解同余方程 $a_1x_1+a_2x_2+\cdots+a_nx_n\equiv b(\mathrm{mod}m)$

李鹤年 凌鄂生

（宜春师专） （机关总支）

摘 要

用矩阵的初等变换给出了同余方程 $\sum_{i=1}^{n}a_ix_i\equiv b(\mathrm{mod}m)$ 有解的充分与必要条件的新的证明，而且在这个证明中提供了求解的方法.

关键词：同余方程的解；求最大公约数的辗转相减法；互素；素因数；矩阵的初等变换

本文讨论解同余方程

$$a_1x_1+a_2x_2+\cdots+a_nx_n\equiv b(\mathrm{mod}m) \tag{1}$$

即求这个同余方程的解的问题.

众所周知：同余方程（1）有解的充分与必要条件是 a_1，a_2，…，a_n，m 这 $n+1$ 个整数的最大公约数（a_1，a_2，…，a_n，m）整除 b，记为$(a_1,a_2,\cdots,a_n,m)|b$；而且在（1）有解时，它有 $m^{n-1}d$ 个解，其中 $d=(a_1,a_2,\cdots,a_n,m)$. 对于这个结论的证明通常都是用数学归纳法，这样做虽然较为简单，但却没有提供求解的方法，很多数论著作就只讨论到此为止，没有进一步讨论求解的方法. 下面给出同余方程（1）有解的充分与必要条件的新的证明，在这个证明中提供了求解的方法.

引理 1 假设 a，b，c 是三个整数，$b\neq0$，a 与 b 的最大公约数 $(a,b)=d>1$，a 与 c 互素，即它们的最大公约数 $(a,c)=1$，则存在一个整数 q 使 $a+cq$ 与 b 互素，即 $(a+cq,b)=1$.

证明 因为 $(a,b)=d>1$，所以记 $a=a_1d$，$b=b_1ed$ 时，由最大公约数的性质知道 $(a_1,b_1e)=1$. 此外还可以让 $(b_1,e)=1$，$(b_1,d)=1$，而且 $e\neq1$ 时 e 的素因数都是 d 的素因数，于是又有 $(de,b_1)=1$，$(a,b_1)=1$. 又因为 $(a,c)=1$，所以 $(a,cb_1)=1$. 现在取 $q=b_1$，得 $(a+cq,b)=(a_1d+cb_1,deb_1)$，在这里用反证法很容易证明 a_1d+cb_1 与 deb_1 没有相同的素因数，即是说 $(a_1d+cb_1,deb_1)=1$. 这就证明了存在一个整数 q 使 $(a+cq,b)=1$. 证毕.

本文于1994年4月19日收到

引理 2　假设 $M=\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ 是 $n+1$ 行 n 列的整数矩阵，其中第一行的元素不全为零，从第二行起的各行元素形成一个单位矩阵. 则可以对它的列进行初等变换化为整数矩阵

$$N=\begin{pmatrix} 0 & \cdots & S & \cdots & 0 \\ q_{21} & \cdots & q_{2t} & \cdots & q_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ q_{(n+1)1} & \cdots & q_{(n+1)t} & \cdots & q_{(n+1)n} \end{pmatrix}.$$

其中第一行元素只有 $S\neq 0$，并且 $(b_1, b_2, \cdots, b_n)=|S|$，$b_1q_{2t}+b_2q_{3t}+\cdots+b_nq_{(n+1)t}=S$，$(b_n, q_{it})=1$，$2\leqslant i\leqslant n$.

证明　众所周知：根据矩阵的初等变换知道，取一个适当的整数乘矩阵 M 的某一列的元素的结果加到它的另一列的元素上去，可以使矩阵 M 的第一行的某个元素的绝对值变小，这样不断地做下去，最后可以得到一个第一行只有一个元素 S 不为零的矩阵 N'.

又根据求最大公约数的辗转相减法知道，对矩阵 M 的列进行初等变换变成矩阵 N' 以后，它们各行的 n 个元素的最大公约数是不变的，因此，$(b_1, b_2, \cdots, b_n)=(0, \cdots, S, \cdots, 0)=|S|$ 成立.

