2$ 和 $x^2 + 2y^2 = z^2$	37
§ 6 不定方程 $ax^2 + by^2 + cz^2 = 0$	40
第三章 三次不定方程	45
§ 1 解不定方程 $y^2 = x^3 + k$ 的初等方法	46
§ 2 关于代数数论	49
§ 3 解不定方程 $y^2 = x^3 + k$ 的代数数论方法	55
§ 4 一些三元三次不定方程	61
§ 5 不定方程 $x^3 + y^3 + z^3 + w^3 = n$	66
第四章 四次不定方程	69
§ 1 仅有平凡解的四次不定方程	69
§ 2 递归序列与四次不定方程	73
§ 3 不定方程 $x^4 - Dy^2 = 1$	82

第五章 费马大定理	92
§1 初等方法	92
§2 代数数论的方法——库默的工作	97
§3 其他一些结果	107
第六章 与连续整数有关的不定方程	110
§1 不定方程 $y^2+1=x^p$	110
§2 三个连续数的问题	113
§3 不定方程 $x^2+1=y^2$	119
§4 不定方程 $\sum_{j=0}^h (x+j)^n = (x+h+1)^n$	123
第七章 某些指数不定方程	129
§1 一个关于商高数的猜想	129
§2 不定方程 $x^2+7=2^n$	132
§3 不定方程 $x^m y^n = z^2$	137
第八章 某些不定方程整数解的上界	142
§1 从 Thue 的定理谈起	142
§2 几类不定方程解的上界	146
§3 Baker 方法举例	149

# 第一章 一次不定方程

在本书中,凡方程的解如未加说明,都指整数解.

本章将给出一次不定方程有解的充分必要条件和求解的方法. 对于多个一次不定方程联立的某些情形,虽然人们也得出了有解的充分必要条件和求解的方法,但是远不如一个时简单. 一次不定方程与规划论有联系,它还有一些其他方面的应用,例如本章介绍的 Frobenius 问题,就在合理下料等实际问题上有应用.

## §1 二元一次不定方程

二元一次不定方程是指

$$a_1x_1 + a_2x_2 = n, \quad (1)$$

其中  $a_1, a_2, n$  是给定的整数,  $a_1a_2 \neq 0$ .

我们有

**定理 1** 方程(1)有解的充分必要条件是①

$$(a_1, a_2) | n. \quad (2)$$

证 如果(1)有解,显然(2)成立.

反之,不失一般,可设  $(a_1, a_2) = 1$  和  $a_1 > 0, a_2 > 0$ , 如  $a_1 = 1$ , 则解为  $x_1 = n - a_2x_2$ . 若  $a_1 > 1$  我们用辗转相除法来求

---

① 在本书中,常以小写拉丁字母  $a, b, c, \dots$  代表整数;设  $b \neq 0, b$  整除  $a$ , 以  $b|a$  表示;  $(a, b)$  表示  $a, b$  的最大公因数,我们假定读者知道求  $(a, b)$  的辗转相除法.



(1)的一组解. 写

$$a_2 = q_1 a_1 + r_1, \quad 0 < r_1 < a_1, \quad (r_1, a_1) = 1,$$

则 
$$x_1 = -q_1 x_2 + \frac{-r_1 x_2 + n}{a_1} = -q_1 x_2 + x_3,$$

这里

$$r_1 x_2 + a_1 x_3 = n, \quad (3)$$

由于  $x_2, x_3$  的值可以给出  $x_1$ , 这样, 求(1)的解化为求(3)的解. 写

$$a_1 = q_2 r_1 + r_2, \quad 0 < r_2 < r_1, \quad (r_2, r_1) = 1,$$

则 
$$x_2 = -q_2 x_3 + \frac{-r_2 x_3 + n}{r_1} = -q_2 x_3 + x_4,$$

这里

$$r_2 x_3 + r_1 x_4 = n. \quad (4)$$

这样, 求(1)的解化为求(4)的解. 以上步骤继续下去(即通常求最大公因数的方法), 由于  $a_1 > r_1 > r_2 > \dots$ , 在有限步后, 有  $r_{k+1} = 0$ , 而  $r_k = (a_1, a_2) = 1$ , 且

