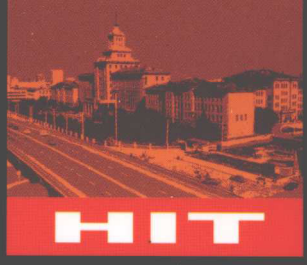
About Indeterminate Equation



数论经典著作系列

谈谈不定方程

柯召　孙琦　编著

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

数论经典著作系列

谈谈不定方程

About Indeterminate Equation

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

内 容 简 介

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.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.

图书在版编目(CIP)数据

谈谈不定方程/柯召,孙琦编著.—哈尔滨:哈尔滨工业大学出版社,2011.3

ISBN 978-7-5603-2870-6

Ⅰ.谈… Ⅱ.①柯…②孙… Ⅲ.①不定方程 Ⅳ.①0122.2

中国版本图书馆 CIP 数据核字(2011)第 080050 号

策划编辑 刘培杰
责任编辑 张永芹
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 8.25 字数 152 千字
版 次 2011 年 3 月第 1 版 2011 年 3 月第 1 次印刷
书 号 ISBN 978-7-5603-2870-6
定 价 28.00 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 $f(x_1,\cdots,x_s)=0$ 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,从整体上说,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，书中的缺点和疏漏一定不少，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

一次不定方程

第一章

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.一次不定方程与线性规划论有联系，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

$$a_1x_1 + a_2x_2 = n \tag{1}$$

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

$$(a_1, a_2) \mid n \tag{2}$$

证 如果(1)有解，显然(2)成立.

① 在本书中，常以小写拉丁字母 $a, b, c, \cdots$ 代表整数；设 $b \neq 0$，b 整除 a，以 $b \mid a$ 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) 的辗转相除方法.

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)的一组解.写

$$a_2=q_1a_1+r_1,0<r_1<a_1,(r_1,a_1)=1$$

则

$$x_1=-q_1x_2+\frac{-r_1x_2+n}{a_1}=-q_1x_2+x_3$$

这里

$$r_1x_2+a_1x_3=n \tag{3}$$

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

$$a_1=q_2r_1+r_2,0<r_2<r_1,(r_2,r_1)=1$$

则

$$x_2=-q_2x_3+\frac{-r_2x_3+n}{r_1}=-q_2x_3+x_4$$

这里

$$r_2x_3+r_1x_4=n \tag{4}$$

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$a_1>r_1>r_2>\cdots$,在有限步后,有$r_{k+1}=0$,而$r_k=(a_1,a_2)=1$,且

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

其中$k\geqslant 0,r_0=a_1,r_{-1}=a_2$.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,……,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$(a_1,a_2)=1$,以上的后一半证明是构造性的,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

$$x=x_0+a_2t,y=y_0-a_1t \tag{5}$$

其中x_0,y_0为(1)的一组解,t为任意整数.

证明 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 $a_2 \mid x_1 - x_0$,可设

$$x_1 - x_0 = a_2t_1 \quad 或 \quad x_1 = x_0 + a_2t_1$$

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

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

其中 t 为任意整数.

§2 $s(s \geqslant 2)$ 元一次不定方程

设 $s \geqslant 2$,s 元一次不定方程是指

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = n \tag{1}$$

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

我们有

定理 1 (1) 有解的充分必要条件是

$$(a_1, a_2, \cdots, a_n) \mid n \tag{2}$$

证 (1) 如有解,显然(2) 成立.

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

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

如果 $a_1 = 1$,则(1) 的解为 $x_1 = n - a_2 x_2 - \cdots - a_s x_s$. 如 $a_1 > 1$,则 $r_2, \cdots, r_s$ 中至少有一个不为 0,设

$$\begin{aligned} x_1 &= x_{s+1} - q_2 x_{s+2} - q_3 x_{s+3} - \cdots - q_s x_{2s} \\ x_i &= x_{s+i}, i = 2, \cdots, s \end{aligned} \tag{3}$$

把(3) 代入(1) 得

$$\begin{gathered} a_1 x_{s+1} + r_2 x_{s+2} + r_3 x_{s+3} + \cdots + r_s x_{2s} = n \\ (a_1, r_2, \cdots, r_s) = 1 \end{gathered} \tag{4}$$

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

$$\begin{gathered} a_1 = t_1 r_2 + l_1, \quad 0 \leqslant l_1 < r_2 \\ r_j = i_j r_2 + l_j, \quad 0 \leqslant l_j < r_2, \quad j = 3, \cdots, s_j \end{gathered}$$

设 $l_1, l_3, \cdots, l_s$ 中至少有一个不为 0.

