数学奥赛辅导丛书

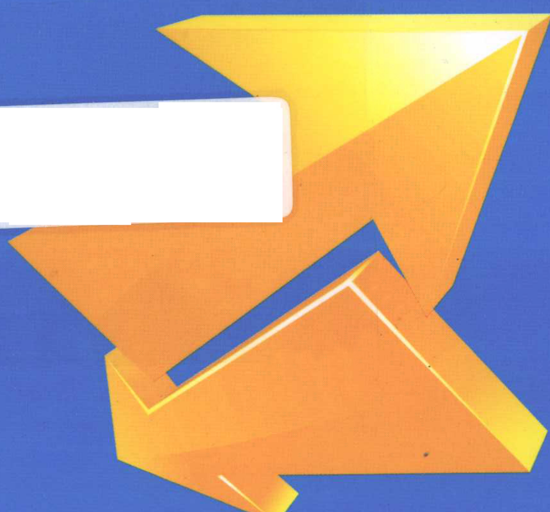
第二辑

不定方程

Buding Fangcheng

第2版

单 墫 余红兵 著



中国科学技术大学出版社

数学奥赛辅导丛书·第二辑

不定方程

第2版

单 墫 余红兵 著

中国科学技术大学出版社

图书在版编目(CIP)数据

不定方程/单墫,余红兵著. —2 版. —合肥:中国科学技术大学出版社,2012.2

(数学奥赛辅导丛书·第二辑)

ISBN 978-7-312-02913-4

Ⅰ.不… Ⅱ.①单… ②余… Ⅲ. 不定方程—高中—教学参考资料 Ⅳ.G634.623

中国版本图书馆 CIP 数据核字(2011)第 236691 号

中国科学技术大学出版社出版发行

地址:安徽省合肥市金寨路 96 号,230026

网址:http://press.ustc.edu.cn

合肥现代印务有限公司印刷

全国新华书店经销

*

开本:880 mm×1230 mm 1/32 印张:5.875 字数:132 千

1991 年 9 月第 1 版 2012 年 2 月第 2 版

2012 年 2 月第 2 次印刷

定价:14.00 元

再版前言

这本小册子于 1991 年初版，至今已有二十余年了. 这次再版，仅更动了很少的地方，基本保持了原来的面貌.

作者

前　言

不定方程肇源极古，我国古代算书《周髀算经》中已记载着“勾三股四弦五”的结论，这实际上给出了三元二次不定方程 $x^2+y^2=z^2$ 的一组整数解．一千七百多年前的古希腊数学家丢番图(Diophantus)对不定方程作过很多研究，因此，不定方程也称为丢番图方程．

随着数学的不断发展，不定方程的重要性日益显著．现代数学的重要分支，如代数数论，代数几何，表示理论……都在这里交汇．不定方程几乎成为一块试金石，用以检验新的数学理论和新的数学方法．

本书是为丰富中学生的数学知识而写的小册子．为便于学生学习，尽量使用初等方法来讨论在初等数学(特别是各级数学竞赛)中经常遇到的不定方程．学生阅读不定方程所需的一些整数知识，在本书的附录中也作了阐述，可供参考．

作者

目　　录

再版前言……………………………………………………（Ⅰ）
前言…………………………………………………………（Ⅲ）
1　一次不定方程 ……………………………………………(001)
2　一次不定方程组 …………………………………………(023)
3　分解 ………………………………………………………(036)
4　估计 ………………………………………………………(046)
5　同余 ………………………………………………………(062)
6　恒等式 ……………………………………………………(079)
7　佩尔方程 …………………………………………………(089)
8　勾股数 ……………………………………………………(103)
9　无穷递降法 ………………………………………………(118)
10　杂例………………………………………………………(137)
11　习题………………………………………………………(157)
12　习题解答概要……………………………………………(161)
附录　整数的基本知识………………………………………(173)

1 一次不定方程

考虑一个古老的问题：

笼子中装有若干只三脚怪兽和山羊，共有 23 只脚，如果怪兽多于 1 只，问：其中有多少只脚是怪兽的？

设 x 为笼子中的怪兽数，y 为山羊数，则有

$$3x + 4y = 23. \tag{1.1}$$

很明显，这个二元一次方程有无穷多组实数解. 但这里要求 x 和 y 都是正整数.