$$r_k x_{k+1} + r_{k-1} x_{k+2} = n,$$

其中  $k \geq 0$ ,  $r_0 = a_1$ ,  $r_{-1} = a_2$ . 于是, 我们把  $x_{k+1} = n - r_{k-1} x_{k+2}$  代入  $x_k$  的表达式, 再把  $x_{k+1}, x_k$  代入  $x_{k-1}$  的表达式,  $\dots$ , 最后可得(1)的含参数  $x_{k+2}$  的解. 证完.

往后, 在(1)有解的情况下, 我们总可以假设  $(a_1, a_2) = 1$ . 以上的后半证明是构造性的, 即证明定理充分性的过程, 实际上就是求(1)的全部解的过程. (1)的全部解, 可由以下定理给出.

**定理 2** 设  $(a_1, a_2) = 1$ , 则(1)的全部解可表为

$$x = x_0 + a_2 t, \quad y = y_0 - a_1 t, \quad (5)$$

其中  $x_0, y_0$  为(1)的一组解,  $t$  为任意整数.

证 设  $t$  为任意整数, 把(5)代入(1)得

$$a_1(x_0 + a_2t) + a_2(y_0 - a_1t) = a_1x_0 + a_2y_0 = n,$$

故  $t$  为任意整数时, (5)均为(1)的一组解.

反之, 设  $x_1, y_1$  为(1)的任意一组解, 由

$$a_1x_1 + a_2y_1 = n$$

和

$$a_1x_0 + a_2y_0 = n$$

可得

$$a_1(x_1 - x_0) + a_2(y_1 - y_0) = 0,$$

因  $(a_1, a_2) = 1$ , 所以  $a_2 | x_1 - x_0$ , 可设

$$x_1 - x_0 = a_2t_1 \quad \text{或} \quad x_1 = x_0 + a_2t_1.$$

则

$$y_1 = y_0 - a_1t_1.$$

这就证明了(1)的任一组解具有形状(5). 证完.

例 求不定方程

$$11x_1 + 15x_2 = 7 \tag{6}$$

的全部解.

由于  $(11, 15) = 1$ , 故(6)有解. 由  $15 = 1 \times 11 + 4$ , 可设

$$x_1 = -x_2 + x_3,$$

这里

$$4x_2 + 11x_3 = 7,$$

由  $11 = 2 \times 4 + 3$ , 可设

$$x_2 = -2x_3 + x_4,$$

这里

$$3x_3 + 4x_4 = 7,$$

由  $4 = 1 \times 3 + 1$ , 可设

$$x_3 = -x_4 + x_5,$$

这里

$$x_4 + 3x_5 = 7,$$

令  $x_5 = t$ , 可得

$$x_1 = -28 + 15t, \quad x_2 = 21 - 11t,$$

其中  $t$  为任意整数.

## § 2 $s (s \geq 2)$ 元一次不定方程

设  $s \geq 2$ ,  $s$  元一次不定方程是指

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = n, \quad (1)$$

其中  $a_i (i=1, \dots, s)$ ,  $n$  都是给定的整数,  $a_1 \cdots a_s \neq 0$ .

我们有

**定理 1** (1) 有解的充分必要条件是

$$(a_1, a_2, \dots, a_s) | n. \quad (2)$$

证 (1) 如有解, 显然 (2) 成立.