再设

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

把(5) 代入(4) 得

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

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,继续做下去,因为 $a_1 > r_2 > l_3 > \cdots$,在有限步之后,存在 $k \geqslant 1$ 和行列式为 1 的变换

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

使得

$$x_{ks+1} + v_2 x_{ks+2} + \cdots + v_s x_{ks+s} = n \tag{8}$$

再令

$$\begin{aligned} x_{ks+1} &= X_1 - v_2X_2 - \cdots - v_sX_s \\ x_{ks+j} &= X_j, j = 2, \cdots, s \end{aligned} \tag{9}$$

代入(8)得

$$X_1 = n$$

再将 $X_1 = n$ 代入(9)得

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

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 $\boldsymbol{A}$,$\boldsymbol{A}$ 的元素均为整数,$\boldsymbol{A}$ 的行列式 $|\boldsymbol{A}| = \pm 1$,形如

$$\begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = \boldsymbol{A} \begin{pmatrix} X_1 \\ \vdots \\ X_s \end{pmatrix} \tag{10}$$

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,立即可得如下推论:

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

$$ax + by + cz = n \tag{11}$$

的全部解可表为

$$x = x_0 + b_1t_1 - u_1ct_2, y = y_0 - a_1t_1 - u_2ct_2, z = z_0 + dt_2 \tag{12}$$

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

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

可得

$$d(a_1(x - x_0) + b_1(y - y_0)) = -c(z - z_0) \tag{13}$$

由 $(d, c) = 1$,故有整数 t_2,使

$$z = z_0 + dt_2 \tag{14}$$

将(14)代入(13)得

$$a_1(x - x_0) + b_1(y - y_0) = -ct_2 \tag{15}$$

由于 $-u_1ct_2$ 和 $-u_2ct_2$ 是 $a_1X+b_2Y=-ct_2$ 的一组解，由(15)存在整数 t_1，使

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

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

$$25x_1+13x_2+7x_3=4 \tag{16}$$

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

$$4x_4+6x_5+7x_6=4 \tag{17}$$

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

$$4x_7+2x_8+3x_9=4 \tag{18}$$

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

$$2x_{11}+x_{12}=4 \tag{19}$$

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

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

$$x_3=-2X_2-7X_3+8 \tag{20}$$

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

$$a_1x_1+\cdots+a_sx_s=n \tag{1}$$

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

定理1 在 $n>a_1a_2-a_1-a_2$ 时，(1)有非负解 $x_1\geqslant 0,x_2\geqslant 0$，但在 $n=a_1a_2-a_1-a_2$ 时，(1)没有非负解 $x_1\geqslant 0,x_2\geqslant 0$．

证 由 §1 的定理 1 知

$$a_1x_1 + a_2x_2 = n \tag{2}$$

的全部解可表为

$$x_1 = x'_1 + a_2t, x_2 = x'_2 - a_1t$$

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

$$0 \leqslant x_2 = x'_2 - a_1t < a_1$$

即

$$0 \leqslant x'_2 - a_1t \leqslant a_1 - 1$$

又由 $n > a_1b_1 - a_1 - b_1$ 可得

$$(x'_1 + a_2t)a_1 = n - (x'_2 - a_1t)a_2 >$$

$$a_1a_2 - a_1 - a_2 - (a_1 - 1)a_2 = -a_1$$

即

$$x'_1 + a_2t > -1$$

故对上述 t 来说

$$x_1 = x'_1 + a_2t \geqslant 0$$

这就证明了 $n > a_1a_2 - a_1 - a_2$ 时，(2) 存在解 $x_1 \geqslant 0, x_2 \geqslant 0$.

如果 $n = a_1a_2 - a_1 - a_2$，(2) 有解 $x_1 \geqslant 0, x_2 \geqslant 0$，则由

$$a_1a_2 - a_1 - a_2 = a_1x_1 + a_2x_2$$

得

$$a_1a_2 = (x_1 + 1)a_1 + (x_2 + 1)a_2$$

因 $(a_1, a_2) = 1$，可得

$$a_1 \mid x_2 + 1, a_2 \mid x_1 + 1$$

因为 $x_2 + 1 > 0, x_1 + 1 > 0$，故

$$x_2 + 1 \geqslant a_1, x_1 + 1 \geqslant a_2$$

得

$$a_1a_2 = (x_1 + 1)a_1 + (x_2 + 1)a_2 \geqslant 2a_1a_2$$

此不可能，所以在 $n = a_1a_2 - a_1 - a_2$ 时，(2) 没有非负解 $x_1 \geqslant 0, x_2 \geqslant 0$. 证完.

