Nanjing Univ. J. Math. Biquarterly, 19(2002), no.1, 61–67.

关于线性丢番图方程组和线性同余式组

潘 颢　　孙 智 伟

(南 京 大 学 数 学 系)

摘要 在本文中我们证明了整系数线性方程组

$$\begin{cases} a_{11}x_1+\cdots+a_{1l}x_l=b_1 \\ a_{21}x_1+\cdots+a_{2l}x_l=b_2 \\ \cdots\cdots\cdots\cdots \\ a_{k1}x_1+\cdots+a_{kl}x_l=b_k \end{cases}$$

有整数解当且仅当对任何 $1\le i_1<\cdots<i_h\le k$ 及 $1\le j_1<\cdots<j_{h-1}\le l$ 诸

$$\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & a_{i_1j} \\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & a_{i_2j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & a_{i_hj} \end{vmatrix} \quad (j=1,\cdots,l)$$

的最大公因数整除

$$\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & b_{i_1} \\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & b_{i_2} \\ \vdots & \ddots & \vdots & \vdots \\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & b_{i_h} \end{vmatrix}.$$

我们还证明了，$k>l$ 时含未知数 $x_1,\cdots,x_l$ 的 k 个线性同余式有公解当且仅当其中任何 $l+1$ 个同余式有公解。

关键词 线性丢番图方程组，线性同余式组，整数解

中图法分类号 O156.7

一、引 言

设 $a_1,\cdots,a_l,b\in\mathbb{Z}$。熟知线性丢番图方程

$$a_1x_1+\cdots+a_lx_l=b \tag{1}$$

本文第二作者受到了教育部高校优秀青年教师教学科研奖励基金与国家自然科学基金的资助.

第一作者简介：潘颢，男， 1979 年 5 月生，现为第二作者指导的研究生.

有整数解当且仅当 $a_1,\cdots,a_l$ 的最大公因数 $(a_1,\cdots,a_l)$ 整除 b. 著名的中国剩余定理 (又称孙子定理) 断言 $m_1,\cdots,m_k$ 为两两互素的正整数时, 对任何 $b_1,\cdots,b_k\in\mathbb{Z}$ 丢番图方程组

$$\begin{cases} m_1x_1+x_{k+1}=b_1\\ m_2x_2+x_{k+1}=b_2\\ \qquad\cdots\cdots\\ m_kx_k+x_{k+1}=b_k \end{cases} \tag{2}$$

总有整数解 (参看 [1]). 1989 年孙智伟在 [2] 中证明了整系数丢番图方程组

$$\begin{cases} a_1x_1+\cdots+a_lx_l=b\\ c_1x_1+\cdots+c_lx_l=d \end{cases} \tag{3}$$

有整数解当且仅当 (3) 中两个方程分别有解, 且对 $i=1,\cdots,l$ 都有

$$\left(\left|\begin{matrix}a_i & a_1\\ c_i & c_1\end{matrix}\right|,\cdots,\left|\begin{matrix}a_i & a_l\\ c_i & c_l\end{matrix}\right|\right)\ \Big|\ \left|\begin{matrix}a_i & b\\ c_i & d\end{matrix}\right|. \tag{4}$$

在本文中我们将推广上述结果, 给出一般的整系数线性方程组有整数解的简明充要条件。我们的主要结果如下:

定理 1. 设 $a_{i1},\cdots,a_{il},b_i\in\mathbb{Z}$ $(i=1,\cdots,k)$. 则有 $x_1,\cdots,x_l\in\mathbb{Z}$ 使得

$$\begin{cases} a_{11}x_1+\cdots+a_{1l}x_l=b_1\\ a_{21}x_1+\cdots+a_{2l}x_l=b_2\\ \qquad\cdots\cdots\cdots\cdots\\ a_{k1}x_1+\cdots+a_{kl}x_l=b_k, \end{cases} \tag{5}$$

