青年科學叢書

方程式的整數解

蓋里馮德著

中国青年出版社

青年科學叢書

方程式的整數解

蓋里馮德著
劉尼譯

中国青年出版社
一九五五年·北京

書號 663　數理化 66

方程式的整數解

著　者　〔蘇聯〕蓋里馮德

譯　者　劉尼

青年·開明聯合組設

出版者　中國青年出版社

北京東四12條老君堂11號

總經售　新華書店

印刷者　北京中國青年出版社印刷廠

開本 787×1092 1/32　　一九五五年四月北京第一版

印張 2 1/16　　一九五五年四月北京第一次印刷

字數 38,000　　印數 1—27,000

北京市書刊出版業營業許可證出字第036號

定價 0.24 元

序

這本書是根據我1951年在莫斯科大學數學競賽會上宣讀過的方程式整數解的講演稿編寫的. 我利用這個機會,順便向我的學生戈羅博夫(Н. М. Коробов)講師致謝,他依照我講演稿的大綱,幫助我編寫了第一、第二兩節和第三節的一部分.

這本書對於高年級的中學生是不難了解的.

A. 蓋里馮德

目　　次

緒　言

數論基本上研究的是自然數列中數的算術性質，換句話說，就是正整數的算術性質，它是一門古老的數學。所謂數的解析理論中的一個中心問題，就是自然數列中質數分佈的問題。只能夠被自己和 1 除盡的任何大於 1 的正整數，叫做質數。自然數列中質數分佈的問題，在於研究當數值 N 很大時，小於 N 的質數的數目的變化規律。在這方面，第一個結果，我們可以在歐幾里得（公元前四世紀）的著作裏找到，即質數列是無限的證明。而在歐幾里得以後的第二個結果，是十九世紀後半期偉大的俄國數學家切貝雪夫（П. Л. Чебышев）得到的。數論的另外一個基本問題，就是關於用某種類型的整數和來表示整數的問題，例如用三個質數的和來表示一個奇數的問題。後面一個問題，就是哥特巴赫問題，是在不久以前，由數論的傑出代表、蘇聯數學家維諾格拉多夫（И. М. Виноградов）解決的。

請讀者注意，這本書講的也是數論中特別有趣味的一部分，即方程式的整數解。

求具有一個以上未知數的整數係數代數方程式的整數解，是數論中一個很困難的問題。許多古代最卓越的數學家都曾經研究過許多這樣的問題，例如希臘數學家畢達果拉斯（公元前六世紀），亞歷山大城的丟番圖（公元二-三世紀）以及

比較近代的最優秀數學家飛馬(十七世紀),歐拉(十八世紀),拉格朗奇(十八世紀)等等. 不管若干代卓越數學家們怎樣努力,在這個領域中,仍然缺乏某種一般性的方法,能夠用來解決非常複雜的解析數論的問題,如像維諾格拉多夫的三角法的和那一類型的方法那樣.

求方程式整數解的問題,結局只解決了二元二次方程式的問題. 我們注意,對於一元任意次方程式來說,這個問題並沒有多大用處,因爲這個問題可以借助於有限個數目的試驗來解決. 對於高於二次的二元或多元方程式,不只是求一切整數解的問題,甚至於更簡單的,確定這樣的解是有限或無限多的問題都是極困難的.

求方程式的整數解不只具有理論的利益. 這樣的方程式有時在物理學中也會遇到.

方程式整數解的理論利益是非常鉅大的,因爲這些方程式和許多數論問題都有密切聯系. 除此以外,在這書裏敍述的這種方程式的初步理論,對於中學生、專科學校和高等師範教員,用來擴大數學的眼界也是可能有效的.

在這本書裏,我們敍述了方程式整數解在理論上得到的幾個主要結果. 書裏敍述的定理,在它的證明非常簡易的時候,我們就給與證明.

一　一元方程式

我們來研究一元一次方程式

$$a_1x+a_0=0. \tag{1}$$

設方程式的係數 a_1 和 a_0 是整數. 很明白地，這個方程式的解

$$x=-\frac{a_0}{a_1},$$

只有在 a_0 能夠被 a_1 整除的時候，它才是整數. 由此可知，方程式(1)不是隨時都有整數解的；例如，這兩個方程式

$$3x-27=0 \text{ 和 } 5x+21=0$$

中，第一個具有整數解 $x=9$，而第二個就不可能有整數解.

在次數高於一的方程式中，我們也遇到同樣的情形：二次方程式

$$x^2+x-2=0$$

具有整數解 $x_1=1$，$x_2=-2$；方程式

$$x^2-4x+2=0$$

就不可能有整數解，因爲它的根 $x_{1,2}=2\pm\sqrt{2}$ 是無理數.