反之, 如果 (2) 成立. 不失一般, 可设  $(a_1, \dots, a_s) = 1$ ,  $a_i > 0 (i=1, \dots, s)$ ,  $a_1$  是  $a_1, \dots, a_s$  中最小的数, 写

$$a_j = q_j a_1 + r_j, \quad 0 \leq r_j < a_1,$$

如果  $a_1 = 1$ , 则 (1) 的解为  $x_1 = n - a_2x_2 - \cdots - a_sx_s$ . 如  $a_1 > 1$ , 则  $r_2, \dots, r_s$  中至少有一个不为 0, 设

$$\begin{aligned} x_1 &= x_{s+1} - q_2x_{s+2} - q_3x_{s+3} - \cdots - q_sx_{2s}, \\ x_i &= x_{s+i}, \quad i=2, \dots, s, \end{aligned} \quad (3)$$

把 (3) 代入 (1) 得

$$\begin{aligned} a_1x_{s+1} + r_2x_{s+2} + r_3x_{s+3} + \cdots + r_sx_{2s} &= n, \\ (a_1, r_2, \dots, r_s) &= 1, \end{aligned} \quad (4)$$

因为 (3) 的变换矩阵的行列式为 1, 所以 (1) 的解  $(x_1, \dots, x_s)$  与 (4) 的解  $(x_{s+1}, x_{s+2}, \dots, x_{2s})$  之间是一一对应的. 因此只需解 (4). 不失一般, 设  $r_2$  是  $r_2, \dots, r_s$  中最小的正数, 写

$$\begin{aligned} a_1 &= t_1r_2 + l_1, \quad 0 \leq l_1 < r_2, \\ r_j &= t_jr_2 + l_j, \quad 0 \leq l_j < r_2, \quad j=3, \dots, s, \end{aligned}$$

设  $l_1, l_3, \dots, l_s$  中至少有一个不为 0.

再设

$$\begin{cases} x_{s+1} = x_{2s+1} \\ x_{s+2} = -t_1 x_{2s+1} + x_{2s+2} - t_3 x_{2s+3} - \cdots - t_s x_{3s} \\ x_{s+j} = x_{2s+j}, j = 3, \cdots, s, \end{cases} \quad (5)$$

把(5)代入(4)得

$$\begin{aligned} l_1 x_{2s+1} + r_2 x_{2s+2} + l_3 x_{2s+3} + \cdots + l_s x_{3s} &= n, \\ (l_1, r_2, l_3, \cdots, l_s) &= 1, \end{aligned} \quad (6)$$

因为(5)的变换矩阵的行列式为1, 所以(4)的解与(5)的解之间是一一对应的, 因而(1)的解与(5)的解之间是一一对应的. 因此只需解(6). 设  $l_3$  是  $l_1, l_3, \cdots, l_s$  中最小的正数, 继续作下去, 因为  $a_1 > r_2 > l_3 > \cdots$ , 在有限步之后, 存在  $k \geq 1$  和行列式为1的变换

$$\begin{aligned} x_{(k-1)s+1} &= x_{ks+1} - u_2 x_{ks+2} - u_3 x_{ks+3} - \cdots - u_s x_{ks+s} \\ x_{(k-1)s+j} &= x_{ks+j}, j = 2, \cdots, s. \end{aligned} \quad (7)$$

使得

$$x_{ks+1} + v_2 x_{ks+2} + \cdots + v_s x_{ks+s} = n, \quad (8)$$

再令

$$\begin{aligned} x_{ks+1} &= X_1 - v_2 X_2 - \cdots - v_s X_s, \\ x_{ks+j} &= X_j, j = 2, \cdots, s, \end{aligned} \quad (9)$$

代入(8)得  $X_1 = n$ ,

再将  $X_1 = n$  代入(9)得

$$x_{ks+1} = n - \sum_{j=2}^s v_j X_j, \quad x_{ks+j} = X_j, \quad j = 2, \cdots, s,$$

逐次代入, 最后可得  $x_1, \cdots, x_s$  的一组含  $s-1$  个参数  $X_2, \cdots, X_s$  的解. 证完.

