

第6章 合同式を解く

6.1 1次合同式

整数 a が m を法として可逆であることは,

$$ax \equiv 1 \pmod{m}$$

をみたす整数 x が存在することであった。また, a が零因子であることは,

$$ax \equiv 0, \quad x \not\equiv 0 \pmod{m}$$

をみたす整数 x が存在することであった。これらの性質は, 与えられた合同式を未知数 x をもつ方程式のように扱い, その整数解の存在によって特徴づけられていると考えることができる。この章では, 方程式としての合同式を扱い, その整数解について述べる。

まず最初に, すでに学んだ1次不定方程式の理論を書き換えることにより, 次を得る。

定理 6.1 整数 a_1, \dots, a_n, b, m に対して合同式

$$a_1x_1 + \dots + a_nx_n \equiv b \pmod{m}$$

が整数解 x_1, \dots, x_n をもつための必要十分条件は, b が $\gcd(a_1, \dots, a_n, m)$ の倍数であることである。

証明 与えられた合同式が整数解 x_1, \dots, x_n をもつことと, 1次不定方程式

$$a_1x_1 + \dots + a_nx_n = b + my, \quad \text{すなわち} \quad a_1x_1 + \dots + a_nx_n - my = b$$

が整数解 x_1, \dots, x_n, y をもつことは同値, よって, 定理 3.4 より定理の主張を得る。□

この定理を用いれば, とくに, a が m を法として可逆であることと $\gcd(a, m) = 1$ の同値性 (定理 5.9 の一部) が得られる。なぜなら, 上記定理を $n = 1, b = 1$ として適用すれば, 「合同式 $ax \equiv 1 \pmod{m}$ が整数解もつ」 \Leftrightarrow 「1 が $\gcd(a, m)$ を約数としてもつ」 \Leftrightarrow 「 $\gcd(a, m) = 1$ 」がいえるからである。さらに, 次の系が成り立つこともすぐにわかる。

系 6.2 整数 a, m が互いに素ならば, 任意の整数 b に対して, 合同式

$$ax \equiv b \pmod{m}$$

は整数解をもつ。さらに, 解は m を法として一意的に定まる。すなわち, $x, x' \in \mathbf{Z}$ がともに解ならば $x \equiv x' \pmod{m}$ が成り立つ。

系 6.2 は、以下に述べるように、連立合同式に拡張することができる。いま、整数 a_{ij} および b_i ($i, j = 1, \dots, n$) に対して、 x_1, \dots, x_n を未知数とする法 m に関する連立合同式

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod{m} \\ \vdots \quad \quad \quad \ddots \quad \quad \quad \vdots \quad \quad \quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n \pmod{m} \end{cases}$$

を考える。これを、線形代数で学んだときのように、 n 次正方形行列 $A = (a_{ij})$ と n 次元列ベクトル $\mathbf{b} = (b_i)$ 、および未知数からなる列ベクトル $\mathbf{x} = (x_i)$ を用いて

$$A\mathbf{x} \equiv \mathbf{b} \pmod{m}$$

と表すと便利である。次の定理が系 6.2 の一般化になっている。

定理 6.3 A を整数を成分とする n 次正方形行列、 m を整数とする。 $\det A$ と m が互いに素ならば、任意の整数成分 n 次元列ベクトル \mathbf{b} に対して、 m を法とする連立合同式

$$A\mathbf{x} \equiv \mathbf{b} \pmod{m}$$

は整数を成分とするベクトル解をもつ。さらに、解は m を法として一意的に定まる。

証明 A の余因子行列 \tilde{A} は整数を成分とする n 次正方形行列であり、

$$\tilde{A}A = A\tilde{A} = (\det A)E$$

が成り立つことに注意する。ここで E は n 次単位行列を表す。仮定より、 $\det A$ の法 m に関する逆元 c がとれて、 $c \det A \equiv 1 \pmod{m}$ をみたすから、

$$A(c\tilde{A}\mathbf{b}) = c(A\tilde{A})\mathbf{b} = (c \det A)\mathbf{b} \equiv \mathbf{b} \pmod{m}.$$

よって $\mathbf{x} = c\tilde{A}\mathbf{b}$ は解である。 □

例 6.4 連立合同式 $\begin{cases} 2x - 7y \equiv 3 \pmod{17} \\ -5x + 3y \equiv -8 \pmod{17} \end{cases}$ を解け。

解 まず、係数行列式

$$\begin{vmatrix} 2 & -7 \\ -5 & 3 \end{vmatrix} = -29$$

が法 17 と互いに素だから、定理 6.3 より、整数解 x, y をもつことが保証される。実際に解を求めるために、ここではクラメルの公式を用いる。クラメルの公式から

$$-29x = \begin{vmatrix} 3 & -7 \\ -8 & 3 \end{vmatrix} = -47, \quad -29y = \begin{vmatrix} 2 & 3 \\ -5 & -8 \end{vmatrix} = -1.$$

これらの等式を、法 17 についての合同式に置き換えて、 $5x \equiv 4$ 、 $5y \equiv -1 \pmod{17}$ となるが、法 17 に関する 5 の逆元として 7 がとれるから、 $x \equiv 4 \cdot 7 = 28$ 、 $y \equiv -7 \pmod{17}$ 、したがって、解 $x \equiv 11$ 、 $y \equiv 10 \pmod{17}$ を得る。

6.2 中国の剰余定理

前節では、共通の法をもついくつかの合同式からなる連立合同式を扱った。この節では異なる法をもつ連立合同式を考える。

定理 6.5 (中国の剰余定理) m_1, m_2, \dots, m_r をどの2つも互いに素な自然数とすると、任意の整数 a_1, a_2, \dots, a_r に対して、連立合同式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