方程(1.1)的正整数解可以用尝试法来求，先将方程(1.1)变形为

$$x = \frac{23 - 4y}{3}.$$

由于 x 和 y 必须是正整数，而当 $y>5$ 时，x 为负数，所以 $y\leqslant 5$. 令 $y=1,2,3,4,5$，并算出相应的 x 值，如表 1.1 所示.

表 1.1

y	1	2	3	4	5
x	$\frac{19}{3}$	5	$\frac{11}{3}$	$\frac{7}{3}$	1

因此，方程(1.1)有两组正整数解：$x=5$，$y=2$ 及 $x=1$，$y=5$. 但原问题中指明笼中怪兽多于 1 只，所以怪兽有 5 只，从而有 15 只脚是怪兽的.

像(1.1)这样的方程,未知数的个数多于方程的个数,而解的取值范围有某种限制(如必须为有理数、整数、正整数等),就称为不定方程(组).

如无特别说明,本书中字母均代表整数.并且,我们只讨论不定方程的整数解.

本章,我们先讨论二元一次不定方程

$$ax + by = c, \tag{1.2}$$

其中 a, b, c 都是已知的整数,且 a, b 不全为 0.

方程(1.2)显然有无穷多组实数解.它甚至有无穷多组有理数解,因为(不妨设 $b \neq 0$)x 可任取一个有理数值 r,解出 $y = \frac{c - ar}{b}$,也是有理数.

但方程(1.2)不一定有整数解.

例 1 证明:不定方程

$$10x - 5y = 48$$

没有整数解.

证明 用反证法.假设方程有一组整数解 $x = x_0, y = y_0$,则有

$$10x_0 - 15y_0 = 48,$$

即

$$5(2x_0 - 3y_0) = 48.$$

上式左端能被 5 整除,但右边不能.这就导出矛盾.

论证的关键是 10 和 15 的最大公约数 5 不能整除方程的常数项 48.由此可见,方程(1.2)有整数解的必要条件是 a, b 的最大公约数整除 c,即 $(a, b) \mid c$(于是,如果读者愿意的话,可以随

手写出许多没有整数解的二元一次方程).

条件$(a,b)\mid c$也是充分的,这就是下面的定理1.它是不定方程中最基本的结论.

定理1 设a,b,c都是整数,且a,b不全为0,则不定方程

$$ax+by=c \tag{1.2}$$

有整数解的充分必要条件是$(a,b)\mid c$.

证明 考虑集合

$$S=\{ax+by\mid x,y\text{是任意整数}\}.$$

这样,方程有整数解的充分必要条件是$c\in S$.

请注意,集合S的元素全是整数,并且有两个简单的性质:

(i)如果$m,n\in S$,则$m\pm n\in S$;

(ii)如果$m\in S$,k是任意整数,则$km\in S$.

因为$m,n\in S$,则有整数x_1,y_1,x_2,y_2,使得

$$m=ax_1+by_1,\quad n=ax_2+by_2,$$

从而

$$m\pm n=a(x_1\pm x_2)+b(y_1\pm y_2)\in S.$$

类似地,可以证明性质(ii).

S中有正整数(例如$|a|,|b|$都在S中).设d是S中的最小正整数,我们证明S中所有的数都是d的倍数.

对任意的$m\in S$,由带余除法可知存在整数q,r,使

$$m=dq+r\quad(0\leqslant r<d).$$

由$d\in S$及性质(ii)知$dq\in S$.又$m\in S$,再由性质(i)得出$r=m-dq\in S$.但$0\leqslant r<d$,d是S中的最小正数,所以$r=0$,即$m=qd$.

特别地,$a,b\in S$都是d的倍数,因而d是a,b的一个公因

数,故由最大公约数的性质知$d\mid(a,b)$.