设  $s$  阶方阵  $A$ ,  $A$  的元素均为整数,  $A$  的行列式  $|A| = \pm 1$ , 形如

$$\begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = A \begin{pmatrix} X_1 \\ \vdots \\ X_s \end{pmatrix} \quad (10)$$

的变换叫单位模变换. 由于变换(9)、(7)、…、(3)均为单位模变换, 单位模变换的乘积仍是单位模变换, 因此由定理1的证明, 立即可得

**推论** 存在单位模变换(10), 把  $a_1x_1 + \cdots + a_sx_s$ , ( $a_1, \cdots, a_s$ ) = 1, 变为  $X_1$ .

由定理1的证明还告诉我们(1)的通解含  $s-1$  个参数, 上一节给出了  $s=2$  的通解公式, 由此可推出  $s=3$  时(1)的通解公式,  $s>3$  的情形可以逐步推出. 下面我们来证明

**定理2** 设  $(a, b, c) = 1$ ,  $(a, b) = d$ ,  $a = da_1$ ,  $b = db_1$ , 不定方程

$$ax + by + cz = n \quad (11)$$

的全部解可表为

$$x = x_0 + b_1t_1 - u_1ct_2, \quad y = y_0 - a_1t_1 - u_2ct_2, \quad z = z_0 + dt_2, \quad (12)$$

其中  $x_0, y_0, z_0$  是(11)的一组解,  $u_1, u_2$  满足  $a_1u_1 + b_1u_2 = 1$ ,  $t_1, t_2$  为任意整数.

**证** 对于任意的整数  $t_1, t_2$ , 将(12)代入(11), 易知是(11)的一组解.

反之, 设  $x, y, z$  是(11)的一组解. 由

$$ax_0 + by_0 + cz_0 = n, \quad ax + by + cz = n,$$

可得

$$d(a_1(x - x_0) + b_1(y - y_0)) = -c(z - z_0), \quad (13)$$

由  $(d, c) = 1$ , 故有整数  $t_2$ , 使

$$z = z_0 + dt_2 \quad (14)$$

将(14)代入(13)得

$$a_1(x-x_0) + b_1(y-y_0) = -ct_2, \quad (15)$$

由于  $-u_1ct_2$  和  $-u_2ct_2$  是  $a_1X + b_1Y = -ct_2$  的一组解, 由(15)存在整数  $t_1$ , 使

$$x = x_0 + b_1t_1 - u_1ct_2, \quad y = y_0 - a_1t_1 - u_2ct_2,$$

这就证明了(11)的任一组解可表为形状(12). 证完.

例 求出不定方程

$$25x_1 + 13x_2 + 7x_3 = 4 \quad (16)$$

的全部解.

我们用证明定理 1 充分性的方法来求解. 由于  $25 = 3 \times 7 + 4$ ,  $13 = 1 \times 7 + 6$ , 可设  $x_1 = x_4$ ,  $x_2 = x_5$ ,  $x_3 = -3x_4 - x_5 + x_6$ , 代入(16)得

$$4x_4 + 6x_5 + 7x_6 = 4, \quad (17)$$

由于  $6 = 4 + 2$ ,  $7 = 4 + 3$ , 可设  $x_4 = x_7 - x_8 - x_9$ ,  $x_5 = x_8$ ,  $x_6 = x_9$ , 代入(17)得

$$4x_7 + 2x_8 + 3x_9 = 4, \quad (18)$$

由于  $4 = 2 \times 2$ ,  $3 = 2 + 1$ , 可设  $x_7 = x_{10}$ ,  $x_8 = -2x_{10} + x_{11} - x_{12}$ ,  $x_9 = x_{12}$ , 代入(18)得

$$2x_{11} + x_{12} = 4, \quad (19)$$

最后设  $x_{12} = X_1 - 2X_2$ ,  $x_{11} = X_2$ ,  $x_{10} = X_3$ , 代入(19)得

$$X_1 = 4,$$

故  $x_{12} = 4 - 2X_2$ ,  $x_{11} = X_2$ ,  $x_{10} = X_3$ , 逐次代入, 可得

$$x_1 = -X_2 + 3X_3, \quad x_2 = 3X_2 - 2X_3 - 4,$$

$$x_3 = -2X_2 - 7X_3 + 8, \quad (20)$$

其中  $X_2, X_3$  为任意整数. (20)就是(16)的通解.