按矩阵的乘法，把一行 n 列矩阵 $(b_1, b_2, \cdots, b_n)$ 分别乘矩阵 M 的从第二行起的各列得

$$b_1\cdot 0+\cdots+b_t\cdot 1+\cdots+b_n\cdot 0=b_t,\qquad t=1,2,3,\cdots,n$$

再假设对矩阵 M 进行了若干次上述的列的初等变换而变成了整数矩阵 M' 后得

$$M'=\begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ C_{(n+1)1} & C_{(n+1)2} & \cdots & C_{(n+1)n} \end{pmatrix},$$

并且 $b_1C_{2t}+b_2C_{3t}+\cdots+b_nC_{(n+1)t}=C_{1t}$，　$t=1, 2, \cdots, n$. 然后又把整数 e 乘矩阵 M' 的第 i 列的元素的结果加到它的第 j 列上去得矩阵 M''. 于是

$$M''=\begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1j}+eC_{1i} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2j}+eC_{2i} & \cdots & C_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ C_{(n+1)1} & C_{(n+1)2} & \cdots & C_{(n+1)j}+eC_{(n+1)i} & \cdots & C_{(n+1)n} \end{pmatrix}.$$

这里 $b_1(C_{2j}+eC_{2i})+b_2(C_{3j}+eC_{3i})+\cdots+b_n(C_{(n+1)j}+eC_{(n+1)i})=(b_1C_{2j}+b_2C_{3j}+\cdots+b_nC_{(n+1)j})+(b_1C_{2i}+b_2C_{3i}+\cdots+b_nC_{(n+1)i})=C_{1j}+C_{1i}$. 由此可见这样不断地做下去，当把矩阵 M 变成了矩阵 N 时，$b_1q_{2t}+b_2q_{3t}+\cdots+b_nq_{(n+1)t}=S$ 一定成立.

最后来证明矩阵 N 的第 t 列中有一个元素 q_{it} 满足条件：$(b_n, q_{it})=1$，$i\leqslant 2\leqslant n$.

当矩阵 M 进行列的初等变换变成了整数矩阵 N' 以后得到

$$N'=\begin{pmatrix} 0 & \cdots & S & \cdots & 0 \\ a_{21} & \cdots & a_{2t} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{(n+1)1} & \cdots & a_{(n+1)t} & \cdots & a_{(n+1)n} \end{pmatrix}$$

时，第一种情况是看得出 N' 的第 t 列中有一个元素 a_{it} 满足条件：$(a_{it}, b_n)=1$，$2\leqslant i\leqslant n$，这时矩阵 N' 就是矩阵 N；第二种情况是看不出 N' 的第 t 列中有元素 a_{it} $(2\leqslant i\leqslant n)$ 与 b_n 互素，但看得出有一个元素 a_{ij} 与 a_{it} 互素，$2\leqslant i\leqslant n$，$j\neq t$，在这种情况下算出 $(a_{it}, b_n)=d$ 来. 若 $d=1$，这时矩阵 N' 还是矩阵 N. 若 $d\neq 1$，则按照引理 1 算出 $b_n=deh$ 来，其中 $(d, h)=1$，$(e, h)=1$，$e\neq 1$ 时 e 的素因数都是 d 的素因数，然后把 h 乘 N' 的第 j 列元素的结果加到它的第 t 列上去，这样得到的矩阵就是矩阵 N，因为它的第 t 列中有一个元素 $a_{it}+ha_{ij}$ 满足条件：$(a_{it}+ha_{ij}, b_n)=1$，$2\leqslant i\leqslant n$；第三种情况是看不出矩阵 N' 中有上述二种情况，这时在矩阵 N' 的第二行至第 n 行中任取一行，不妨就取第二行，然后在保持第 t 列的元素不变的要求下对 N' 的列进行初等变换，变为第二行中除 a_{2t} 外只有一个元素 $r_{2j}\neq 0$ 时为止，这样得到矩阵 N''.

$$N''=\begin{pmatrix} 0 & \cdots & 0 & \cdots & S & \cdots & 0 \\ 0 & \cdots & r_{2j} & \cdots & a_{2t} & \cdots & 0 \\ r_{31} & \cdots & r_{3j} & \cdots & a_{3t} & \cdots & r_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ r_{(n+1)1} & \cdots & r_{(n+1)j} & \cdots & a_{(n+1)t} & \cdots & r_{(n+1)n} \end{pmatrix}$$

或

$$\begin{pmatrix} 0 & \cdots & S & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & a_{2t} & \cdots & r_{2j} & \cdots & 0 \\ r_{31} & \cdots & a_{3t} & \cdots & r_{3j} & \cdots & r_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ r_{(n+1)1} & \cdots & a_{(n+1)t} & \cdots & r_{(n+1)j} & \cdots & r_{(n+1)n} \end{pmatrix}$$

由前面的证明知道矩阵 M 的第二行元素的最大公约数与矩阵 N'' 的第二行元素的最大公约数相同，因此 $1=(1, 0, \cdots, 0)=(0, \cdots, r_{2j}, \cdots a_{2t}, \cdots, 0)=(r_{2j}, a_{2t})$. 再由矩阵 N' 的第二种情况知道矩阵 N'' 或者是矩阵 N，或者可以变为矩阵 N，两者必居其一. 证毕.

