驚くべき中国式剰余定理

上野孝司

2017 年 5 月 9 日

概要

驚くべき中国式剰余定理

１．孫子定理と百五減算

“３で割って２余り、５で割って３余り、７で割って５余る数を求めよ”なる問題はたびたび目にする問題である。実はこの問題の解決法は、古代中国から知られており、南北朝時代（439 − 589）に編纂されたといわれる算術書「孫子算経」に記述があり**「孫子定理」**として解法が記されている。この問題は「孫子算経」とともに日本にも伝わり、後に和算が起こった江戸時代に**「百五減算」**として知られた（105 は、３と５と７の積に由来する）。

一方で孫子定理は、数学の王者ガウスが「整数論」（1801 年）で体系的に扱っており、欧米では**中国式剰余定理（**$chinese\ remainder\ theorem$) として現代数学に代数学の一大定理としての地歩を築いている。可換環論にも現れる重要な定理となっている。現代代数学でも重要な役割を果たしているこの定理がすでに古代中国で扱われていたことは驚くべき事実である。本稿では、整数の最大公約数を求める一般的方法として知られるユークリッドの互除法を述べた後、ガウスが対称性を伴って求めた中国式剰余定理の一般的解法を紹介する。

２．ユークリッドの互除法

ユークリッドの互除法は、次の単純な補題に基づく。

補題：整数 a, b の差 $a - b$ が $m(\neq 0)$ で割り切れるならば、$(a, m) = (b, m)$ ((m, n) は m と n の最大公約数）である。すなわち、

$$a \equiv b (\mathrm{mod}\, m) \Rightarrow (a, m) = (b, m)$$

[証明]$a - b = mq$ と表せるから、$b = a - mq$　または　$a = b + mq$. よって、a, m の任意の公約数は b の約数となり、逆に b, m の任意の公約数は a の約数となる。よって、a, m の公約数の全体と b, m の公約数の全体は一致する。よって、特に公約数のうち最大の整数は一致する。■

この補題を用いてユークリッドの互除法を述べる。いま a, b を正の整数（$a \geq b$) として、次のような

割り算の列をつくる。

$$
\begin{array}{lcll}
a & = & b \times q_1 + r_2 & 0 < r_2 < b \\
b & = & r_2 \times q_2 + r_3 & 0 < r_3 < r_2 \\
r_2 & = & r_3 \times q_3 + r_4 & 0 < r_4 < r_3 \\
 & & \cdots\cdots\cdots\cdots & \\
r_{n-2} & = & r_{n-1}q_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} & = & r_n q_n &
\end{array}
$$

$$
\begin{aligned}
r_2 &= r_3 \times q_3 + r_4 \\
r_3 &= r_4 \times q_4 + r_5
\end{aligned}
$$

n 列	除数	余り	
	↓	↓	→ くり返し
$(n+1)$ 列	被除数	除数	

という規則がくり返し用いられていることに注意されたい。ここで、b, r_2, r_3 は正の整数の減少列で、たかだか b 個の数しか含み得ないから、必ず有限回の後には割り切れる場合が必ず生じるのである。

このとき、補題をくり返し用いると
$(a,b) = (b,r_2) = (r_2,r_3) = \cdots\cdots = (r_{n-1},r_n)$
となるが、$r_n | r_{n-1}$ であるから、$(r_{n-1},r_n) = r_n$
ゆえに、$(a,b) = r_n$ となる。
[例 1]
$a = 255, b = 221$
$255 = 221 \times 1 + 34$
$221 = 34 \times 6 + 17$
$34 \quad = 17 \times 2$
$\therefore (255, 221) = 17$
[例 2]
$a = 7935,\ b = 5796$
$7935 = 5796 \times 1 + 2139$
$5796 = 2139 \times 2 + 1518$
$2139 = 1518 \times 1 + 621$
$1518 = 621 \times 2 + 276$
$621 \quad = 276 \times 2 + 69$
$276 \quad = 69 \times 4$
$\therefore (7935, 5796) = 69$

ところで、上述の割り算の過程をよくみると、(a,b) の最大公約数 d を a, b の一次式で表すことができる。
例 1 では
$34 = a - b$
$17 = b - 34 \times 6 = b - 6(a-b)$
$\quad = b - 6a + 6b$
$\quad = -6a + 7b$