下面证明 $d=(a,b)$. 由于 $d\in S$,所以存在整数 x,y 使得

$$d = ax + by.$$

但$(a,b)\mid a$,$(a,b)\mid b$,因而$(a,b)\mid d$,故由已证的 $d\mid(a,b)$可知 $d=(a,b)$.

S 中的数都是(a,b)的倍数. 由性质(ⅱ),(a,b)的倍数也都在 S 中. 所以,S 就是(a,b)的倍数所成的集合.

我们已经说过,方程(1.2)有整数解的充分必要条件是 $c\in S$,这结论就等价于$(a,b)\mid c$. 证毕.

例 2 判断不定方程

$$51x + 45y = 357$$

是否有整数解.

解 为求出(51,45),我们将 51 和 45 作素因数分解:

$$51 = 3\times 17,\quad 45 = 3^2\times 5,$$

因此$(51,45)=3$. 显然 $3\mid 357$,由定理 1 可知原不定方程有整数解.

例 3 证明:不定方程

$$ax + by = (a,b) \tag{1.3}$$

有整数解,其中 a,b 是不全为 0 的整数.

证明 由于$(a,b)\mid(a,b)$,由定理 1,方程(1.3)有整数解.

(1.3)就是著名的裴蜀(Bézout)恒等式. 特别地,在整数 a,b 互素即$(a,b)=1$ 时,有整数 x,y 使得

$$ax + by = 1. \tag{1.4}$$

方程(1.3)及方程(1.4)在数论中用处甚多.

注 1.1 当方程(1.2)有整数解时,可以假设$(a,b)=1$. 因

为由定理 1，这时$(a,b)\mid c$，将方程(1.2)两边同除以(a,b)就化为同解方程

$$\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=\frac{c}{(a,b)},$$

而$\frac{a}{(a,b)}$与$\frac{b}{(a,b)}$互素，这在研究方程(1.2)的一般理论时经常用到.

定理 1 虽然给出了判别方程(1.2)是否有整数解的法则，但并未告诉我们在有解时怎样实际地求出解来. 这件事将在下面解决.

当$|a|$，$|b|$都不太大时，尝试法是可行的.

例 4 判断方程

$$7x+15y=1\,989 \tag{1.5}$$

是否有整数解. 如果有，试求出一组解.

解 因为$(7,15)=1$整除 1 989，由定理 1 可知方程(1.5)有整数解，为求方程(1.5)的一组解，可以先求方程

$$7x+15y=1 \tag{1.6}$$

的一组整数解. 不难看出$x=-2$，$y=1$是方程(1.6)的一组整数解. 所以$x=-2\times1\,989$，$y=1\,989$是方程(1.5)的一组整数解.

从定理 1 已经看到，方程(1.2)的求解与(a,b)有密切的关系，求(a,b)的一种方法是将a，b分解(如例 2). 但一个大整数的素因数分解并非易事(试分解$2^{101}-1$). 另一种求(a,b)的方法是欧几里得算法(辗转相除法). 它的优点之一是顺便给出了方程(1.2)的求解方法.

欧几里得算法 设a，b都是整数，$b>0$，则按下述方式反复作带余除法，余数的值严格递降，有限步后余数必为 0：

用 b 除 a，

$$a = bq_0 + r_0 \quad (0 < r_0 < b);$$

用 r_0 除 b，

$$b = r_0 q_1 + r_1 \quad (0 < r_1 < r_0);$$

用 r_1 除 r_0，

$$r_0 = r_1 q_2 + r_2 \quad (0 < r_2 < r_1);$$

……

用 r_{n-1}除 r_{n-2}，

$$r_{n-2} = r_{n-1} q_n + r_n \quad (0 < r_n < r_{n-1});$$

用 r_n 除r_{n-1}，

$$r_{n-1} = r_n q_{n+1}.$$

作最后一步除法后，余数为 0. 这时$(a,b) = r_n$.

例 5 判断方程

$$5\,767x + 4\,453y = -1\,679 \tag{1.7}$$

是否有整数解.