在引理 2 的证明中提供了一个对已知的 n 个整数 $a_1, a_2, \cdots, a_n$ 求使 $a_1q_1+a_2q_2+\cdots+a_nq_n=(a_1, a_2, \cdots, a_n)$ 成立的整数 $q_1, q_2, \cdots, q_n$ 的方法. 这个方法比现在数论著作中常见的方法好，在 $n>2$ 时更显得出它的优越性，值得提倡.

例 1 求使 $1008q_1+1260q_2+882q_3+2268q_4=d$ 成立的整数 q_1, q_2, q_3, q_4, d，其中 $d=(1008, 1260, 882, 2268)$.

解：

作矩阵 $M=\begin{pmatrix} 1008 & 1260 & 882 & 2268 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. 在矩阵 M 中第 1 列减第 3 列，第 2 列减第

3 列，第 4 列减第 3 列乘 3 得矩阵 M_1

$$M_1=\begin{pmatrix}126 & 378 & 882 & -378\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ -1 & -1 & 1 & -3\\ 0 & 0 & 0 & 1\end{pmatrix}.$$

在矩阵 M_1 中第 4 列减第 2 列乘 -1，第 2 列减第 1 列乘 3，第 3 列减第 1 列乘 7 得矩阵 M_2

$$M_2=\begin{pmatrix}126 & 0 & 0 & 0\\ 1 & -3 & -7 & 0\\ 0 & 1 & 0 & 1\\ -1 & 2 & 8 & -4\\ 0 & 0 & 0 & 1\end{pmatrix}.$$

从矩阵 M_2 中得 $d=(1008, 1260, 882, 2268)=126$；$q_1=1$，$q_2=0$，$q_3=-1$，$q_4=0$ 时使得

$1008\times1+1260\times0-882\times1+2268\times0=126$ 成立.

定理　同余方程 (1) 有解的充分与必要条件是 $d\mid b$，其中 $d=(a_1, a_2, \cdots, a_n, m)$，并且 (1) 有解时关于模 m 共有 $m^{n-1}d$ 个解.

证明　条件的必要性显然成立，因此只证明条件的充分性成立.

若同余方程 (1) 中有 $(a_i, m)=1$，$1\leqslant i\leqslant n$，这时 $(a_1, a_2, \cdots, a_n, m)=1$. 为方便起见不妨认为 $(a_1, m)=1$，在这种情况下把 (1) 改写为

$$a_1x_1\equiv b-a_2x_2-a_3x_3-\cdots-a_nx\pmod m. \tag{2}$$

其中 $(a_1, m)=1$. 由同余方程 $ax\equiv b\pmod m$ 有解的充分与必要条件知道，在 (2) 中 x_2，x_3，$\cdots$，x_n 取定为任意整数时 x_1 关于模 m 都有唯一解，这就证明了 (2) 有解，即是说 (1) 有解. 由于 x_2，x_3，$\cdots$，x_n 可取任意整数代入 (2) 去求 x_1 时都有解，这对于模 m 来说 x_i 总共只有 $x_i\equiv0$，1，2，$\cdots$，$m-1\pmod m$ 这 m 个互不相同的值，其中 $i=2$，3，$\cdots$，n. 这 $m(n-1)$ 个整数总共可分为 x_2，x_3，$\cdots$，x_n 的 m^{n-1} 个不同的组合，每一组 x_2，x_3，$\cdots$，x_n 代入 (2) 都使 x_1 有唯一解，从而得到 (2) 的一个解，因此，(2) 关于模 m 总共有 m^{n-1} 个解. 这就证明了在这种情况下 (1) 有解时共有 m^{n-1} 个解.