よって
$d = -6a + 7b$

例２では
$2139 = a - b$
$1518 = b - 2139 \times 2 = b - 2(a - b) = -2a + 3b$
$621 \quad = (a - b) - 1518 = (a - b) - (-2a + 3b)$
$\qquad = 3a - 4b$
$276 = 1518 - 621 \times 2 = (-2a + 3b) - 2(3a - 4b)$
$\quad = -8a + 11b$
$69 = 621 - 2 \times 276 = 3a - 4b - 2(-8a + 11b)$
$\quad = 19a - 26b$
よって、
$d = 19a - 26b$

以上から次の重要な定理が得られる。
【定理１】a, b を整数としたとき、a, b の最大公約数 $d = (a, b)$ は
適当な整数 u, v によって

$$\underline{d = au + bv}$$

の形に表せる。特に a と b が互いに素、つまり $(a, b) = 1$ のとき

$$\underline{1 = au + bv}$$

となる整数 u, v が存在する。
また、$ax + by$ の形の整数は、すべて d の倍数である ことが示される（証明略)。

$$\{ax + by | x, y \in \mathbb{Z}\} = \{kd | k \in \mathbb{Z}\}$$

３．１次の合同方程式

整数の定数 a, b, m, 未知の整数 x に対して

$$ax \equiv b (\mathrm{mod}\, m)$$

のような形の方程式を１次の合同方程式という。例えば

$$5x \equiv 2 (\mathrm{mod}\, 17)$$

は、５倍して２を引いて 17 で割り切れる数を求める。あるいは、5 を何倍すれば 17 で割った余りが２になるか？という問題である。以下、この種の合同方程式の一般解を求める方法を示す。

$$ax \equiv b (\mathrm{mod}\, m)$$

は、

$$ax - b = my \Longleftrightarrow ax - my = b \cdots (1)$$

の整数解を求めることである。定理１より(1) に解があるための必要十分条件は、b が a と m の最大公約数 $(a, m) = d$ の倍数
ことである。このとき、

$a = a'd,\ m = m'd,\ b = b'd$ とおけるから (1) を d で割ると

$$a'x - m'y = b' \cdots (2)$$

ここでユークリッドの互除法を用いて (2) の特殊解 (x_0, y_0) を一組求めると、(2) の一般解を以下のように
求めることができる。

$\begin{cases} a'x - m'y = b' \\ a'x_0 - m'y_0 = b' \end{cases}$ より

$a'(x - x_0) = m'(y - y_0)$

$(a', m') = 1$ により、

$x - x_0 = \dfrac{m'}{a'}(y - y_0)$ よって

$y - y_0 = qa'$

$x - x_0 = \dfrac{m'}{a'} \cdot qa' = qm'$ 以上より、

$\begin{cases} x = x_0 + m'q \\ y = y_0 + a'q \end{cases}$

(q は任意の整数)

を得る。この解を法 m で考えると、２つの解

$x_1 = x_0 + m'q_1, x_2 = x_0 + m'q_2$ をとると、$x_1 = x_2 (\mathrm{mod}\, m)$ となる条件は

$x_0 + m'q_1 \equiv x_0 + m'q_2 (\mathrm{mod}\, m) \rightarrow m'q_1 \equiv m'q_2 (\mathrm{mod}\, m) \Longleftrightarrow m'q_1 - m'q_2 = mz (z \in \mathbb{Z})$

両辺を m' で割って、

$$q_1 - q_2 = dz (m = m'd) \Longleftrightarrow q_1 \equiv q_2 (\mathrm{mod}\, d)$$

したがって、法 m で相異なる解は、法 d の類の個数 d だけあり、それらは、

$$x = x_0 + m'i (\mathrm{mod}\, m)(i = 0, 1, 2, \cdots, d - 1)$$

の d 個であることがわかる。■

以上より、以下の定理を得る。

【定理２】 １次の合同方程式 $ax = b (\mathrm{mod}\, m)$ は、b が $(a, m) = d$ の倍数であるときのみ解を持ち、その解は m を法として d 個ある。特に、$(a, m) = 1$ のとき、上の合同方程式は m を法としてただ一つの解を持つ。