当且仅当对任何 $1\le i_1<\cdots<i_h\le k$ 及 $1\le j_1<\cdots<j_{h-1}\le l$, 最大公因数

$$\left(\left|\begin{matrix}a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & a_{i_11}\\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & a_{i_21}\\ \vdots & \ddots & \vdots & \vdots\\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & a_{i_h1}\end{matrix}\right|,\cdots,\left|\begin{matrix}a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & a_{i_1l}\\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & a_{i_2l}\\ \vdots & \ddots & \vdots & \vdots\\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & a_{i_hl}\end{matrix}\right|\right) \tag{6}$$

整除

$$\left|\begin{matrix}a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & b_{i_1}\\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & b_{i_2}\\ \vdots & \ddots & \vdots & \vdots\\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & b_{i_h}\end{matrix}\right|. \tag{7}$$

从定理 1 我们可导出

定理 2. 设 $a_{ij},b_i,m_i\in\mathbb{Z}$ $(i=1,\cdots,k;\ j=1,\cdots,l)$. 则 $k>l$ 时线性同余式组

$$\begin{cases} a_{11}x_1+\cdots+a_{1l}x_l\equiv b_1\pmod{m_1}\\ a_{21}x_1+\cdots+a_{2l}x_l\equiv b_2\pmod{m_2}\\ \qquad\cdots\cdots\cdots\cdots\\ a_{k1}x_1+\cdots+a_{kl}x_l\equiv b_k\pmod{m_k} \end{cases} \tag{8}$$

有解当且仅当其中任何 $l+1$ 个同余式有公解。

注. $m_1=\cdots=m_k=0$ 时 (8) 退化成 (5)。

定理 2 中取 $l=1$ 立得

推论. 设 $a_i,b_i,m_i\in\mathbb{Z}$ $(i=1,\cdots,k)$. 则

$$\begin{cases} a_1x\equiv b_1 \pmod{m_1} \\ a_2x\equiv b_2 \pmod{m_2} \\ \quad\cdots\cdots \\ a_kx\equiv b_k \pmod{m_k} \end{cases}$$

有整数解当且仅当对任何 $1\le i\le j\le k$ 同余式组

$$\begin{cases} a_ix\equiv b_i \pmod{m_i} \\ a_jx\equiv b_j \pmod{m_j} \end{cases}$$

有解。

注. 上述推论是中国剩余定理的推广，孙智伟在 [2] 中用归纳法证明了它。

二、定理 1、2 的证明

定理 1 的证明：先证必要性。设整数 $x_1,\cdots,x_l$ 适合 (5)，$1\le i_1<\cdots<i_h\le k$ 且 $1\le j_1<\cdots<j_{h-1}\le l$。记 (7) 中行列式为 D，则

$$D=\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & \sum\limits_{j=1}^{l}a_{i_1j}x_j \\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & \sum\limits_{j=1}^{l}a_{i_2j}x_j \\ \vdots & \ddots & \vdots & \vdots \\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & \sum\limits_{j=1}^{l}a_{i_hj}x_j \end{vmatrix}=\sum_{j=1}^{l}x_j\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & a_{i_1j} \\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & a_{i_2j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & a_{i_hj} \end{vmatrix},$$

从而 (6) 中最大公因数整除 D.

再证充分性。让

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kl} \end{pmatrix},\quad B=\begin{pmatrix} & b_1 \\ & b_2 \\ A & \vdots \\ & b_k \end{pmatrix}.$$

任给 $1\le h\le\min\{k,l\}$，由条件知 A 的所有 h 阶子行列式的最大公因数 (称为 A 的 h 阶不变因子) 等于 B 的所有 h 阶子行列式的最大公因数。$k\le l$ 时由华罗庚 [3] 知方程组

$$A\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_l \end{pmatrix}=\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix}$$