若 (1) 中 $(a_1, a_2, \cdots, a_n, m)=d>1$，并且 $d\mid b$. 由引理 2 可求得整数 q_1，q_2，$\cdots$，q_n，q_{n+1} 使 $a_1q_1+a_2q_2+\cdots+a_nq_n+mq_{n+1}=d$，并且不妨认为其中 $(q_1, m)=1$，再约去 d 得

$$a'q_1\equiv1-a_2'q_2-a_3'q_3-\cdots-a_n'q_n\pmod{m'}. \tag{3}$$

其中 $m=m'd$，$a_i=a_i'd$，$i=1,2,\cdots,n$，又把 (1) 改写为

$$a_1'x_1+a_2'x_2+\cdots+a_n'x_n\equiv b'\pmod{m'} \tag{4}$$

由 (3) 知 (4) 中 $(a_1', a_2', \cdots, a_n', m')=1$，因为 $(q_1', m')=1$，所以 (4) 等价于 $a_1'q_1x_1+a_2'q_1x_2+\cdots+a_n'q_1x_n\equiv b'q_1\pmod{m'}$. (5)

代 (3) 入 (5) 得

$$y_1\equiv b'q_1-a_2'y_2-a_3'y_3-\cdots-a_n'y_n\pmod{m'} \tag{6}$$

其中 $y_1\equiv x_1\pmod{m'}$，$y_i\equiv q_1x_i-q_ix_1\pmod{m'}$，$i=2,3,\cdots,n$. (7)

显然，由 (4) 的一个解可算得 (6) 的一个解；反之，把 (6) 的一个解代入 (7) 中，因 $(q_1, m')=1$ 的缘故也算得 (4) 的一个解，而且只有一个解，又由前面的证明知道 (6) 总

共有 m'^{n-1} 个解，因此（4）也有 m'^{n-1} 个解. 不难看出（4）只有这 m'^{n-1} 个解. 任取（4）的一个解 $x_1\equiv x_{01}(\mathrm{mod}m')$，$x_2\equiv x_{02}(\mathrm{mod}m')$，…，$x_n\equiv x_{0n}(\mathrm{mod}m')$，把这个解换成以 m 为模恰好分为

$$\begin{aligned}
&x_1 \equiv x_{01}, x_{01}+m', x_{01}+2m', \cdots, x_{01}+(d-1)m' (\mathrm{mod}m),\\
&x_2 \equiv x_{02}, x_{02}+m', x_{02}+2m', \cdots, x_{02}+(d-1)m' (\mathrm{mod}m),\\
&\qquad\cdots\quad\cdots\quad\cdots\\
&x_n \equiv x_{0n}, x_{0n}+m', x_{0n}+2m', \cdots, x_{0n}+(d-1)m' (\mathrm{mod}m)
\end{aligned} \tag{8}$$

其中 $m=dm'$. （8）中的 dn 个同余式总共可组合成 x_1，x_2，…，x_n 的不同的组合为 d^n 组，每一组 x_1，x_2，…，x_n 都使同余方程（4）成立，显然也使同余方程（1）成立. 这就证明了（1）有解，而且有 $m'^{n-1}\cdot d^n=m^{n-1}\cdot d$ 个解. 反之不难看出以 m' 为模时，同余方程（1）的以 m 为模的 d^n 个解是（4）的一个解. 这就证明了同余方程（1）这时有解，而且共有 $m^{n-1}\cdot d$ 个解. 证毕.

在上述定理的证明中提供了求同余方程（1）的解的方法.

例 2 叙述同余方程 $136x_1+221x_2+391x_3\equiv 119\ (\mathrm{mod}476)$ 的解法.

解：

作矩阵 $M=\begin{pmatrix}136 & 221 & 391 & 476\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$. 在矩阵 M 中，第 4 列减第 2 列乘 2，第 2 列减第 1 列乘 2，第 3 列减第 1 列乘 3 得矩阵 M_1.

$M_1=\begin{pmatrix}136 & -51 & -17 & 34\\ 1 & -2 & -3 & 0\\ 0 & 1 & 0 & -2\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$. 在矩阵 M_1 中，第 4 列减第 3 列乘 -2，第 2 列减第 3 列乘 -3，第 1 列减第 3 列乘 -8 得矩阵 M_2.