[例]

$$12x \equiv 9 (\mathrm{mod}\, 45)$$

$(12, 45) = 3$ で割ると、

$$4x \equiv 3 (\mathrm{mod}\, 15)$$

$$4x - 15y = 3 \cdots (3)$$

の特殊解を求める。$(4, 15) = 1$ により確かに特殊解は存在する。
$4u - 15v = 1$
の特殊解を互除法（または直感）で求めると
$4 \cdot 4 - 15 \cdot 1 = 1$　より、　$u = 4, v = 1$　　よって (3) の特殊解は
$x_0 = 4 \times 3 = 12,\ \ y_0 = 1 \times 3 = 3$
このとき、$m' = 15$ だから求める解は、

$$x = x_0 + m'i (\mathrm{mod}\, m)$$

$$= 12 + 15i (i = 0, 1, 2) (\mathrm{mod}\, 45)$$

の３つが解。つまり、

$$x = 12, 27, 42 (\mathrm{mod}\, 45)$$

４．中国式剰余定理

３では単一の１次合同方程式を扱ったが、本節では本稿の主題である中国式剰余定理、すなわち、一次の連立合同方程式の解法を求める。

【定理】（中国式剰余定理）

$m_1, m_2, \cdots, m_n$ を対ごとに（どの２つをとっても）互いに素な整数としたとき、１次の連立合同方程式

$$x \equiv b_1 (\mathrm{mod}\, m_1)$$

$$x \equiv b_2 (\mathrm{mod}\, m_2)$$

$$\vdots$$

$$x \equiv b_n (\mathrm{mod}\, m_n)$$

は積 $M = m_1 m_2 \cdots m_n$ を法としてただ一つの解を持つ。
[証明]$M = m_1 m_2 \cdots m_n, M_i = \dfrac{M}{m_i}$　とおくと
仮定から $(m_i, M_i) = 1$　　よって定理２より

$$M_i f_i \equiv 1 (\mathrm{mod}\, m_i)$$

を満たす整数 $f_i (i = 1, 2, \cdots, n)$ が求められる。

$$t_i = M_i f_i$$

とすると、$t_i \equiv 1 (\mathrm{mod}\, m_i), t_i = 0 (\mathrm{mod}\, j)$
であるから

$$t_1 b_1 + t_2 b_2 + \cdots + t_n b_n \equiv b_i (\mathrm{mod}\, m_i)$$

となることがわかり、

$$x = t_1 b_1 + t_2 b_2 + \cdots + t_n b_n$$

が一つの解となる。
[例]

$$x \equiv 2 (\mathrm{mod}\, 3)$$

$$x \equiv 3 (\mathrm{mod}\, 5)$$

$$x \equiv 5 (\mathrm{mod}\, 7)$$

$M_1 = 35, M_2 = 21, M_3 = 15$

$$\begin{cases} 35 f_1 \equiv 1 (\mathrm{mod}\, 3) \rightarrow f_1 = -1 \\ 21 f_2 \equiv 1 (\mathrm{mod}\, 5) \rightarrow f_2 = 1 \\ 15 f_3 \equiv 1 (\mathrm{mod}\, 7) \rightarrow f_3 = 1 \end{cases}$$

$$x = t_1 b_1 + t_2 b_2 + t_3 b_3$$

$$\begin{cases} t_1 = M_1 f_1 = 35 \times (-1) = -35 \\ t_2 = M_2 f_2 = 21 \times 1 = 21 \\ t_3 = M_3 f_3 = 15 \times 1 = 15 \end{cases}$$

よって、

$$\begin{aligned} x &= -35 \times 2 + 21 \times 3 + 15 \times 5 \\ &= 68 (\mathrm{mod}\, 105) \end{aligned}$$

$x = 68 + 105k (k \in \mathbb{Z})$ ■

[例 2]

$$x \equiv b_1 (\mathrm{mod}\, 3)$$

$$x \equiv b_2 (\mathrm{mod}\, 7)$$

$$x \equiv b_3 (\mathrm{mod}\, 16)$$

$M = 3 \times 7 \times 16$

$$\begin{cases} M_1 = 7 \times 16 = 112 \\ M_2 = 3 \times 16 = 48 \\ M_3 = 3 \times 7 = 21 \end{cases}$$

$$\begin{cases} 112 f_1 \equiv 1 (\mathrm{mod}\, 3) \\ 48 f_2 \equiv 1 (\mathrm{mod}\, 7) \\ 21 f_3 = 1 (\mathrm{mod}\, 16) \end{cases}$$

$\rightarrow f_1 = 1, f_2 = -1, f_3 = -3$

$$\begin{cases} t_1 = M_1 f_1 = 112 \\ t_2 = M_2 f_2 = -48 \\ t_3 = M_3 f_3 = -63 \end{cases}$$

よって

$x = 112b_1 - 48b_2 - 63b_3$ ■

＊本稿の執筆に際しては、以下を参考とした。

・ガロワと方程式（草場公邦、朝倉書店）

・代数系入門（松坂和夫、岩波書店）