### §3 关于一次不定方程的 Frobenius 问题

设  $s \geq 2$ ,  $n$  和  $a_i (i=1, \dots, s)$  都是正整数, 且  $(a_1, \dots, a_s) = 1$ , 考虑一次不定方程

$$a_1 x_1 + \dots + a_s x_s = n \quad (1)$$

的非负解  $x_i \geq 0 (i=1, \dots, s)$  的问题. 在  $s=2$  时, 我们有

**定理 1** 在  $n > a_1 a_2 - a_1 - a_2$  时, (1) 有非负解  $x_1 \geq 0, x_2 \geq 0$ , 但在  $n = a_1 a_2 - a_1 - a_2$  时, (1) 没有非负解  $x_1 \geq 0, x_2 \geq 0$ .

证 由 §1 的定理 1 知

$$a_1 x_1 + a_2 x_2 = n \quad (2)$$

的全部解可表为

$$x_1 = x'_1 + a_2 t, \quad x_2 = x'_2 - a_1 t,$$

其中  $x'_1, x'_2$  是 (2) 的一组解,  $t$  为任意整数. 不难知道, 可取  $t$  使

$$0 \leq x_2 = x'_2 - a_1 t < a_1,$$

即 
$$0 \leq x'_2 - a_1 t \leq a_1 - 1,$$

又由  $n > a_1 a_2 - a_1 - a_2$  可得

$$\begin{aligned} (x'_1 + a_2 t) a_1 &= n - (x'_2 - a_1 t) a_2 \\ &> a_1 a_2 - a_1 - a_2 - (a_1 - 1) a_2 = -a_1, \end{aligned}$$

即 
$$x'_1 + a_2 t > -1,$$

故对上述  $t$  来说

$$x_1 = x'_1 + a_2 t \geq 0,$$

这就证明了  $n > a_1 a_2 - a_1 - a_2$  时, (2) 存在解  $x_1 \geq 0, x_2 \geq 0$ .

如果  $n = a_1 a_2 - a_1 - a_2$ , (2) 有解  $x_1 \geq 0, x_2 \geq 0$ , 则由

$$a_1 a_2 - a_1 - a_2 = a_1 x_1 + a_2 x_2$$

得  $a_1 a_2 = (x_1 + 1) a_1 + (x_2 + 1) a_2,$

因  $(a_1, a_2) = 1,$  可得

$$a_1 | x_2 + 1, \quad a_2 | x_1 + 1,$$

因为  $x_2 + 1 > 0, x_1 + 1 > 0,$  故

$$x_2 + 1 \geq a_1, \quad x_1 + 1 \geq a_2,$$

得  $a_1 a_2 = (x_1 + 1) a_1 + (x_2 + 1) a_2 \geq 2 a_1 a_2,$

此不可能, 所以在  $n = a_1 a_2 - a_1 - a_2$  时, (2) 没有非负解  $x_1 \geq 0, x_2 \geq 0.$  证完.

此定理可简述为: 设  $(a_1, a_2) = 1, a_1 > 0, a_2 > 0,$  凡大于  $a_1 a_2 - a_1 - a_2$  的数必可表为  $a_1 x_1 + a_2 x_2 (x_1 \geq 0, x_2 \geq 0)$  之形状, 但  $a_1 a_2 - a_1 - a_2$  不能表成此形状.

人们自然会提出这样的问题, 对于一般的  $s (s \geq 2)$  元线性型  $a_1 x_1 + \dots + a_s x_s, a_i > 0 (i = 1, \dots, s), (a_1, \dots, a_s) = 1,$  是否存在一个仅与  $a_1, \dots, a_s$  有关的整数  $N(a_1, \dots, a_s),$  凡大于  $N(a_1, \dots, a_s)$  之数必可表为  $a_1 x_1 + \dots + a_s x_s (x_i \geq 0, i = 1, \dots, s)$  的形状? 问题的回答是肯定的. 下面就来证明这个结果.