此定理可简述为：设 $(a_1, a_2) = 1, a_1 > 0, a_2 > 0$，凡大于 $a_1a_2 - a_1 - a_2$ 的数必可表为 $a_1x_1 + a_2x_2 (x_1 \geqslant 0, x_2 \geqslant 0)$ 之形状，但 $a_1a_2 - a_1 - a_2$ 不能表示成此形状.

人们自然会提出这样的问题，对于一般的 $s (s \geqslant 2)$ 元线性型 $a_1x_1 + \cdots + a_sx_s, a_i > 0 (i = 1, \cdots, s), (a_1, \cdots, a_s) = 1$，是否存在一个仅与 $a_1, \cdots, a_s$ 有关的整数 $N(a_1, \cdots, a_s)$，凡大于 $N(a_1, \cdots, a_s)$ 之数必可表为 $a_1x_1 + \cdots + a_sx_s (x_i \geqslant 0, i = 1, \cdots, s)$ 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 $a_1,\cdots,a_s$ 有关的整数 $N(a_1,\cdots,a_s)$，当 $n > N(a_1,\cdots,a_s)$ 时，(1) 有非负解 $x_1 \geqslant 0,\cdots,x_s \geqslant 0$.

证　我们对 s 施行归纳法.

由定理 1，$s = 2$ 时定理显然成立.

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

$$a_1' x_1 + \cdots + a_{s-1}' x_{s-1} = \frac{n - a_s b_s}{d} \tag{3}$$

由于 $(a_1',\cdots,a_s') = 1$，由归纳假设，存在整数 $N(a_1',\cdots,a_{s-1}')$，当

$$\frac{n - a_s b_s}{d} \geqslant \frac{n - a_s(d-1)}{d} > N(a_1',\cdots,a_{s-1}')$$

时，(3) 有非负解 $x_1 = b_1,\cdots,x_{s-1} = b_{s-1}$，即当

$$n > dN(a_1',\cdots,a_{s-1}') + a_s(d-1) = N(a_1,\cdots,a_s)$$

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

这个定理还告诉我们，对 s 元 $(s \geqslant 2)$ 线性型 $a_1x_1 + \cdots + a_sx_s, a_i > 0 (i = 1,\cdots,s)$，$(a_1,\cdots,a_s) = 1$，存在一个仅与 $a_1,\cdots,a_s$ 有关的整数 $g(a_1,\cdots,a_s)$，凡大于 $g(a_1,\cdots,a_s)$ 之数必可表为 $a_1x_1 + \cdots + a_sx_s (x_i \geqslant 0, i = 1,\cdots,s)$ 的形状，而 $g(a_1,\cdots,a_s)$ 不能表为 $a_1x_1 + \cdots + a_sx_s (x_i \geqslant 0, i = 1,\cdots,s)$ 的形状，因此，称 $g(a_1,\cdots,a_s)$ 为所给线性型的最大不可表数. 求出 $g(a_1,\cdots,a_s)$ 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 $g(a_1,a_2) = a_1a_2 - a_1 - a_2$；但是，对于 $s \geqslant 3$，一般的只找到了求出 $g(a_1,\cdots,a_s)$ 的一些算法. 对于 $n = 3$，我们有

定理 3①

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

且当

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

时，有

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

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

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

$$x = x_0 + b_1t_1 - u_1ct_2, y = y_0 - a_1t_1 - u_2ct_2, z = z_0 + dt_2$$

其中 x_0, y_0, z_0 是 $ax + by + cz = n$ 的一组解，$(a,b) = d, a = da_1, b = db_1$，$u_1, u_2$ 满足 $a_1u_1 + a_2u_2 = 1$，t_1, t_2 为任意整数. 不难知道，可取整数 t_2 使

$$0 \leqslant z = z_0 + dt_2 \leqslant d - 1$$

对于这样的 t_2，还可以取适当的 t_1，使得

$$0 \leqslant x = x_0 + b_1t_1 - u_1ct_2 \leqslant b_1 - 1$$

对于上面选定的 t_1, t_2，在 $n > \frac{ab}{(a,b)} + c(a,b) - a - b - c$ 时，有

$$b(y_0 - a_1t_1 - u_2ct_2) = n - ax - cz \geqslant n - a(b_1 - 1) - c(d - 1) =$$

$$n - ab_1 - cd + a + c =$$

$$n - \frac{ab}{(a,b)} - c(a,b) + a + c > -b$$

即得

$$y > -1 \text{ 或 } y = y_0 - a_1t_1 - u_2ct_2 \geqslant 0$$

这就证明了(4).

