講義資料 (7): 合同式，中国人の剰余定理

7.1 合同式

本節は，教科書 3.3 節の前半 (pp.127–131) に対応する．

定義 7.1 整数 a, b の差 $a - b$ が，ある整数 n $(\neq 0)$ の倍数であるとき，a, b は n **を法として合同** (congruence modulo n) であるといい，$a \equiv b \pmod{n}$ と記す．また，この形の式を**合同式** (congruence expression) と呼ぶ． □

定理 7.2 以下の 3 条件は同値である．

(1) $a \equiv b \pmod{n}$

(2) $\exists t \in \mathbb{Z}.\ a = b + tn$

(3) $a \bmod n = b \bmod n$

証明

- (1)⇒(2) を示す．$a \equiv b \pmod{n} \Rightarrow \exists t \in \mathbb{Z}.\ a - b = tn \Rightarrow \exists t \in \mathbb{Z}.\ a = b + tn$
- (2)⇒(3) を示す．$a \bmod n = (b + tn) \bmod n = b \bmod n$
- (3)⇒(1) を示す．$a \bmod n = b \bmod n$ とする．mod の定義より，ある整数 q, q' が存在して $a = qn + (a \bmod n)$ かつ $b = q'n + (b \bmod n)$．よって，$a - qn = b - q'n$．よって，$a - b = (q - q')n$ であるので合同式の定義より $a \equiv b \pmod{n}$． □

定理 7.3 $a \equiv b \pmod{n}$ で整数上の関係を与えると同値関係になる．すなわち，以下の 3 つの性質が成り立つ．

(反射性) $a \equiv a \pmod{n}$

(対称性) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

(推移性) $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

証明

(反射性) $a - a = 0 = 0 \cdot n$ なので $a \equiv b \pmod{n}$.

(対称性) $a \equiv b \pmod{n}$ とする．定義より，ある整数 t が存在して $a - b = tn$．よって，$b - a = (-t)n$ なので $b \equiv a \pmod{n}$ を得る．

(推移性) $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ とする．定義より，ある整数 s, t が存在して $a - b = sn$ かつ $b - c = tn$．よって，$a - c = (s + t)n$ なので $a \equiv c \pmod{n}$ を得る．
□

NOTE: 推移性が成り立つので，$a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ を，$a \equiv b \equiv c \pmod{n}$ と略記することが多い．例えば，$25 + 4 \equiv 29 \equiv 1 \pmod{7}$.

定理 7.4 a, b, c, d を任意の整数とし，n を 0 でない任意の整数とする．

- $a \equiv b \pmod{n}$ と $c \equiv d \pmod{n}$ が成立するならば以下の合同式も成立.

  (1) $a + c \equiv b + d \pmod{n}$

  (2) $a - c \equiv b - d \pmod{n}$

  (3) $ac \equiv bd \pmod{n}$

  (4) $a^k \equiv b^k \pmod{n}$　for any $k \in \mathbb{N}$

- $c \neq 0$ とし，$(c, n) = d$ とすると以下が成立.

  (5) $ca \equiv cb \pmod{n}$ ならば $a \equiv b \pmod{\frac{n}{d}}$

証明

- $a \equiv b \pmod{n}$ かつ $c \equiv d \pmod{n}$ とする．ある整数 s, t が存在して $a - b = sn$ かつ $c - d = tn$.

  (1) $(a + c) - (b + d) = (s + t)n$ なので定義より $a + c \equiv b + d \pmod{n}$.

  (2) $(a - c) - (b - d) = (s - t)n$ なので定義より $a - c \equiv b - d \pmod{n}$.

  (3) $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d) = snc + btn = (sc + bt)n$ なので定義より $ac \equiv bd \pmod{n}$.