有整数解，即丢番图方程组 (5) 有解。

如果 $k>l$，则 (5) 等价于方程组

$$\begin{cases} a_{11}x_1+\cdots+a_{1l}x_l+0x_{l+1}+\cdots+0x_k=b_1\\ a_{21}x_1+\cdots+a_{2l}x_l+0x_{l+1}+\cdots+0x_k=b_2\\ \qquad\cdots\cdots\cdots\cdots\\ a_{k1}x_1+\cdots+a_{kl}x_l+0x_{l+1}+\cdots+0x_k=b_k. \end{cases}$$

它有整数解是因为 $1\le i_1<\cdots<i_h\le k$ 且 $1\le j_1<\cdots<j_{h-1}\le l$ 时诸

$$\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & a_{i_1j}\\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & a_{i_2j}\\ \vdots & \ddots & \vdots & \vdots\\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & a_{i_hj} \end{vmatrix} \quad (1\le j\le l)$$

的最大公因数整除

$$\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & 0\\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & 0\\ \vdots & \ddots & \vdots & \vdots\\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & 0 \end{vmatrix}=0.$$

定理 1 证毕。

定理 2 的证明：我们对 k 进行归纳，$k=l+1$ 时结论显然。

下设 $k-1>l$。注意 (8) 有解当且仅当线性丢番图方程组

$$\begin{cases} a_{11}x_1+\cdots+a_{1l}x_l+m_1x_{l+1}=b_1\\ a_{21}x_1+\cdots+a_{2l}x_l+m_2x_{l+2}=b_2\\ \qquad\cdots\cdots\cdots\cdots\\ a_{k1}x_1+\cdots+a_{kl}x_l+m_kx_{l+k}=b_k \end{cases} \tag{9}$$

有公解。由归纳假设知 (8) 中任何 $k-1$ 个同余式有公解，亦即 (9) 中任何 $k-1$ 个方程有公解。由定理 1，要证 (9) 有整数解，只需再说明 $1\le j_1<\cdots<j_{s-1}\le l$ 且 $1\le r_1<\cdots<r_{k-s}\le k$ 时，对

$$M=\begin{pmatrix} a_{1j_1} & \cdots & a_{1j_{s-1}} & m_{1r_1} & \cdots & m_{1r_{k-s}}\\ a_{2j_1} & \cdots & a_{2j_{s-1}} & m_{2r_1} & \cdots & m_{2r_{k-s}}\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ a_{kj_1} & \cdots & a_{kj_{s-1}} & m_{kr_1} & \cdots & m_{kr_{k-s}} \end{pmatrix}$$

(其中 m_{ij} 在 $i=j$ 时为 m_i，此外为 0)，

$$d=\left(\begin{vmatrix} & a_{11}\\ M & \vdots\\ & a_{k1} \end{vmatrix},\cdots,\begin{vmatrix} & a_{1l}\\ M & \vdots\\ & a_{kl} \end{vmatrix},\begin{vmatrix} & m_1\\ M & 0\\ & \vdots\\ & 0 \end{vmatrix},\cdots,\begin{vmatrix} & 0\\ M & \vdots\\ & 0\\ & m_k \end{vmatrix}\right)$$

整除

$$\begin{vmatrix} & b_1 \\ M & \vdots \\ & b_k \end{vmatrix}.$$

设 $\{1,\cdots,k\}\backslash\{r_1,\cdots .r_{k-s}\}$ 中元从小到大依次是 $i_1,\cdots,i_s$, 让

$$N=\begin{pmatrix} a_{i_1j_1} & a_{i_1j_2} & \cdots & a_{i_1j_{s-1}} \\ a_{i_2j_1} & a_{i_2j_2} & \cdots & a_{i_2j_{s-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_sj_1} & a_{i_s,j_2} & \cdots & a_{i_sj_{s-1}} \end{pmatrix}.$$