现在，我们来证明由(5)可推出式(6). 由于 $\frac{ab}{(a,b)} = da_1b_1, c(a,b) = cd$；若设 $g(a,b,c)$ 可表，即

$$g(a,b,c) = da_1b_1 + cd - a - b - c = ax + by + cz$$

则有

$$d(a_1b_1 + c) = da_1(x + 1) + db_1(y + 1)c(z + 1) \tag{7}$$

由于 $(d,c) = 1$，式(7)推出 $d \mid z + 1$；令 $z + 1 = dk$，由 $z \geqslant 0$，故 $k > 0$，代入式(7)并在两端消去 d，得

$$a_1b_1 + c = a_1(x + 1) + b_1(y + 1) + ck$$

则有

$$a_1b_1 = a_1(x + 1) + b_1(y + 1) + c(k - 1) \tag{8}$$

如果 $k = 1$，由 $(a_1, b_1) = 1$，式(8)推出 $a_1 \mid y + 1, b_1 \mid x + 1$，加之 $y + 1 > 0$，$x - 1 > 0$，有 $y + 1 \geqslant a_1, x + 1 \geqslant b_1$，这时式(8)给出矛盾结果 $a_1b_1 \geqslant 2a_1b_1$. 如果 $k > 1$，式(8)给出 $a_1b_1 \geqslant a_1 + b_1 + c$，与(5)矛盾. 故式(6)成立. 证完.

从式(5)及定理1，立刻可得：

推论1 如果 $(a,b) = 1, c > g(a,b)$，则

$$g(a,b,c) = g(a,b)$$

推论2 设 $a = \lambda\mu, b = \mu\gamma, c = \gamma\lambda, \lambda > 0, \mu > 0, \gamma > 0, (\lambda,\mu) = (\mu,\gamma) = (\lambda,\gamma) = 1$，则

$$g(a,b,c) = 2\lambda\mu\gamma - \lambda\mu - \mu\gamma - \gamma\lambda$$

证 由于

$$\gamma\lambda > \frac{\lambda\mu \cdot \mu\gamma}{\mu^2} - \frac{\lambda\mu}{\mu} - \frac{\mu\gamma}{\mu} = \gamma\lambda - \lambda - \gamma$$

故有

$$g(a,b,c) = \frac{\lambda\mu \cdot \mu\gamma}{\mu} + \mu\gamma\lambda - \lambda\mu - \mu\gamma - \gamma\lambda =$$

$$2\mu\gamma\lambda - \lambda\mu - \mu\gamma - \gamma\lambda$$

例 设 $a = 12, b = 13, c = 28$,由于

$$28 > \frac{12 \times 13}{(12,13)^2} - \frac{12}{(12,13)} - \frac{13}{(12,13)}$$

不能成立,只能得出

$$g(a,b,c) \leqslant \frac{12 \times 13}{(12,13)} + 28(12,13) - 12 - 13 - 28 = 131$$

但如果将 a,b,c 作如下轮换:$a \to c \to b \to a$,用轮换所得公式,当

$$b > \frac{ca}{(c,a)^2} - \frac{c}{(c,a)} - \frac{a}{(c,a)}$$

则

$$g(a,b,c) = g(c,a,b) = \frac{ca}{(c,a)} + b(a,c) - a - b - c$$

此时

$$13 > \frac{28 \times 12}{(28,12)^2} - \frac{28}{(28,12)} - \frac{12}{(28,12)} = 21 - 7 - 3 = 11$$

故

$$g(a,b,c) = \frac{28 \times 12}{(28,12)} + 13(28,12) - 28 - 12 - 13 = 83$$

即线性型 $12x + 13y + 28z$ 的最大不可表数为 83.

§4 联立一次不定方程组

对于联立的情形,我们首先证明

定理 1 设 $L_r(x) = a_{r1}x_1 + \cdots + a_{rs}x_s (r = 1,\cdots,s), a_{ij} \geqslant 0, i,j = 1,\cdots,s$,是 s 个整系数的线性型,设其系数矩阵 $\boldsymbol{D} = (a_{ij})$,且 $|\boldsymbol{D}| > 0$,则存在单位模变换

$$\begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = \boldsymbol{P} \begin{pmatrix} X_1 \\ \vdots \\ X_s \end{pmatrix} \tag{1}$$

变 $L_r(x)(r = 1,\cdots,s)$ 为