解 将 5 767 及 4 453 作标准分解并不容易. 为了求(5 767，4 453)，我们作欧氏算法如下(请对照上面的一般形式，取 $a = 5\,767$，$b = 4\,453$)：

$$5\,767 = 4\,453 \times 1 + 1\,314,$$

$$4\,453 = 1\,314 \times 3 + 511,$$

$$1\,314 = 511 \times 2 + 292,$$

$$511 = 292 \times 1 + 219,$$

$$292 = 219 \times 1 + 73,$$

$$219 = 73 \times 3.$$

所以$(5\,767, 4\,453) = 73$. 不难验证(作除法)$1\,679 = 73 \times 23$，即

$73 \mid 1\,679$，由定理 1 可知方程(1.7)有整数解.

欧氏算法不仅是求(a,b)的实用方法，实际上我们还能借助它来求得方程

$$ax+by=(a,b) \tag{1.3}$$

的一组整数解.请注意，有了方程(1.3)的一组整数解(x,y)，便立刻得出方程(1.2)的一组解$\left(\frac{c}{(a,b)}x,\frac{c}{(a,b)}y\right)$.这样，我们顺便又给了定理 1 中充分性的另一种证法，这证法是构造性的.求方程(1.3)的一组解的具体做法是将前面说的欧氏算法倒推回去：

由算法中的倒数第二行，得到

$$(a,b)=r_n=r_{n-2}-r_{n-1}q_n,$$

这就将(a,b)表示成r_{n-2}，r_{n-1}的整系数的线性组合.用算法中在其前面的一行

$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}$$

代入上式，消去r_{n-1}，得

$$\begin{aligned}(a,b)&=r_{n-2}-(r_{n-3}-r_{n-2}q_{n-1})q_n\\&=r_{n-2}(1+q_{n-1}q_n)-r_{n-3}q_n.\end{aligned}$$

再用

$$r_{n-4}=r_{n-3}q_{n-2}+r_{n-2}$$

代入，消去r_{n-2}，得

$$(a,b)=r_{n-3}\times 整数+r_{n-4}\times 整数,$$

继续做下去，便求得整数x，y，使

$$ax+by=(a,b).$$

我们看一个用倒推法求方程(1.3)的一组解的具体例子.

例 6 求出方程

$$5\,767x + 4\,453y = -1\,679 \tag{1.7}$$

的一组整数解.

解 应用例5中的欧氏算法,将算法倒推回去,有

$$\begin{aligned}73 &= 292 - 219 \times 1\\ &= 292 - (511 - 292 \times 1)\\ &= 2 \times 292 - 511\\ &= 2 \times (1\,314 - 511 \times 2) - 511\\ &= 2 \times 1\,314 - 5 \times 511\\ &= 2 \times 1\,314 - 5 \times (4\,453 - 1\,314 \times 3)\\ &= 17 \times 1\,314 - 5 \times 4\,453\\ &= 17 \times (5\,767 - 4\,453 \times 1) - 5 \times 4\,453\\ &= 17 \times 5\,767 - 22 \times 4\,453.\end{aligned}$$

因此,$x = 17$,$y = -22$ 是方程

$$5\,767x + 4\,453y = 73$$

的一组整数解.从而方程(1.7)有一组整数解 $x = 17 \times \left(\frac{-1\,679}{73}\right) = -391$,$y = -22 \times \left(\frac{-1\,679}{73}\right) = 506$.

例7 判断方程

$$107x + 73y = 230 \tag{1.8}$$

是否有整数解.若有,试求出一组解.

解 如果看出107及73都是素数(从而它们互素),便立即得知方程有整数解.我们也可以作欧氏算法:

$$\begin{aligned}107 &= 73 \times 1 + 34,\\ 73 &= 34 \times 2 + 5,\\ 34 &= 5 \times 6 + 4,\end{aligned}$$

$$5 = 4 \times 1 + 1,$$
$$4 = 1 \times 4.$$

因此(107,73) = 1,所以方程(1.8)有整数解.要求得一组解,可以像例 6 那样地进行.但列成下面的表格,则更为方便.

表 1.2 中的第二行为各次带余除法所得的商(最后一次的商 4 不载入表中).

