合同式と中国剰余定理
Congruence Relation
& Chinese Remainder Theorem

文字は全て整数とする.

定義 1 a, b の差が m の倍数であるとき，a と b は m を法 (modulus) として互いに**合同** (congluent modulo n) であるといい,

$$a \equiv b \pmod{m}$$

と表す.

定理 1 m を法として,

$$a \equiv b, c \equiv d$$

ならば,

$$a \pm c \equiv b \pm d$$

$$ac \equiv bd$$

このように合同式は加減乗法に関しては等式を同じように扱えるが，除法に関しては等式とは違う.

定理 2

$$ac \equiv bc \pmod{m}$$

のとき,

$$a \equiv b \pmod{\frac{m}{(m,c)}}$$

[証明] $(m, c) = d, c = c'd, m = m'd$ とすると,

$$c'd(a - b) = m'dk$$

とおける．つまり

$$c'(a - b) = m'k$$

であり，$(c', m') = 1$ なので，$a - b$ は m' の倍数である.

$$\therefore a \equiv b \pmod{m'}$$

[証明おわり]

このことは等式において，両辺を 0 で割ってはいけないことと似ている.

定理 3 $(a, m) = 1$ のとき，一次合同式

$$ax \equiv b \pmod{m} \tag{1}$$

は一つの解を有す.

[証明]　$(a, m) = 1$ であるため，

$$0, a, 2a, \cdots, (m-1)a \tag{2}$$

は全て不合同である．なぜならば，(2) の元のうち，$ia \equiv ja$ とすると，$a(i-j) \equiv 0$ となり，$i = j$ 以外の場合がないからである．よって，(2) は m を法とする剰余系をなす．つまり (1) の b は (2) のどれかの数であり，x は対応する a の係数のいずれかである．つまり解は唯一である．　[証明おわり]

定理 4　$(a, m) = d$ のとき，一次合同式

$$ax \equiv b \pmod{m} \tag{3}$$

は b が d の倍数である場合に限って解をもつ．解の個数は d 個である．

[証明]　$a = a'd, m = m'd$ とすると，(3) は

$$a'dx \equiv b \pmod{m'd}$$

つまり，

$$a'dx - b = m'dk$$

とおける．

$$(a'x - m'k)d = b$$

より b は d の倍数でなければならない．$b = b'd$ とおくと，

$$(a'x - m'k)d = b'd$$

$$a'x - m'k = b'$$

つまり x は

$$a'x \equiv b' \pmod{m'} \tag{4}$$

の解であり，定理 3 より解を一つもつ．この解の個数は m' を法とした場合であって，m を法とした場合ではない．(4) の解を $x_0 (0 \leq x_0 < m')$ とすると，(3) を満たす解は

$$x_0, x_0 + m', x_0 + 2m', \cdots, x_0 + (d-1)m' (< m'd = m)$$

である．つまり d 個の解がある．　[証明おわり]

合同式

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

を解く事は不定方程式

$$ax - my = b$$

を解く事とひとしい．

定理 5　$(m, n) = 1$ のとき，連立一次合同式

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

の解は mn を法としてただ一つある．

[証明]

$$\begin{cases} x = a + mt & (5) \\ x = b + nu & (6) \end{cases}$$

を解くと

$$a + mt = b + nu$$

となり，これは不定方程式

$$mt - nu = b - a$$

を解くことと等しい．$b - a = A$ とすると，これは合同式

$$mt \equiv A \pmod{n}$$

を解くこととひとしく，$(m, n) = 1$ なので解は一つあり，それを t_0 とすると

$$t = t_0 + kn \text{ と表せる．}$$

これを (5) に代入してやると

$$x = a + mt_0 + kmn$$

つまり mn を法として解は一つあり，その解は

$$x \equiv a + mt_0 \pmod{mn}$$

である． [証明おわり]

定理 6 $(m_1, m_2, m_3, \cdots, m_k) = 1$ のとき連立一次合同式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ \cdots\cdots\cdots\cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

の解は $m_1 m_2 m_3 \cdots m_k$ を法としてただ一つ存在する．

[証明略] 定理 5 の証明を繰り返せばよいだけのことである．
定理 5 および 6 は**中国剰余定理** (Chinese remainder theorem)[*1]と呼ばれることもある．

定理 7 $(m, n) = d, \mathrm{lcm}(m, n) = l$ のとき，連立一次合同式

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

[*1] 中国の算術書『孫子算経』に書かれた「3 で割ると 2 余り，5 で割ると 3 余り，7 で割ると 2 余る数は何か」という問題とその解法に由来する ([2]).『孫子算経』は中国の古い数学書．唐の時代に官吏を養成するための教科書として選定された「十部算経」のひとつ．著者不詳だが，おそらく 3〜5 世紀の三国時代か晋，あるいは劉宋時代に成立したと考えられている．(引用 [3])