**定理 2** 存在仅与  $a_1, \dots, a_s$  有关的整数  $N(a_1, \dots, a_s),$  当  $n > N(a_1, \dots, a_s)$  时, (1) 有非负解  $x_1 \geq 0, \dots, x_s \geq 0.$

证 我们对  $s$  施行归纳法.

由定理 1,  $s = 2$  时定理显然成立.

设  $s - 1$  个元时定理成立, 我们来证明  $s$  元时的情形. 设  $(a_1, \dots, a_{s-1}) = d, a_i = a'_i d (i = 1, \dots, s - 1);$  由  $(a_1, \dots, a_s) = 1$  可知  $(d, a_s) = 1,$  从而可把 (1) 化成: 存在  $0 \leq b_s \leq d - 1,$  使  $a_s b_s \equiv n \pmod{d}.$  由 (1) 得

$$a'_1 x_1 + \dots + a'_{s-1} x_{s-1} = \frac{n - a_s b_s}{d}. \quad (3)$$

由于  $(a'_1, \dots, a'_s) = 1,$  由归纳假设, 存在整数  $N(a'_1, \dots,$



$a'_{s-1}$ ), 当  $\frac{n-a_s b_s}{d} \geq \frac{n-a_s(d-1)}{d} > N(a'_1, \dots, a'_{s-1})$  时, (3) 有

非负解  $x_1 = b_1, \dots, x_{s-1} = b_{s-1}$ , 即当

$$n > dN(a'_1, \dots, a'_{s-1}) + a_s(d-1) = N(a_1, \dots, a_s)$$

时, (1) 有非负解  $x_1 = b_1, \dots, x_{s-1} = b_{s-1}, x_s = b_s$ . 证完.

这个定理还告诉我们, 对  $s$  元 ( $s \geq 2$ ) 线性型  $a_1 x_1 + \dots + a_s x_s$ ,  $a_i > 0$  ( $i = 1, \dots, s$ ),  $(a_1, \dots, a_s) = 1$ , 存在一个仅与  $a_1, \dots, a_s$  有关的整数  $g(a_1, \dots, a_s)$ , 凡大于  $g(a_1, \dots, a_s)$  之数必可表为  $a_1 x_1 + \dots + a_s x_s$  ( $x_i \geq 0, i = 1, \dots, s$ ) 的形状, 而  $g(a_1, \dots, a_s)$  不能表为  $a_1 x_1 + \dots + a_s x_s$  ( $x_i \geq 0, i = 1, \dots, s$ ) 的形状, 因此, 称  $g(a_1, \dots, a_s)$  为所给线性型的最大不可表数. 求出  $g(a_1, \dots, a_s)$  的问题, 即所谓一次不定方程的 Frobenius 问题. 由定理 1 知,  $s = 2$  时, Frobenius 问题已告解决: 我们求得  $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$ ; 但是, 对于  $s \geq 3$ , 一般地只找到了求出  $g(a_1, \dots, a_s)$  的一些算法. 对于  $n = 3$ , 我们有

**定理 3<sup>[1]</sup>**

$$g(a, b, c) \leq \frac{ab}{(a, b)} + c(a, b) - a - b - c, \quad (4)$$

且当

$$c > \frac{ab}{(a, b)^2} - \frac{a}{(a, b)} - \frac{b}{(a, b)} \quad (5)$$

时, 有

$$g(a, b, c) = \frac{ab}{(a, b)} + c(a, b) - a - b - c. \quad (6)$$

显然, 以上  $a, b, c$  可以轮换.

证 由 § 2 的 (12) 知,  $ax + by + cz = n$  的全部解可表为

$$x = x_0 + b_1 t_1 - u_1 c t_2, \quad y = y_0 - a_1 t_1 - u_2 c t_2, \quad z = z_0 + d t_2,$$

[1] 柯召, 关于方程  $ax + by + cz = n$ , 四川大学学报(自然科学版), 1 (1955), 1~4.