表 1.2

n	-1	0	1	2	3	4
q_{n-1}			1	2	6	1
x_n	1	0	1	2	13	15
y_n	0	1	1	3	19	22

第一、二列是固定的.第三行的其他数由递推公式

$$x_n = q_{n-1}x_{n-1} + x_{n-2}$$

算出.第四行由公式

$$y_n = q_{n-1}y_{n-1} + y_{n-2}$$

算出.最后得到

$$x_4 = 15, \quad y_4 = 22,$$

则

$$x = (-1)^{4-1}x_4, \quad y = (-1)^4 y_4.$$

即 $x = -15, y = 22$ 是方程

$$107x + 73y = 1$$

的一组解,于是 $x = -15 \times 230, y = 22 \times 230$ 是方程(1.8)的一组整数解.

我们再用上面的方法求例 6 中方程

$$5\,767x + 4\,453y = 73$$

的一组解. 由例 5 中的欧氏算法得出表 1.3.

表 1.3

n	-1	0	1	2	3	4	5
q_{n-1}			1	3	2	1	1
x_n	1	0	1	3	7	10	17
y_n	0	1	1	4	9	13	22

所以 $x_5=17$, $y_5=22$, 则 $x=(-1)^{5-1}x_5=17$, $y=(-1)^5 y_5=-22$是所求的一组解.

我们已建立了判别方程(1.2)是否有解的法则, 并且在有解时能够实际地求得一组解(这组解通常称为方程(1.2)的一组特解). 然而这仅仅走了第一步. 一般来说, 考虑不定方程有下述三个步骤(请注意, 问题的难度随之而增):

(ⅰ) 判断方程是否有整数解. 如果有, 求出一组解;

(ⅱ) 判别方程是否有无穷多组整数解;

(ⅲ) 求出方程的全部整数解.

方程(1.2)如果有解, 是否一定有无穷多组解呢? 答案是肯定的. 因为设 $x=x_0$, $y=y_0$ 是方程(1.2)的一组解, 则 $x=x_0+bt$, $y=y_0-at$ (t 是任意整数)都是方程(1.2)的整数解(请读者自己代入验证). 要求出方程(1.2)的全部整数解也并不困难. 这时我们可以设 $(a,b)=1$ 来讨论(见注 1.1).

定理 2 设 $(a,b)=1$, $x=x_0$, $y=y_0$ 是方程

$$ax+by=c \tag{1.2}$$

的一组解(特解), 则其全部整数解(通解)为

$$\begin{cases} x=x_0+bt, \\ y=y_0-at. \end{cases} \tag{1.9}$$

这里 t 是任意整数.(1.9)一般称为方程(1.2)的通解公式.

证明 上面已经说过,(1.9)给出的 x,y 都是方程(1.2)的解,所以只要证明方程(1.2)的任意一组整数解都可写成(1.9)的形式.设(x',y')是方程(1.2)的一组解,则

$$ax'+by'=c.$$

再由

$$ax_0+by_0=c,$$

两式相减得

$$a(x_0-x')+b(y_0-y')=0, \tag{1.10}$$

因此

$$a\mid b(y_0-y').$$

但$(a,b)=1$,故 $a\mid(y_0-y')$.于是有

$$y_0-y'=at,$$

其中 t 为整数,即

$$y'=y_0-at.$$

代入方程(1.10),得 $x'=x_0+bt$.证毕.

当$(a,b)>1$时,如方程(1.2)有整数解,则其全部整数解为

$$\begin{cases} x=x_0+\dfrac{b}{(a,b)}t, \\ y=y_0-\dfrac{a}{(a,b)}t, \end{cases}$$

这里(x_0,y_0)是方程(1.2)的一组特解,t 是任意整数.

由(1.9)不难看出,方程(1.2)的整数解 x,y 分别组成公差为 b 及 $-a$ 的(两端无限的)等差数列.对于方程(1.2)的两组不同特解,相应的通解表达式(1.9)的形式虽不完全一样,但由此得出的方程(1.2)的解集是相同的.