  (4) k に関する帰納法で示す．$k = 0$ のときは $a^k = b^k$ なので明らか．$k > 0$ とする．帰納法の仮定より $a^{k-1} \equiv b^{k-1} \pmod{n}$．よって，(3) より $aa^{k-1} \equiv bb^{k-1} \pmod{n}$，すなわち，$a^k \equiv b^k \pmod{n}$.

- $c \neq 0$ とし，$(c, n) = d$ とする．

  (5) $ca \equiv cb \pmod{n}$ とする．定義より，ある整数 t が存在して $ca - cb = tn$．また，d は c, n の最大公約数なので，ある整数 c', n' が存在して $(c', n') = 1$ かつ $c = c'd, n = n'd$．ここで，$c|(ca - cb)$ より $c|tn$．$c \neq 0$ より $d \neq 0$．よって $c'|tn'$ となり，$c'|t$ となるので，$\frac{t}{c'} \in \mathbb{Z}$．以上より $a - b = \frac{ca-cb}{c} = \frac{tn}{c} = \frac{t}{c'}\frac{n}{d}$ となり $a \equiv b \pmod{\frac{n}{d}}$ を得る．　□

例 7.5 以下の合同式が成立.

(1) $365a + b \equiv a + b \pmod{7}$

(2) $10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}$

(3) $1000^n a_n + 1000^{n-1} a_{n-1} + \cdots + 1000a_1 + a_0 \equiv a_0 + (-1)^1 a_1 + \cdots + (-1)^n a_n \pmod{7}$

これらの合同式は結構有用である．個別に見ていこう.

(1) この式は曜日の計算に便利．例えば，2003 年 12 月 4 日が木曜日である事を知っているとき，2005 年 12 月 4 日が何曜日かを簡単に調べることができる．2004 年度はうるう年であることを考えて，

$$365 \times 2 + 1 \equiv 2 + 1 \equiv 3 \pmod 7$$

よって，2005 年 12 月 4 日が日曜日であることが分かる (木曜日の 3 日後は日曜日)．

(2) この式は，与えられた整数が 9 の倍数であるかどうかの判定に便利．実際，整数 123456789 が与えられた場合

$$123456789 \equiv 1 + 2 + \cdots + 9 \equiv 45 \equiv 4 + 5 \equiv 0 \pmod 9$$

となるので，123456789 が 9 の倍数であることが分かる．

(3) この式は，与えられた整数が 7 の倍数であるかどうかの判定に便利．実際，整数 123456789 が与えられた場合

$$123456789 \equiv 789 - 456 + 123 \equiv 456 \pmod 7$$

となる．$456 \bmod 7 = 1$ を計算することにより，123456789 は 7 の倍数ではなく，7 で割ると 1 余る事が分かる．

一応，最後に証明も記しておこう．

(1) $365 - 1 = 364 = 7 \times 52$ なので $365 \equiv 1 \pmod 7$．定理 7.4(1)(3) より $365a + b \equiv a + b \pmod 7$．

(2) $10 \equiv 1 \pmod 9$ なので，各 $i = 1, 2, \ldots, n$ に対し，定理 7.4(4) より $10^i \equiv 1 \pmod 9$ となり，定理 7.4(3) より $10^i a_i \equiv a_i \pmod 9$ となる．よって， 定理 7.4(1) を繰り返し用いることにより求める合同式を得る．

(3) $1001 = 7 \times 11 \times 13$ であるので $1000 \equiv -1 \pmod 7$．各 $i = 1, 2, \ldots, n$ に対し，定理 7.4(4) より $1000^i \equiv (-1)^i \pmod 7$ となり，定理 7.4(3) より $1000^i a_i \equiv (-1)^i a_i \pmod 7$ となる．よって， 定理 7.4(1) を繰り返し用いることにより求める合同式を得る．□

7.2 1 次合同方程式

本節は，教科書 3.3 節の中程 (pp.131–134) に対応する．

定義 7.6 未知数を含む合同式を**合同方程式** (congruence equation) と呼ぶ．合同方程式を**解く** (solve) とは合同方程式を成立させる未知数の値を求めることである (通常は合同式を用いて表現する)． □

例 7.7 合同方程式 $5x \equiv 1 \pmod 4$ を解くと $x \equiv 1 \pmod 4$ を得る． □

定理 7.8 $(a, m) = 1$ ならば合同方程式 $ax \equiv b \pmod{m}$ は m を法として只一つの解を持つ.

