一般の連立1 次合同式に関する1 つの注意

宮崎大学教育文化学部紀要　創立 130 周年記念特別号

一般の連立 1 次合同式に関する 1 つの注意

谷本　洋

A Remark on General Linear Congruences

Hiroshi TANIMOTO

1．はじめに

[1]に，次の定理が述べられている。

定理 A ([1]) 互いに素な自然数 $m_1, m_2, \dots, m_k$ と任意の整数 $a_1, a_2, \dots, a_k$ について，$M = m_1 m_2 \dots m_k$ とおけば，次の連立 1 次合同式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

は $mod\ M$ で唯 1 つの解を持つ。

[1]ではこのあと，互いに素では必ずしもない一般の自然数 $m_1, m_2, \dots, m_k$ について，この連立 1 次合同式が解を持つための $a_1, a_2, \dots, a_k$ の満たすべき必要十分条件が与えられている。この論文の目的は，[1]で示されている帰納的な方法とは別の方法でこの性質が正しいことを示すことである。この方法は，[1]で扱われている互いに素の場合の直接的なガウスの方法を用いるものである。合同式を使って示すこともできるが，ここでは剰余類群を使って示す。

2．準備

自然数 n と，$0 \leqq i < n$ を満たす整数 i に対し集合

$S = \{ a \in \mathbb{Z} \mid a \text{ を } n \text{ で割った余りは } i \text{ となる。} \}$ を定め，S の任意の元 b について $S = \overline{b}$ と表す。すると，$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{n-1}$ となる。このとき，$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ とおくと，これは加法について群になる。これを，$\mathbb{Z}$ の n による剰余類群という。剰余類群の言葉を使えば，定理 A は次のように言い換えることができる。

定理 B　互いに素な自然数 $m_1, m_2, \dots, m_k$ と任意の整数 $a_1, a_2, \dots, a_k$ について，$M = m_1 m_2 \dots m_k$ とおけば，次の連立 1 次方程式

$$\begin{cases} \mathbb{Z}_{m_1} \text{ において} & \overline{x} = \overline{a_1} \\ \mathbb{Z}_{m_2} \text{ において} & \overline{x} = \overline{a_2} \\ \quad\vdots & \\ \mathbb{Z}_{m_k} \text{ において} & \overline{x} = \overline{a_k} \end{cases}$$

は $\mathbb{Z}_M$ において唯 1 つの解を持つ。

さらに，上で述べている[1]の「必要十分条件」は剰余類群の言葉を使えば次のように言い表すことができる。

定理 C　自然数 $m_1, m_2, \dots, m_k$ と整数 $a_1, a_2, \dots, a_k$ について，任意の i, j に対し $M_{i,j} = GCD(m_i, m_j)$ とおけば，次の連立 1 次方程式

$$\begin{cases} \mathbb{Z}_{m_1} \text{ において} & \overline{x} = \overline{a_1} \\ \mathbb{Z}_{m_2} \text{ において} & \overline{x} = \overline{a_2} \\ \quad\vdots & \\ \mathbb{Z}_{m_k} \text{ において} & \overline{x} = \overline{a_k} \end{cases}$$

が解を持つための必要十分条件は，任意の i, j に対し $\mathbb{Z}_{M_{i,j}}$ において $\overline{a_i} = \overline{a_j}$ が成り立つことである。しかもこのとき，$L = LCM(m_1, m_2, \dots, m_k)$ とおけば，これは $mod\ L$ で唯 1 つの解を持つ。

次は自明な性質であるが，ここで役に立つ。

補題　自然数 m, n に対し，

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_n,\ f(\overline{x}) = \overline{x}$$

が写像になるための必要十分条件は $n|m$ が成り立つことである。

3．定理 C の証明と例

定理 C の証明　示すべきことは，与えられた条件の十分性である。

まず，$m_1, m_2, \dots, m_k$ を素因数分解する。

$$\begin{cases} m_1 = p_1^{e_{11}} p_2^{e_{12}} \cdots p_t^{e_{1t}} \\ m_2 = p_1^{e_{21}} p_2^{e_{22}} \cdots p_t^{e_{2t}} \\ \quad\vdots \\ m_k = p_1^{e_{k1}} p_2^{e_{k2}} \cdots p_t^{e_{kt}} \end{cases}, \quad p_1, p_2, \cdots, p_t \text{ は相異なる素数，任意の } e_{ij} \text{ は非負整数}$$