は整数解 x をもつ。さらに、 $M = m_1 \cdots m_r$ とすると、解は M を法として一意である。

最後の部分、すなわち一意性は次のようにして確かめられる。 $x, x' \in \mathbf{Z}$ がどちらも上の合同式をみたすならば、 $x - x'$ は m_1, m_2, \dots, m_r すべての倍数である。一方、仮定より m_1, m_2, \dots, m_r はどの2つも互いに素だから、これらの最小公倍数は $M = m_1 \cdots m_r$ であり、 $x - x'$ はその倍数、したがって $x \equiv x' \pmod{M}$ が確かめられた。

以下において、解が存在することの証明を2つ与える。

第1証明 $r = 1$ のときは明らかなので $r \geq 2$ としよう。まず、第1の合同式から解は $a_1 + m_1 y$ の形をしている。これが第2の式をみたしているので

$$a_1 + m_1 y \equiv a_2 \pmod{m_2} \quad \text{すなわち} \quad m_1 y \equiv a_2 - a_1 \pmod{m_2}.$$

ここで、 m_1, m_2 は互いに素なので、定理 5.9 より、法 m_2 に関する m_1 の逆元 b がとれ、それをを用いて $y \equiv b(a_2 - a_1) \pmod{m_2}$ と書ける。 m_1 を掛けて

$$m_1 y \equiv m_1 b(a_2 - a_1) \pmod{m_1 m_2},$$

したがって、第1、第2の合同式はひとつの合同式

$$x \equiv a_1 + m_1 b(a_2 - a_1) \pmod{m_1 m_2}$$

に置き換えることができ、 $r = 2$ ならば右辺が解を与えることになる。 $r \geq 3$ のときも、この操作を繰り返すことで最終的にひとつの合同式に帰着され、それが解を与える（正確には数学的帰納法による）。□

第2証明 まず、 $n_1, \dots, n_r \in \mathbf{Z}$ を次式で定める;

$$m_i n_i = m_1 \cdots m_r \quad (i = 1, \dots, r).$$

すなわち n_i は m_1, \dots, m_r から m_i を除いたものの積であり、仮定より m_i, n_i は互いに素である。このとき、 n_1, \dots, n_r の最大公約数は1である。実際、そうでないとすると、

$n_1 \equiv \cdots \equiv n_r \equiv 0 \pmod{p}$ をみたす素数 p が存在する. とくに $m_2 \cdots m_r = n_1 \equiv 0 \pmod{p}$ より, $m_j \equiv 0 \pmod{p}$ をみたす $2 \leq j \leq r$ がとれるが, これは m_j, n_j が互いに素であることに矛盾する. よって $\gcd(n_1, \dots, n_r) = 1$ が示され, 定理 3.4 より

$$n_1 t_1 + \cdots + n_r t_r = 1$$

をみたす $t_1, \dots, t_r \in \mathbf{Z}$ が存在する. このとき, n_i の定義から, $1 \leq i, j \leq r$ に対して

$$n_i t_i \equiv \begin{cases} 1 & (i = j) \\ 0 & (i \neq j) \end{cases} \pmod{m_j}$$

であることがわかり, したがって $x = a_1 n_1 t_1 + \cdots + a_r n_r t_r$ が解を与える. \square

上記 2 つの証明は, 実際に解を求める計算法も与えている. 数学的帰納法による第 1 証明は, 合同式を 2 つずつ順々に解いていく方法, 第 2 証明はすべての合同式を同時に扱い, 解を一気に構成する方法である.

以下ではひとつの例題に対し, 第 1 および第 2 証明にそった解法をそれぞれ例示する.

例 6.6 次の連立合同式を解け.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

解 1 まず第 1 の合同式から, 解は $2 + 3k$ の形をしている. これが第 2 の式をみたすから $2 + 3k \equiv 3 \pmod{5}$, これを解いて $k \equiv 2 \pmod{5}$ したがって $3k \equiv 6 \pmod{15}$ となるから, 第 1, 第 2 の合同式はひとつの合同式 $x = 2 + 3k \equiv 8 \pmod{15}$ に帰着する. 続けて, この式から解は $8 + 15l$ の形をしていて, それを第 3 の合同式に当てはめると, l は $8 + 15l \equiv 2 \pmod{7}$ をみたさなければならない. これを解いて $l \equiv 1 \pmod{7}$, したがって $15l \equiv 15 \pmod{105}$. これから, 解 $x = 8 + 15l \equiv 23 \pmod{105}$ を得る.

解 2 まず, $35t_1 + 21t_2 + 15t_3 = 1$ の形の式を見つけない. そのために $5 \cdot (-1) + 3 \cdot 2 = 1$ と $7 \cdot (-2) + 15 = 1$ に注目して,

$$1 = 7 \cdot (-2) + 15 = 7 \cdot (-2) \cdot (5 \cdot (-1) + 3 \cdot 2) + 15 = 35 \cdot 2 + 21 \cdot (-4) + 15 \cdot 1,$$

すなわち $(t_1, t_2, t_3) = (2, -4, 1)$ が求まる. これを用いて, 解

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot (-4) + 2 \cdot 15 \cdot 1 = -82$$

を得る. $-82 \equiv 23 \pmod{105}$ より, 解 1 と同じ解が得られたことに注意せよ (当たり前だ).

この例は 3~5 世紀頃書かれた中国の算術書【孫子算經】に載っていて, 上にあげた解 2 と同じ趣旨の解法も与えられている. 解 2 は各合同式を同等に扱い (つまり対称性があり) 理論的にも優れていると思われるが, 途中の計算の意味がとらえにくいのが欠点である. 私自身は, 解 1 の方が計算しやすいと思うが, みんなはどう思う?