

⑧ 中国剰余定理 (Chinese Remainder Theorem: CRT)
(§4.8, p. 62)

R : Euclid 整域.

・ 線型合同式: $m, a, b \in R$.

$a \equiv b \pmod{m}$ は x に関する解.

・ 連立線型合同式

$$\begin{cases} m_1, \dots, m_k \in R : \text{互いに素} (\forall i \neq j \Rightarrow m_i \perp m_j) \\ a_1, \dots, a_k \in R \end{cases}$$

のとき,

$$a \equiv a_i \pmod{m_i} \quad (i=1, 2, \dots, k)$$

をみたす $a \in R$ が存在する.

Theorem 4.60 (Chinese Remainder Theorem)
(see also Thm. 3.58)

$$\begin{cases} m_1, \dots, m_k \in R : \text{互いに素} \\ a_1, \dots, a_k \in R \end{cases}$$

のとき,

$$\exists a \in R \text{ s.t. } a \equiv a_i \pmod{m_i} \quad (i=1, \dots, k). \quad (*)$$

さらに, $a' \in R$ も合同式 (*) の解

$$\Leftrightarrow a \equiv a' \pmod{m}, \quad m = m_1 \cdots m_k.$$

Proof 次の性質をみたす $e_1, \dots, e_k \in R$ の存在を示す:
 $i, j \in \{1, \dots, k\}$ に対し.

$$e_j \equiv \begin{cases} 1 & \pmod{m_i} \text{ if } j=i, \\ 0 & \pmod{m_i} \text{ if } j \neq i. \end{cases} \quad (**)$$

(**) をみたす e_j が得られれば,

$$a := \sum_{i=1}^k a_i e_i$$

とおく (これは).

$$a \equiv \sum_{i=1}^k a_i e_i \equiv a_j \pmod{m_j}$$

($j=1, \dots, k$) が成り立つ.

$e_1, \dots, e_k$ の存在:

$$m := m_1 \cdots m_k, \quad m_i^* := \frac{m}{m_i} = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$$

($i=1, \dots, k$) とおくと, $m_1, \dots, m_k$ は互いに素より, $\gcd(m_i, m_i^*) = 1$.
ゆえに $t_i := (m_i^*)^{-1} \pmod{m_i}$ が存在. $\rightarrow$ (EEA, 法逆元計算 p. 35.)

そこで, $e_i := t_i m_i^*$ とおくと, e_i は $(**)$ を満たす.
さらに, a' と別の解とすると, $i=1, \dots, k$ に対して

$$\begin{aligned} a &\equiv a_i \equiv a' \pmod{m_i} && \text{for } i=1, \dots, k \\ \Leftrightarrow m_i \mid a - a' && \text{for } i=1, \dots, k \\ \Leftrightarrow m_1, \dots, m_k \text{ は互いに素より } m_1 \cdots m_k \mid a - a' \\ \Leftrightarrow a &\equiv a' \pmod{m}. \end{aligned}$$

問題 3.59 (テキスト p. 34) $a \equiv 2 \pmod{5}$, $a \equiv 3 \pmod{6}$,
 $a \equiv 5 \pmod{7}$ を満たす $a \in \mathbb{Z}$ ($0 \leq a < 5 \cdot 6 \cdot 7 = 210$)
を求めよ.

$$\left. \begin{array}{l} m_1 = 5, \quad m_2 = 6, \quad m_3 = 7. \\ a_1 = 2, \quad a_2 = 3, \quad a_3 = 5, \end{array} \right\} \text{ に対して, } e_1, e_2, e_3 \text{ を求めよ.}$$

① e_1 の計算.

$$\begin{aligned} m_1^* &= m/m_1 = 210/5 = 42. \\ (m_1^*)^{-1} \pmod{m_1} &\text{ を EEA}(42, 5) \text{ によって求める.} \end{aligned}$$