關於求出整數係數的 n 次方程式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0=0 \quad (n\geqslant 1) \qquad (2)$$

的整數根，這個問題很容易解決. 事實上，設 $x=\alpha$ 是這個方程式的整數根，那末

$$a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots\cdots+a_1\alpha+a_0=0,$$

$$a_0=-\alpha(a_n\alpha^{n-1}+a_{n-1}\alpha^{n-2}+\cdots\cdots+a_1).$$

從末了一個等式可以看出，a_0 能被 α 除盡；由此可知，方程式(2) 的每一個整數根都是這個方程式絕對項的因數. 要求出這個方程式的整數解，就應當從 a_0 的因數中去挑選，把挑選出的數代入方程式，方程式就會變成恆等式. 例如，從方程式

$$x^{10}+x^7+2x^3+2=0$$

的絕對項分解出來的一切因數 $1,-1,2$ 和 -2 中，只有 -1 是

這個方程式的根. 由此可知,這個方程式具有唯一的整數根 $x=-1$. 用同樣的方法,容易證明,方程式

$$x^6-x^5+3x^4+x^2-x+3=0$$

不可能有整數根.

求多元方程式的整數解是很有趣的.

二 二元一次方程式

我們來研究二元一次方程式

$$ax+by+c=0, \tag{3}$$

這兒 a 和 b 是零以外的整數,而 c 是任意的整數. 我們將認定係數 a 和 b 不具有 1 以外的公因數⊖. 事實上,如果這兩個係數有 1 以外的最大公因數 $d=(a,b)$,則等式

$$a=a_1d, \quad b=b_1d,$$

是正確的;而方程式(3)就具有這樣的形式

$$(a_1x+b_1y)d+c=0,$$

因而只有在 c 能被 d 整除的情況,它才能夠具有整數解. 這樣一來,在 $(a,b)=d\neq1$ 的情況下,方程式(3)的一切係數都應當能夠被 d 整除,並且用 d 除(3),使方程式成爲

$$a_1x+b_1y+c_1=0 \qquad (c_1=\frac{c}{d}),$$

方程式的係數 a_1 和 b_1 就是互質數.

我們首先研究當 $c=0$ 時的情形. 將方程式(3)改寫成這樣:

⊖ 這樣的數 a 和 b 叫做**互質數**;我們用 (a,b) 來表示兩個數 a 和 b 的最大公因數,對於互質數就得 $(a,b)=1$.

$$ax+by=0, \tag{3'}$$

對於 x 解這個方程式，得：

$$x=-\frac{b}{a}y.$$

很明白地，當 y 被 a 除得盡的時候，在這種情形也只有在這種情形，x 才具有整數值． 但 a 的倍數的一切整數 y，可以表示成這樣

$$y=at,$$

這兒 t 可以取任何整數值($t=0, \pm1, \pm2, \cdots\cdots$)．將這個 y 的值代入上面的方程式，則

$$x=-\frac{b}{a}at=-bt,$$

於是我們得到包括方程式(3′)的一切整數解的公式：

$$x=-bt,\ y=at\ (t=0, \pm1, \pm2, \cdots\cdots).$$

現在我們進到 $c\neq0$ 的情形．

我們首先證明，要求方程式(3)的一切整數解，只須找出它的任何一組解就夠了，也就是求出這樣的整數 x_0, y_0，使得

$$ax_0+by_0+c=0.$$

〔定理 1〕 設 a 和 b 是互質數，$[x_0, y_0]$ 是方程式

$$ax+by+c=0 \tag{3}$$

的某一組解㊀；則公式

$$x=x_0-bt,\ y=y_0+at, \tag{4}$$

取 $t=0, \pm1, \pm2, \cdots\cdots$ 就給出方程式(3)的一切解．

〔證明〕 設 $[x, y]$ 是方程式(3)的任何一組解．則從等式

㊀ 一對適合於方程式的整數 x 和 y，叫做一組解，而用$[x, y]$表示．

$$ax+by+c=0 \quad 和 \quad ax_0+by_0+c=0,$$

我們得：

$$ax-ax_0+by-by_0=0; \quad y-y_0=\frac{a(x_0-x)}{b}.$$

因為 $y-y_0$ 是整數，並且 a 和 b 是互質數，則 x_0-x 必須能夠被 b 整除，即 x_0-x 具有這樣的形式

$$x_0-x=bt,$$

這兒 t 是整數．於是

$$y-y_0=\frac{abt}{b}=at,$$

並且我們得：

$$x=x_0-bt, \quad y=y_0+at.$$

這樣一來，就證明了任何一組解 $[x,y]$ 具有形式(4)．還剩下來檢查一下，由公式(4)取整數 $t=t_1$，得出來的任何一對數 $[x_1,y_1]$ 都是方程式(3)的解．為了施行這樣的檢查，將數值

$$x_1=x_0-bt_1, \quad y_1=y_0+at_1$$

代入方程式(3)的左邊，

$$\begin{aligned}ax_1+by_1+c&=ax_0-abt_1+by_0+abt_1+c\\&=ax_0+by_0+c,\end{aligned}$$