が解をもつための必要十分条件は

$$a \equiv b \pmod{d}$$

であり，その解は l を法としてただ一つある．

[証明]

$$\begin{cases} x = a + mt & (7) \\ x = b + nu & (8) \end{cases}$$

を解くと

$$a + mt = b + nu$$

となり，これは不定方程式

$$mt - nu = b - a$$

を解くことと等しい．一次不定方程式の解の存在に関する定理より，この不定方程式が解を持つ条件は $b - a$ が d の倍数であるときである（あるいは定理 4 からも明らかである）．つまり

$$a \equiv b \pmod{d}$$

である．定理 4（あるいはその証明の過程）より合同式

$$mt \equiv b - a \pmod{n}$$

の解の個数は d 個つまり $\dfrac{n}{d}$ を法として 1 個ある．その 1 個の解を t_0 とすると

$$t = t_0 + \frac{kn}{d} \text{と表せる．}$$

これを (7) に代入してやると

$$x = a + \frac{mt_0}{d} + \frac{kmn}{d} = a + \frac{mt_0}{d} + kl$$

つまり l を法として解は一つあり，その解は

$$x \equiv a + \frac{mt_0}{d} \pmod{l}$$

である． [証明おわり]

問題 1 百五減算（あるいは前述の『孫子算経』に書かれた問題）について考察せよ．

[解]　百五減算というのは和算の用語であるが，『孫子算経』の問題と本質的に同一である．100 以下の自然数（実際は 105 まで許されるのだが）を思い浮かべさせ，その数を 3,5,7 で割った余りを答えさせる．その余りから元の数を当てるというものである．つまりは連立一次合同式

$$\begin{cases} x \equiv a \pmod{3} & (9) \\ x \equiv b \pmod{5} & (10) \\ x \equiv c \pmod{7} & (11) \end{cases}$$

を解くのに等しい．定理 5 より解は $3 \times 5 \times 7 = 105$ を法としてただ一つある．実際に解いてみると，(9) より，

$$x = a + 3t \tag{12}$$

(12) を (10) に代入して

$$a + 3t \equiv b \pmod 5$$

つまり

$$3t \equiv b - a \pmod 5$$

両辺を 2 倍して

$$t \equiv 2(b - a) \pmod 5$$

つまり

$$t = 2(b - a) + 5u$$

とおける．これを (12) に代入して，

$$x = 6b - 5a + 15u \tag{13}$$

これをさらに (11) に代入すると，

$$6b - 5a + 15u \equiv c \pmod 7$$

$$15u \equiv 5a - 6b + c \pmod 7$$

$$u \equiv -2a + b + c \pmod 7$$

$$\therefore u = -2a + b + c + 7v$$

とおける．これを (13) に代入すると

$$\begin{aligned} x &= 6b - 5a + 15(-2a + b + c + 7v) \\ &= -35a + 21b + 15c + 105v \\ \therefore x &\equiv -35a + 21b + 15c \pmod{105} \end{aligned}$$

あるいは

$$x \equiv 70a + 21b + 15c \pmod{105}$$

『孫子算経』に書かれた問題は

$$(a, b, c) = (2, 3, 2)$$

であるので，

$$\begin{aligned} x &\equiv 70 \times 2 + 21 \times 3 + 15 \times 2 \\ &\equiv 233 \\ &\equiv 23 \pmod{105} \end{aligned}$$

となる．百五減算の減は 105 を超えたら 105 を引けという意味である．

定理 8 （ガウスの方法）$(m_1, m_2, m_3, \cdots, m_k) = 1$ のとき連立一次合同式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{14}$$

の解は

$$x \equiv a_1 M_1 t_1 + a_2 M_2 t_2 + a_3 M_3 t_3 + \cdots + a_k M_k t_k \pmod{m_1 m_2 m_3 \cdots m_k} \tag{15}$$

である．ただし，

$$\begin{cases} M_1 = m_2 m_3 m_4 \cdots m_k \\ M_2 = m_1 m_3 m_4 \cdots m_k \\ M_3 = m_1 m_2 m_4 \cdots m_k \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ M_k = m_1 m_2 m_3 \cdots m_{k-1} \end{cases}$$

$$\begin{cases} M_1 t1 \equiv 1 \pmod{m_1} \\ M_2 t_2 \equiv 1 \pmod{m_2} \\ M_3 t_3 \equiv 1 \pmod{m_3} \\ \cdots\cdots\cdots\cdots\cdots \\ M_k t_k \equiv 1 \pmod{m_k} \end{cases}$$

［証明］(15) を満たせば (14) の各式を全て満たす．たとえば (15) の右辺の第 2 項以降は全て m_1 で割り切れるので

$$x \equiv a_1 M_1 t_1 \equiv a_1 \pmod{m_1}$$

他の式も同様である．よって (15) は (14) の解のうちの一つであることは明らかである．(14) の解が (15) 以外にあるかも知れないという疑問が残るが，定理 6 により，この合同式の解は唯一であることがわかっているので (15) がその唯一の解である． ［証明おわり］

問題 1 をガウスの方法で解いてみると，

$$\begin{cases} M_1 = 5 \times 7 = 35 \\ M_2 = 3 \times 7 = 21 \\ M_3 = 3 \times 5 = 15 \end{cases}$$

$$\begin{cases} 35 \times (-1) \equiv 1 \pmod{3} \\ 21 \times 1 \equiv 1 \pmod{5} \\ 15 \times 1 \equiv 1 \pmod{7} \end{cases}$$

より

$$x \equiv -35a + 21b + 15c \pmod{105}$$

参考文献

[1] 高木貞治『初等整数論講義第 2 版」（共立出版社，1997 年）

[2] 「ウィキペディア（Wikipedia)」<http://ja.wikipedia.org/wiki/>

[3] 「エンカルタ百科事典ダイジェスト」<http://jp.encarta.msn.com/>