◎ 中国剰余定理 (Chinese Remainder Theorem ; CRT)

R: Euclid整域.

・ 線型合同式 : $n, a, b \in R$.

$$ax \equiv b \pmod{n}$$ を x について解く.

・ 連立線型合同式

$$\begin{cases} n_1, \dots, n_k \in R : \text{互いに素.} \ (\forall i \neq j \Rightarrow n_i \perp n_j) \\ a_1, \dots, a_k \in R. \end{cases}$$

のとき.

$$a \equiv a_i \pmod{n_i} \quad (i = 1, 2, \dots, k)$$ をみたす $a \in R$ を見つける.

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

$$\begin{cases} n_1, \dots, n_k \in R : \text{互いに素.} \\ a_1, \dots, a_k \in R \end{cases}$$

のとき.

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

さらに, $a' \in R$ も合同式 $(*)$ の解

$$\iff a \equiv a' \pmod{n}, \quad n = n_1 \cdots n_k.$$

Proof) 次の性質をみたす $e_1, \dots, e_k \in R$ の存在を示す:

$i, j = 1, \dots, k$ について.

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

$(**)$ をみたす e_j が得られれば,

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

とおくことにより.

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

が成り立つ.

$e_1, \dots, e_k$ の存在：

$$n := n_1 \cdots n_k, \qquad n_i^* := \frac{n}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k,$$

とおくと．$n_1, \dots, n_k$：互いに素より $\gcd(n_i, n_i^*) = 1$．

ゆえに $t_i := (n_i^*)^{-1} \bmod n_i$ が存在．→ (EEA)

そこで $e_i := t_i n_i^*$ とおくと．e_i は (**) をみたす．

さらに．a' を別の解とすると．$i = 1, \dots, k$ に対して

$a \equiv a_i \equiv a' \pmod{n_i}$．

$\Leftrightarrow$ $n_i \mid a - a'$ for $i = 1, \dots, k$．

$\Leftrightarrow$ $n_1, \dots, n_k$ は互いに素より，$n_1 \cdots n_k \mid a - a'$．

$\Leftrightarrow$ $a \equiv a' \pmod{n}$． ☒

問題 3.59 $a \equiv 2 \bmod 5$，$a \equiv 3 \bmod 6$，$a \equiv 5 \bmod 7$ をみたす $a \in \mathbb{Z}$ を求める．

$n_1 = 5,\ n_2 = 6,\ n_3 = 7,$
$a_1 = 2,\ a_2 = 3,\ a_3 = 5$ } に対し，
e_1, e_2, e_3 を求める．

$n = 5 \cdot 6 \cdot 7 = 210$．
$(0 \le a < 210)$ を求める

① e_1 の計算．

$n_1^* = n/n_1 = 210/5 = 42$．
$(n_1^*)^{-1} \bmod n_1$ を EEA(42, 5) により求める．

$i=0$：	$r_0 = 42$．		$s_0 = 1$，	$t_0 = 0$．
$i=1$：	$r_1 = 5$．		$s_0 = 0$，	$t_0 = 1$．
$i=2$：	$r_2 = 42 - 8 \cdot 5 = 2$．	$q_1 = 8$．	$s_2 = 1 - 0 \cdot 8 = 1$．	$t_2 = 0 - 1 \cdot 8 = -8$
$i=3$：	$r_3 = 5 - 2 \cdot 2 = 1$．	$q_2 = 2$．	$s_3 = 0 - 2 \cdot 1 = -2$	$t_3 = 1 - 2 \cdot (-8) = 17$．

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

$(-2)\cdot 42 \equiv 1 \mod 5$

$3\cdot 42 \equiv 1 \mod 5$

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

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

② e_2 の計算.

$n_2^* = n/n_2 = 210/6 = 35.$

$(n_2^*)^{-1} \mod n_2$ を EEA $(35, 6)$ により求める.

$i=0:\ r_0 = 35,\qquad s_0 = 1,\ t_0 = 0.$

$i=1:\ r_1 = 6\qquad s_1 = 0.\ t_1 = 1.$

$i=2:\ r_2 = 35 - 5\cdot 6 = 5\qquad q_1 = 5,\qquad s_2 = 1 - 0\cdot 5 = 1,\qquad t_2 = 0 - 1\cdot 5 = -5.$

$i=3:\ r_3 = 6 - 1\cdot 5 = 1.\qquad q_2 = 1,\qquad s_3 = 0 - 1\cdot 1 = -1.\qquad t_3 = 1 - 1\cdot(-5) = 6.$

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

$(-1)\cdot 35 \equiv 1 \mod 6.$

$5\cdot 35 \equiv 1 \mod 6$

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

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

③ e_3 の計算.

$n_3^* = n/n_3 = 210/7 = 30.$

$(n_3^*)^{-1} \mod n_3$ を EEA $(30, 7)$ により求める.

$i=0:\ r_0 = 30.\qquad s_0 = 1,\ t_0 = 0$

$i=1:\ r_1 = 7\qquad s_1 = 0,\ t_1 = 1.$

$i=2:\ r_2 = 30 - 4\cdot 7 = 2,\qquad q_1 = 4,\qquad s_2 = 1 - 0\cdot 4 = 1,\qquad t_2 = 0 - 1\cdot 4 = -4.$

$i=3:\ r_3 = 7 - 3\cdot 2 = 1,\qquad q_2 = 3,\qquad s_3 = 0 - 3\cdot 1 = -3,\qquad t_3 = 1 - 3\cdot(-4) = 13.$

$$\therefore\ (-3)\cdot 30 + 13\cdot 7 = 1.$$
$$(-3)\cdot 30 \equiv 1 \mod 7.$$
$$4\cdot 30 \equiv 1 \mod 7$$
$$\therefore\ (30)^{-1} \equiv 4 \mod 7$$
$$\therefore\ e_3 = 4\cdot 30 = 120.$$

④ aの計算.

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

⑤ 検算.

$$\begin{aligned} 117 &\equiv -3 \mod 5 \\ &\equiv 2 \mod 5. \quad \text{— ①} \\ &\equiv 3 \mod 6 \quad \text{— ②} \\ &\equiv 5 \mod 7 \quad \text{— ③} \end{aligned}$$

①, ②, ③よりOK.

ゆえに求めるaの一つは 117.

$\blacksquare$