但因為 $[x_0,y_0]$ 是一組解，所以 $ax_0+by_0+c=0$，由此可見

$$ax_1+by_1+c=0,$$

即 $[x_1,y_1]$ 是方程式(3)的一組解，這定理就完全證明了．

這樣一來，倘若知道了方程式

$$ax+by+c=0$$

的一組解，則其他的一切解可由算術級數求出來，這算術級數

的一般項具有這樣的形式

$$x=x_0-bt,\ y=y_0+at\quad (t=0,\pm1,\pm2,\cdots\cdots).$$

我們注意，在 $c=0$ 時，前面求得的解的公式

$$x=-bt,\quad y=at$$

可以從剛才得到的公式

$$x=x_0-bt,\ y=y_0+at$$

中去掉 $x_0=y_0=0$ 得出來 這是可以做到的，因爲數值 $x=0$, $y=0$ 總是方程式

$$ax+by=0$$

的一組解。

在 $c\neq0$ 的一般情況，怎樣求出方程式(3)的某一組解 $[x_0,y_0]$ 呢？我們先來舉一個例子。

設已知方程式是

$$127x-52y+1=0.$$

我們要改變未知數的係數的比。

首先，分出假分數 $\frac{127}{52}$ 的整數部分：

$$\frac{127}{52}=2+\frac{23}{52}.$$

用等於 $\frac{23}{52}$ 的分數 $\frac{1}{\frac{52}{23}}$ 來代替眞分數 $\frac{23}{52}$。我們得到：

$$\frac{127}{52}=2+\frac{1}{\frac{52}{23}}.$$

把所得分母的假分數 $\frac{52}{23}$，也作同樣的改變：

$$\frac{52}{23}=2+\frac{6}{23}=2+\frac{1}{\frac{23}{6}}.$$

現在,原來的分數已可化成這樣的形式

$$\frac{127}{52}=2+\cfrac{1}{2+\cfrac{1}{\frac{23}{6}}}.$$

對於分數 $\frac{23}{6}$ 再作同樣的演算:

$$\frac{23}{6}=3+\frac{5}{6}=3+\frac{1}{\frac{6}{5}}.$$

於是

$$\frac{127}{52}=2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{\frac{6}{5}}}}.$$

分出假分數 $\frac{6}{5}$ 的整數部分:

$$\frac{6}{5}=1+\frac{1}{5},$$

我們得到最後的結果:

$$\frac{127}{52}=2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{5}}}}.$$

我們得到了叫做有限連分數或有限連鎖分數的式子.去掉這個連分數的最後一個分數五分之一,將所得的新連分數化成普通分數,並且從原來的分數 $\frac{127}{52}$ 減去它:

$$2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1}}}=2+\cfrac{1}{2+\cfrac{1}{4}}=2+\frac{4}{9}=\frac{22}{9},$$

$$\frac{127}{52}-\frac{22}{9}=\frac{1143-1144}{52\cdot 9}=-\frac{1}{52\cdot 9}.$$

把所得的式子通分，並且去掉分母；則

$$127\cdot 9-52\cdot 22+1=0.$$

把所得的等式和方程式

$$127x-52y+1=0$$

相比較，得 $x=9$, $y=22$ 是這個方程式的一組解，並且依照定理它的一切解必包括在級數

$$x=9+52t,\ y=22+127t\ (t=0,\pm1,\pm2,\cdots\cdots)$$

裏面.

所得的結果提供出這樣的觀念，卽在一般的情況，要求方程式

$$ax+by+c=0$$

的整數解，就應當將未知數係數的比化成連分數，去掉它的最後一個分數，並且完成上面所作的類似的計算.

爲了證明這個命題，必須用到連分數的某些性質.