对任何 $c_1,\cdots,c_k\in\mathbb{Z}$,

$$\begin{vmatrix} & c_1 \\ M & \vdots \\ & c_k \end{vmatrix} \quad 与 \quad m_{r_1}\cdots m_{r_{k-s}} \begin{vmatrix} & c_{i_1} \\ N & \vdots \\ & c_{i_s} \end{vmatrix}$$

有相同的绝对值。因此 $d=\left|m_{r_1}\cdots m_{r_{k-s}}\right| d_*$, 这儿

$$d_*=\left(\begin{vmatrix} & a_{i_11} \\ N & \vdots \\ & a_{i_s1} \end{vmatrix},\cdots,\begin{vmatrix} & a_{i_1l} \\ N & \vdots \\ & a_{i_sl} \end{vmatrix},\begin{vmatrix} & m_{i_11} \\ N & \vdots \\ & m_{i_s1} \end{vmatrix},\cdots,\begin{vmatrix} & m_{i_1k} \\ N & \vdots \\ & m_{i_sk} \end{vmatrix}\right).$$

由于 $1\le j_1<\cdots<j_{s-1}\le l$, $s\le l+1<k$. 又因 (9) 中任何 $k-1$ 个方程有公解, 故

$$d_*\left|\begin{vmatrix} & b_{i_1} \\ N & \vdots \\ & b_{i_s} \end{vmatrix}\right..$$

于是 d 整除

$$\begin{vmatrix} & b_1 \\ M & \vdots \\ & b_k \end{vmatrix}=\pm m_{r_1}\cdots m_{r_{k-s}}\begin{vmatrix} & b_{i_1} \\ N & \vdots \\ & b_{i_s} \end{vmatrix}.$$

综上, 定理 2 得证。

参 考 文 献

1. Ireland K. and Rosen M., *A Classical Introduction to Modern Number Theory* (2nd edition), Springer-Verlag, New York, 1990, p. 34.
2. 孙智伟, 两个线性 *Diophantus* 方程有公解的充要条件, 南京大学学报 (自然科学版) **25** (1989), 第 1 期, 10–17.
3. 华罗庚, 数论导引, 科学出版社, 北京, 1979, 419–420.

ON SYSTEMS OF LINEAR DIOPHANTINE EQUATIONS AND LINEAR CONGRUENCES

PAN HAO AND SUN ZHIWEI

(Dept. Math., Nanjing Univ., Nanjing 210093, P.R. China)

ABSTRACT. In this paper we show that the following system

$$\begin{cases} a_{11}x_1+\cdots+a_{1l}x_l=b_1\\ a_{21}x_1+\cdots+a_{2l}x_l=b_2\\ \quad\cdots\cdots\cdots\cdots\\ a_{k1}x_1+\cdots+a_{kl}x_l=b_k\end{cases}$$

of linear equations (with integer coefficients) has integer solutions if and only if for any $1\le i_1<\cdots<i_h\le k$ and $1\le j_1<\cdots<j_{h-1}\le l$, the greatest common divisor of those determinants

$$\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & a_{i_1j}\\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & a_{i_2j}\\ \vdots & \ddots & \vdots & \vdots\\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & a_{i_hj}\end{vmatrix}\quad (j=1,\cdots,l)$$

divides

$$\begin{vmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{h-1}} & b_{i_1}\\ a_{i_2j_1} & \cdots & a_{i_2j_{h-1}} & b_{i_2}\\ \vdots & \ddots & \vdots & \vdots\\ a_{i_hj_1} & \cdots & a_{i_hj_{h-1}} & b_{i_h}\end{vmatrix}.$$

We also prove that if $k>l$ then k linear congruences in $x_1,\cdots,x_l$ have a common solution if and only if any $l+1$ of them have.

Keywords system of linear diophantine equations, system of linear congruences

AMS(2000) Subject Classification 11D04, 11D79

本文第二作者受到了教育部高校优秀青年教师教学科研奖励基金与国家自然科学基金的资助.

第一作者简介：潘颢，男， 1979 年 5 月生，现为第二作者指导的研究生.