初等整数論 (5 回目)

5. 合同式の基礎 (2)

今回は 1 次合同式と連立合同式について紹介する.

定理 5-1.
自然数 m と整数 a, b $(\gcd(a, m) = d)$ に対して 1 次合同式

$$ax \equiv b \pmod{m} \qquad (\star)$$

を考える.

(1) $(\star)$ を満たす整数 x がある $\iff d \mid b$.

(2) $d \mid b$ とする. $m_1 = \frac{m}{d}$ とし, 整数 x_0 を $(\star)$ の解の一つとする. このとき, 整数 x に対し,

$$x \text{ が } (\star) \text{ の解} \iff x \equiv x_0 \pmod{m_1}.$$

つまり, $(\star)$ の解は法 m_1 で一意的に存在する.

[証明]
(1) $\Rightarrow$ について. $b \equiv ax \pmod{m}$ より $b = ax + mk$ $(k \in \mathbb{Z})$ と表せる. $d \mid a,\ d \mid m$ より $d \mid b$.
$\Leftarrow$ について. $d \mid b$ とすると,

$$b \in d\mathbb{Z} = a\mathbb{Z} + m\mathbb{Z}$$

(定理 2-4 を参照). よって $b = ax + my$ $(x, y \in \mathbb{Z})$ と表せる. 従って $b \equiv ax \pmod{m}$.

(2) $\Rightarrow$ について. $ax \equiv b \pmod{m}$ のとき,

$$ax \equiv b \equiv ax_0 \pmod{m}.$$

$\gcd(a, m) = d$ より $x \equiv x_0 \pmod{m_1}$.
$\Leftarrow$ について. $x \equiv x_0 \pmod{m_1}$ とする. $x - x_0 = m_1 k$ $(k \in \mathbb{Z})$ と表せるので

$$ax - ax_0 = am_1 k = m \times \frac{ak}{d} \in m\mathbb{Z}.$$

よって $ax \equiv ax_0 \equiv b \pmod{m}$ を得る.

□

[補足] 自然数 m と整数 a, b $(\gcd(a, m) = d,\ d \mid b)$ に対して, 合同式

$$ax \equiv b \pmod{m} \quad (\diamond)$$

の解は次の手順で求まる. まず,

$$a_1 = \frac{a}{d}, \quad b_1 = \frac{b}{d}, \quad m_1 = \frac{m}{d}$$

と置くと, $a_1 x \equiv b_1 \pmod{m_1}$. ここで, $\gcd(a_1, m_1) = 1$ より, ユークリッド互除法を用いると, $a_1 t + m_1 s = 1$ を満たす整数 s, t が取れる. $a_1 t \equiv 1 \pmod{m_1}$ より合同式 $(\diamond)$ の解は

$$x \equiv a_1 t x \equiv t b_1 \pmod{m_1}$$

で与えられる.

例題 5-1
次を満たす整数 $0 \leq x < 30$ をすべて求めよ.

$$15x \equiv 6 \pmod{33} \qquad (\square)$$

[**解答**]
$3 = \gcd(15, 33) \mid 6$ より合同式 $(\square)$ は法 11 で一意的に解を持つ. 合同式 $(\square)$ の両辺を 3 で割ると,

$$5x \equiv 2 \pmod{11}.$$

$11 + 5 \cdot (-2) = 1$ より $5 \cdot (-2) \equiv 1 \pmod{11}$. よって合同式 $(\square)$ の解は

$$x \equiv -4 \equiv 7 \pmod{11}.$$

$0 < x < 30$ より $x = 7, 18, 29$.

□

問題 5-1 次を満たす整数 $0 \leq x < 50$ をすべて求めよ.

$$11x \equiv 3 \pmod{23}.$$

次に連立合同式を解説する.

定理 5-2 (中国剰余の定理)
自然数 m, n $(\gcd(m, n) = 1)$ と整数 a, b に対して, 次の連立合同式の解は法 mn で一意的に存在する.

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n}. \end{cases}$$

[**証明**]
(存在) $\gcd(m,n)=1$ より $ms-nt=b-a$ となる整数 s,t がある. ここで,

$$x=a+ms=b+nt$$

とおくと,

$$x\equiv a \pmod m, \quad x\equiv b \pmod n.$$

(一意性) 整数 x,y が次を満たすとする.

$$\begin{cases} x\equiv a \pmod m \\ x\equiv b \pmod n \end{cases} \qquad \begin{cases} y\equiv a \pmod m \\ y\equiv b \pmod n. \end{cases}$$

このとき,

$$x\equiv y \pmod m, \quad x\equiv y \pmod n.$$

$m\mid x-y,\ \ n\mid x-y,\ \ \gcd(m,n)=1$ より $mn\mid x-y$. 従って $x\equiv y \pmod{mn}$.

□

例題 5-2
次の連立合同式の解を求めよ.

$$\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 4 \pmod 7 \end{cases} \qquad (\clubsuit)$$

(求め方) 連立合同式の解の構成は定理 5-2 の証明を追えばよい.

[**解答**]
$(-2)\cdot 3-(-1)\cdot 7=1$ より

$$(-4)\cdot 3-(-2)\cdot 7=2=4-2.$$

ここで

$$x=2+(-4)\cdot 3=4+(-2)\cdot 7=-10.$$

と置くと, $x\equiv 2 \pmod 3$, $x\equiv 4 \pmod 7$. 合同式 ($\clubsuit$) の整数解は法 21 で一意的に存在するので, $x\equiv -10\equiv 11 \pmod{21}$ が求める解である.

□

問題 5-2 次の連立合同式の解を求めよ.

$$\begin{cases} x\equiv 3 \pmod 5 \\ x\equiv 1 \pmod 7. \end{cases}$$

例題 5-3
2^{20} を 77 で割った余りを求めよ.

[**解答**]
$2^3 \equiv 1 \pmod 7$ より $2^{20} \equiv 4 \pmod 7$ である. $2^5 \equiv -1 \pmod{11}$ より $2^{20} \equiv 1 \pmod{11}$. 従って $x = 2^{20}$ は次の連立合同式の解になる.

$$\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 1 \pmod{11}. \end{cases}$$

例題 5-2 と同様に連立合同式を解くと $x \equiv 67 \pmod{77}$. よって求める余りは 67.

□

問題 5-3 フィボナッチ数列は次で定義される数列である.

$$F_0 = 0,\ F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}\ (n = 2, 3, ...)$$

このとき, F_{100} を 6 で割った余りを求めよ.