我們來研究既約分數 $\frac{a}{b}$，用 q_1 表示 a 除以 b 的商，用 r_2 表示餘數. 則得

$$a=q_1b+r_2,\quad r_2<b.$$

其次，設 q_2 是 b 除以 r_2 的商，r_3 是餘數. 則

$$b=q_2r_2+r_3,\quad r_3<r_2,$$

同樣

$$r_2=q_3r_3+r_4,\quad r_4<r_3,$$
$$r_3=q_4r_4+r_5,\quad r_5<r_4,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

數值 $q_1, q_2, \cdots\cdots$ 叫做**部分商**．上面引用的構成部分商的過程叫做**歐幾里得算法**．除得的餘數 r_2，r_3，……適合於不等式

$$b>r_2>r_3>r_4>\cdots\cdots\geqslant 0, \tag{5}$$

就是，它們構成一個非負數的遞降數列．

因為這些非負數的整數不超過 b，個數不能無限，所以在過程中的某一步，部分商的構成就終止了，由此以後輪到的餘數 r 就變成了零．設 r_n 是數列(5)中最後一個不等於零的餘數，則 $r_{n+1}=0$，而歐幾里得算法對於數整 a 和 b 具有這樣的形式

$$\left.\begin{aligned} a&=q_1b+r_2,\\ b&=q_2r_2+r_3,\\ r_2&=q_3r_3+r_4,\\ &\cdots\cdots\cdots\cdots\\ r_{n-2}&=q_{n-1}r_{n-1}+r_n,\\ r_{n-1}&=q_nr_n. \end{aligned}\right\} \tag{6}$$

我們將所得的等式改寫成這樣形式：

$$\frac{a}{b}=q_1+\frac{1}{\dfrac{b}{r_2}},$$

$$\frac{b}{r_2}=q_2+\frac{1}{\dfrac{r_2}{r_3}},$$

………………

$$\frac{r_{n-2}}{r_{n-1}}=q_{n-1}+\frac{1}{\frac{r_{n-1}}{r_n}},$$

$$\frac{r_{n-1}}{r_n}=q_n.$$

用這些等式中第二行的相當值來代替第一行的$\frac{b}{r_2}$，用第三行的相當值來代替第二行的$\frac{r_2}{r_3}$，這樣做下去，我們得到 $\frac{a}{b}$ 化成的連分數，

$$\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cdots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}}.$$

在連分數中，從某一部分開始，把在它以後的全部去掉，這樣得到的式子，叫做連分數的**近似分數**．第一近似分數 δ_1 是由去掉從 $\frac{1}{q_2}$ 起的一切部分得到的：

$$\delta_1=q_1<\frac{a}{b}.$$

第二近似分數 δ_2，是由去掉從 $\frac{1}{q_3}$ 起的一切部分得到的：

$$\delta_2=q_1+\frac{1}{q_2}>\frac{a}{b}.$$

同樣地

$$\delta_3=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}<\frac{a}{b},$$

$$\delta_4=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4}}}>\frac{a}{b},$$

等等.

依據構成近似分數的方法,就產生明顯的不等式

$$\delta_1<\delta_3<\cdots\cdots<\delta_{2k-1}<\frac{a}{b};\ \delta_2>\delta_4>\cdots\cdots>\delta_{2k}>\frac{a}{b}.$$

我們將第 k 個近似分數 δ_k 寫成這樣的形式

$$\delta_k=\frac{P_k}{Q_k}\quad(1\leqslant k\leqslant n),$$

而求構成這個近似分數的分子和分母的法則. 我們改變起首幾個近似分數 $\delta_1, \delta_2, \delta_3$ 的形式:

$$\delta_1=q_1=\frac{q_1}{1}=\frac{P_1}{Q_1};\qquad P_1=q_1,\qquad Q_1=1;$$

$$\delta_2=q_1+\frac{1}{q_2}=\frac{q_1q_2+1}{q_2}=\frac{P_2}{Q_2};\qquad P_2=q_1q_2+1,\ Q_2=q_2;$$

$$\delta_3=q_1+\frac{1}{q_2+\frac{1}{q_3}}=q_1+\frac{q_3}{q_2q_3+1}=\frac{q_1q_2q_3+q_1+q_3}{q_2q_3+1}=\frac{P_3}{Q_3};$$

$$P_3=q_1q_2q_3+q_1+q_3,\quad Q_3=q_2q_3+1.$$

由此可得:

$$P_3=P_2q_3+P_1;\quad Q_3=Q_2q_3+Q_1.$$

我們用歸納法⊖來證明,相應於這個情況

$$P_k=P_{k-1}q_k+P_{k-2},\quad Q_k=Q_{k-1}q_k+Q_{k-2},\tag{7}$$

對於一切 $k\geqslant3$ 的數都成立.

事實上,設對於某一個 $k\geqslant3$ 的數等式 (7) 成立,從近似分數的定義直接就可以得出下面的情況: 在式子 δ_k 裏,用 $q_k+\frac{1}{q_{k+1}}$ 來代替 q_k, δ_k 就變成了 δ_{k+1}. 根據歸納法的假設,

⊖ 參看這一套叢書裏索明斯基(И. С. Соминский)著的'數學歸納法',國立技術理論書籍出版社,1950 年出版(已有中譯本, 高徹譯,中國青年出版社出版.——譯者註).