任意の j に対し，

$$e_{uj} = max\{e_{1j}, e_{2j}, \cdots, e_{kj}\} \quad \cdots\cdots (*)$$

となる u を 1 つ定め，$1 \leqq i \leqq k$ を満たす任意の i に対し $h_{ij} = \begin{cases} e_{uj} & (i = u \text{ のとき}) \\ 1 & (i \neq u \text{ のとき}) \end{cases}$ とおき，任意の i に対し $n_i = p_1^{h_{i1}} p_2^{h_{i2}} \cdots p_t^{h_{it}}$ とおく。

$n_1, n_2, \dots, n_k$ は互いに素ゆえに，定理 A より，次の連立 1 次方程式は解 $x = x_0$ を持つ。

$$\begin{cases} \mathbb{Z}_{n_1} \text{ において } \overline{x} = \overline{a_1} \\ \mathbb{Z}_{n_2} \text{ において } \overline{x} = \overline{a_2} \\ \quad\vdots \\ \mathbb{Z}_{n_k} \text{ において } \overline{x} = \overline{a_k} \end{cases}$$

この x_0 が，任意の i に対し $\mathbb{Z}_{m_i}$ において $\overline{x} = \overline{a_i}$ を満たすこと，すなわち，定理 B より，任意の j に対し $\mathbb{Z}_{p_j^{e_{ij}}}$ において $\overline{x_0} = \overline{a_i}$ を満たすことを示せばよい。

まず，$(*)$ より $e_{uj} = max\{e_{1j}, e_{2j}, \cdots, e_{kj}\}$ とすれば，$\mathbb{Z}_{n_u}$ において $\overline{x} = \overline{a_u}$ を満たす。$e_{ij} \leqq e_{uj}$，$p_j^{e_{uj}} \Big| n_u$ ゆえに $p_j^{e_{ij}} \Big| n_u$ より，補題から，$\mathbb{Z}_{p_j^{e_{ij}}}$ において $\overline{x_0} = \overline{a_u}$ となる。一方，$p_j^{e_{ij}} \Big| M_{i,u}$ より，補題から，$\mathbb{Z}_{p_j^{e_{ij}}}$ において $\overline{a_i} = \overline{a_u}$ となる。以上より，$\mathbb{Z}_{p_j^{e_{ij}}}$ において $\overline{x_0} = \overline{a_i}$ を満たすことを示すことができた。

（証明終）

注意　上の証明の中で，$p_1, p_2, \cdots, p_t$ は相異なる素数としたが，証明を見れば，これは「互いに素な自然数」で十分である。

例　$\mathbb{Z}_{3^3 4} \times \mathbb{Z}_{4^2 5} \times \mathbb{Z}_{5^2 3} \ni (\overline{31}, \overline{19}, \overline{34})$ について，$(\overline{31}, \overline{19}, \overline{34}) = (\overline{x}, \overline{x}, \overline{x})$ となる整数 x は定理 C より存在する。このとき，$\mathbb{Z}_{3^3} \times \mathbb{Z}_{4^2} \times \mathbb{Z}_{5^2}$ において，$(\overline{31}, \overline{19}, \overline{34}) = (\overline{x}, \overline{x}, \overline{x})$ となる整数 x を見つければよい。

- $\mathbb{Z}_{3^3}$ において $4^2 5^2 \overline{t} = \overline{1}$ を満たす $\overline{t}$ は $\overline{-2}$ である。
- $\mathbb{Z}_{4^3}$ において $3^2 5^2 \overline{t} = \overline{1}$ を満たす $\overline{t}$ は $\overline{1}$ である。
- $\mathbb{Z}_{5^3}$ において $3^2 4^2 \overline{t} = \overline{1}$ を満たす $\overline{t}$ は $\overline{4}$ である。

よって，求める解は $\mathbb{Z}_{3^3 4^2 5^2}$ において，$\overline{x} = \overline{4^2 5^2 \cdot (-2) \cdot 31 + 3^2 5^2 \cdot 1 \cdot 19 + 3^2 4^2 \cdot 4 \cdot 34} = \overline{2659}$ である。

参考文献

［1］「初等整数論講義」高木貞治，共立出版，1991