$M_2=\begin{pmatrix}0 & 0 & -17 & 0\\ -23 & -11 & -3 & -6\\ 0 & 1 & 0 & -2\\ 8 & 3 & 1 & 2\\ 0 & 0 & 0 & 1\end{pmatrix}$. 从矩阵 M_2 中得 $(136, 221, 391, 476)=17$，并且 $17\mid 119$. 因此，这个同余方程有解，而且有 $476^2\cdot 17$ 个解. 从矩阵 M_2 中又得到 $136\times 3+221\times 0+391\times(-1)+476\times 0=17$，而且 391 的乘数 -1 与这个同余方程的模 476 互素. 约去 17 后把上式改写为

$$23\equiv -1+8\times 3+13\times 0(\mathrm{mod}28). \tag{9}$$

另一方面把这个同余方程也约去 17 得

$$8x_1+13x_2+23x_3\equiv 7(\mathrm{mod}28). \tag{10}$$

再把（9）代入（10）得　$8y_1+13y_2-y_3\equiv 7(\mathrm{mod}28)$. 此即

$$y_3\equiv -7+8y_1+13y_2(\mathrm{mod}28). \tag{11}$$

其中　$y_1\equiv x_1+3x_3(\mathrm{mod}28), y_2\equiv x_2(\mathrm{mod}28), y_3\equiv x_3(\mathrm{mod}28)$. (12)

在同余方程（11）中，y_1，y_2 可取任意整数，因此，得到 $y_1\equiv 0$，1，2，…，27 (mod28)，$y_2\equiv 0$，1，2，…，27 (mod28). 把 y_1 和 y_2 的这些值分成 28^2 个不同的组合分别代入（11）中就求得（11）的全部 28^2 个解. 把（11）的解分别代入（12）中就求得同余方程（10）的全部 28^2 个解. 把（10）的每一个解换成以 476 为模，就可以分组成所求的这个同余方程的 17^3 个解，因此，（10）的全部 28^2 个解都换成以 476 为模就求得出所求的全部 $28^2\times 17^3=476^2\times 17$ 个解.

在同余方程（1）中，当 $n=1$ 时像例 2 叙述的那样来求它的解不但可以，而且同现在流行的各种解法比较起来，就一般性而言还是一个好方法.

例 3　解同余方程 $1277x\equiv 15(\mathrm{mod}3323)$.

解：

作矩阵　$M=\begin{pmatrix}1277 & 3323\\ 1 & 0\\ 0 & 1\end{pmatrix}$. 在矩阵 M 中，第 2 列减第 1 列乘 3 得矩阵 M_1.

$M_1=\begin{pmatrix}1277 & -508\\ 1 & -3\\ 0 & 1\end{pmatrix}$. 在矩阵 M_1 中，第 1 列减第 2 列乘 -3 得矩阵 M_2，

$M_2=\begin{pmatrix}-247 & -508\\ -8 & -3\\ 3 & 1\end{pmatrix}$. 在矩阵 M_2 中，第 2 列减第 1 列乘 2 得矩阵 M_3.

$M_3=\begin{pmatrix}-247 & -14\\ -8 & 13\\ 3 & -5\end{pmatrix}$. 在矩阵 M_3 中，第 1 列减第 2 列乘 18 得矩阵 M_4.

$M_4=\begin{pmatrix}5 & -14\\ -242 & 13\\ 93 & -5\end{pmatrix}$. 在矩阵 M_4 中，第 2 列减第 1 列乘 -3 得矩阵 M_5，

$M_5=\begin{pmatrix}5 & 1\\ -242 & -713\\ 93 & 274\end{pmatrix}$. 由矩阵 M_5 中得到$(1277,3323)=1$，因此，这个同余方程有解，而且只有一个解. 由矩阵 M_5 又得到　$1277\times(-713)+3323\times 274=1$. 于是同余式 $1277\times(-713)\equiv 1(\mathrm{mod}3323)$ 成立. 再从这里得到 $1277\times(-713)\times 15\equiv 15(\mathrm{mod}3323)$成立. 因此 $x\equiv -713\times 15(\mathrm{mod}3323)$，即 $x\equiv -726(\mathrm{mod}3323)$为所求的这个同余方程的唯一解.

参考文献

[1] 华罗庚. 数论导引. 北京：科学出版社，1964，30～32
[2] 张德馨. 整数论. 北京：科学出版社，1965，第1卷 1～30
[3] 彭智. 模变换下的不变量. 宜春师专学报，1984，(1)

Solation of Congruent Equation $a_1x_1+a_2x_2+\cdots+a_nx_n\equiv b(\mathrm{mod}m)$

Li Henian Ling Esheng

ABSTRACT

In this paper, we give a new proof for necessary and sufficient conditions of solution existence of congruent equation $a_1x_1+a_2x_2+\cdots+a_nx_n\equiv b(\mathrm{mod}m)$ by elementary transformation of matrix, and a solving method is given in this proof.

Key words: Solution of congruent equation; Successive sabtraction of the maximal common divisor; Prime; Prime factor; Elementary transformation of matrix