$i=0$	$r_0 = 42,$	$s_0 = 1,$	$t_0 = 0.$
$i=1$	$r_1 = 5,$	$s_1 = 0,$	$t_1 = 1,$
$i=2$	$r_2 = 42 - 8 \cdot 5 = 2,$	$s_2 = 1 - 0 \cdot 8 = 1,$	$t_2 = 0 - 1 \cdot 8 = -8.$
$i=3$	$r_3 = 5 - 2 \cdot 2 = 1.$	$s_3 = 0 - 2 \cdot 1 = -2,$	$t_3 = 1 - 2(-8) = 17.$

$$\therefore (-2) \cdot 42 + 17 \cdot 5 = 1.$$

$$(-2) \cdot 42 \equiv 1 \pmod{5}$$

$$3 \cdot 42 \equiv 1 \pmod{5}$$

$$\therefore (42)^{-1} \equiv 3 \pmod{5}.$$

$$\therefore e_1 = 3 \cdot 42 = 126.$$

② e_2 の計算.

$$m_2^* = m/n_2 = 210/6 = 35.$$

$(m_2^*)^{-1} \bmod m_2$ と EEA (35, 6) により求めよ.

$i=0$	$r_0 = 35,$	$s_0 = 1, t_0 = 0.$	
$i=1$	$r_1 = 6,$	$s_1 = 0, t_1 = 1.$	
$i=2$	$r_2 = 35 - 5 \cdot 6 = 5,$	$s_2 = 1 - 0 \cdot 5 = 1,$	$t_2 = 0 - 1 \cdot 5 = -5.$
$i=3$	$r_3 = 6 - 1 \cdot 5 = 1,$	$s_3 = 0 - 1 \cdot 1 = -1,$	$t_3 = 1 - 1 \cdot (-5) = 6.$

$$\therefore (-1) \cdot 35 + 6 \cdot 6 = 1.$$

$$(-1) \cdot 35 \equiv 1 \pmod{6}.$$

$$5 \cdot 35 \equiv 1 \pmod{6}.$$

$$\therefore (35)^{-1} \equiv 5 \pmod{6}.$$

$$\therefore e_2 = 5 \cdot 35 = 175.$$

③ e_3 の計算.

$$m_3^* = m/n_3 = 210/7 = 30.$$

$(m_3^*)^{-1} \bmod m_3$ と EEA (30, 7) により求めよ.

$i=0$	$r_0 = 30,$	$s_0 = 1, t_0 = 0.$	
$i=1$	$r_1 = 7,$	$s_1 = 0, t_1 = 1.$	
$i=2$	$r_2 = 30 - 4 \cdot 7 = 2,$	$s_2 = 1 - 0 \cdot 4 = 1,$	$t_2 = 0 - 1 \cdot 4 = -4.$
$i=3$	$r_3 = 7 - 3 \cdot 2 = 1,$	$s_3 = 0 - 3 \cdot 1 = -3,$	$t_3 = 1 - 3 \cdot (-4) = 13.$

$$\therefore (-3) \cdot 30 + 13 \cdot 7 = 1.$$

$$(-3) \cdot 30 \equiv 1 \pmod{7}.$$

$$4 \cdot 30 \equiv 1 \pmod{7}.$$

$$\therefore (30)^{-1} \equiv 4 \pmod{7}.$$

$$\therefore e_3 = 4 \cdot 30 = 120.$$

④ a の計算.

$$\begin{aligned} a &= a_1 e_1 + a_2 e_2 + a_3 e_3 \\ &= 2 \cdot 126 + 3 \cdot 175 + 5 \cdot 120 \\ &= 252 + 525 + 600 \\ &= 1377 \\ &\equiv \underline{\underline{117}} \pmod{210}. \end{aligned}$$

⑤ 検算.

$$117 \equiv -3 \pmod{5}$$

$$\equiv 2 \pmod{5}$$

$$\equiv 3 \pmod{6}$$

$$\equiv 5 \pmod{7}$$

— ①

— ②

— ③

①, ②, ③ ok.

中々求めた a の - 2.7 117.



10

15

20

25

30

35

40