アルゴリズム論特論　(塩田)

— Chinese Remainder Algorithm —

定理 1　(中国剰余定理)　m, n を互いに素な 2 つの法とするとき、次の連立合同式は $m \times n$ を法として唯一の解を持つ：

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \cdots\cdots (*)$$

☆　m, n が互いに素なら

mod mn の情報 x　$\overset{1:1}{\longleftrightarrow}$　(mod m の情報, mod n の情報) (a, b)

Alg.2　(中国剰余アルゴリズム)

$$\begin{cases} \text{入力：}\ a, b, m, n \quad (\ \text{ただし}\ \gcd(m, n) = 1\ ) \\ \text{出力：}\ (*)\ \text{の解} \end{cases}$$

1°　拡張ユークリッドアルゴリズムを用いて $mu + nv = 1$ を満たす u, v を求める

2°　$x = a(nv) + b(mu)$ % (mn) を出力

例 3　$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{17} \end{cases}$

$7 \times 5 + 17 \times (-2) = 1$ より

$$x = (3 \times 17 \times (-2) + 5 \times 7 \times 5)\ \%\ (7 \times 17) = (-102 + 175)\ \%\ 119 = 73$$

定理 4　$m_1, m_2, \cdots m_k$ を、どの 2 つも互いに素な k 個の法とするとき、次の連立合同式は $m_1 \times m_2 \times \cdots \times m_k$ を法として唯一の解を持つ：

$$\begin{cases} (1) \quad x \equiv a_1 \pmod{m_1} \\ (2) \quad x \equiv a_2 \pmod{m_2} \\ \qquad \vdots \\ (k) \quad x \equiv a_k \pmod{m_k} \end{cases} \quad \cdots\cdots (\sharp)$$

Alg.5　(**Alg.2** を繰り返し用いる作戦)

$$\begin{cases} \text{入力：}\ a_1, a_2, \cdots, a_k;\ m_1, m_2, \cdots, m_k \\ \qquad (\ \text{ただし}\ m_i\ \text{たちはどの 2 つも互いに素}\ ) \\ \text{出力：}\ (\sharp)\ \text{の解} \end{cases}$$

$A = a_1,\ M = m_1$

for $i = 2$ to k

　　新 $A = \left(\text{連立合同式} \begin{cases} x \equiv A \pmod{M} \\ x \equiv a_i \pmod{m_i} \end{cases} \text{の解} \right)$

　　新 $M = M \times m_i$

A を出力

Alg.7 （ **Alg.2** を一般化する作戦 ）

入出力は **Alg.5** に同じ

1° $M = m_1 \times m_2 \times \cdots \times m_k$ とおく

2° 各 i について、拡張ユークリッドアルゴリズムを用いて
$m_i u_i + (M/m_i)\, v_i = 1$ を満たす u_i, v_i を求め、$w_i = (M/m_i)v_i$ とおく

3° $x = \sum_i a_i w_i$ % M を出力

例
$$\begin{cases} (1) \quad x \equiv 3 \quad (\bmod 7) \\ (2) \quad x \equiv 5 \quad (\bmod 17) \\ (3) \quad x \equiv 11 \quad (\bmod 37) \end{cases}$$

Alg.5 を用いた解法

例 3 より、

(1) かつ (2) $\Leftrightarrow$ (4) $x \equiv 73 \quad (\bmod 119)$

$119 \times 14 + 37 \times (-45) = 1$ より、(4) かつ (3) の解は

$$\begin{aligned} x &= (73 \times 37 \times (-45) + 11 \times 119 \times 14) \text{ \% } (119 \times 37) \\ &= (-121545 + 18326) \text{ \% } 4403 = 2453 \end{aligned}$$

Alg.5 を用いた解法**'** 式を組み合わせる順番を変えてみよう。

(2) かつ (3) の解は、$17 \times (-13) + 37 \times 6 = 1$ より、

$$\begin{aligned} x &= (5 \times 37 \times 6 + 11 \times 17 \times (-13)) \text{ \% } (17 \times 37) \\ &= (1110 - 2431) \text{ \% } 629 = 566 \end{aligned}$$

すなわち

(2) かつ (3) $\Leftrightarrow$ (5) $x \equiv 566 \quad (\bmod 629)$

$629 \times (-1) + 7 \times 90 = 1$ より、(5) かつ (1) の解は

$$\begin{aligned} x &= (566 \times 7 \times 90 + 3 \times 629 \times (-1)) \text{ \% } (629 \times 7) \\ &= (356580 - 1887) \text{ \% } 4403 = 2453 \end{aligned}$$

もちろん、答は同じになる。

Alg.7 を用いた解法

1° $M = 7 \times 17 \times 37 = 4403$

2° $i = 1$: $7 \times 90 + 629 \times (-1) = 1 \Rightarrow w_1 = -629$
$i = 2$: $17 \times 61 + 259 \times (-4) = 1 \Rightarrow w_2 = 259 \times (-4) = -1036$
$i = 3$: $37 \times (-45) + 119 \times 14 = 1 \Rightarrow w_3 = 119 \times 14 = 1666$

3° $x = (3 \times (-629) + 5 \times (-1036)) + 11 \times 1666$ % (4403)
$= 11259$ % $4403 = 2453$