証明 $(a, m) = 1$ と定理 4.10 より，ある整数 x', y' が存在して $ax' + my' = 1$.

(解の存在) 最初に解が存在することを示す．$ax' \equiv 1 - my' \equiv 1 \pmod{m}$．定理 7.4(3) より $a(bx') \equiv b \pmod{m}$．よって，合同方程式 $ax \equiv b \pmod{m}$ は解として $x = bx'$ を持つ.

(解の一意性) 次に解の一意性を示す．x_1, x_2 を二つの解とする，すなわち $ax_1 \equiv b \pmod{m}$ かつ $ax_2 \equiv b \pmod{m}$．よって，$ax_1 \equiv ax_2 \pmod{m}$．定理 7.4(5) と $(a, m) = 1$ より $x_1 \equiv x_2 \pmod{m}$. □

上記の証明より直ちに次のアルゴリズムを得る.

アルゴリズム 7.9

入力: $(a, m) = 1$ となる整数 a, b, m
出力: 合同方程式 $ax \equiv b \pmod{m}$ の一般解

(1) 拡張ユークリッドの互除法を用いて $au + mv = 1$ となる整数 u を求める.
(2) $x \equiv bu \pmod{m}$ を出力 (bu の代りに $bu \bmod m$ を用いた方が綺麗かも). □

定義 7.10 同一の未知数によって構成される合同方程式のリストを**連立合同方程式** (simultaneous congruence equations) と呼ぶ．連立合同方程式を**解く** (solve) とは全ての合同方程式を同時に成立させる未知数の値を求めることである (通常は合同式を用いて表現する). □

例 7.11 連立合同方程式

$$\begin{cases} x & \equiv & 1 & \pmod{2} \\ x & \equiv & 0 & \pmod{3} \end{cases}$$

を解くと $x \equiv 3 \pmod{6}$ を得る. □

定理 7.12 (中国人の剰余定理 (Chinese remainder theorem))
次の連立合同方程式を考える.

$$\begin{cases} a_1 x & \equiv & b_1 & \pmod{m_1} \\ & \vdots & & \vdots \\ a_k x & \equiv & b_k & \pmod{m_k} \end{cases}$$

また，以下の条件が全て満たされるとする.

(1) 全ての i で $(a_i, m_i) = 1$
(2) 全ての相異なる i と j について $(m_i, m_j) = 1$

このとき，この連立合同方程式は解を持ち，その一般解は次のように表される．

$$x \equiv c \pmod{m_1 m_2 \cdots m_k}$$

すなわち，この連立合同方程式は $m_1 \cdots m_k$ を法として只一つの解を持つ．

証明 $M = m_1 m_2 \cdots m_k$ とする．

(解の存在) 解が存在することを示す．各 i で $M_i = \frac{M}{m_i}$ とする．条件 (2) より $(m_i, M_i) = 1$．よって条件 (1) を考えて $(m_i, a_i M_i) = 1$．ここで，合同方程式

$$a_i M_i x_i \equiv 1 \pmod{m_i}$$

を考えると，$(m_i, a_i M_i) = 1$ なので定理 7.8 よりこの方程式は解を持つ．この解の一つを c_i とする．整数 c を

$$c = M_1 c_1 b_1 + M_2 c_2 b_2 + \cdots + M_k c_k b_k$$

で定める．この時，c は連立合同方程式の解となる．実際，全ての i で，条件 (2) より全ての i と異る j に対し $m_i \mid M_j$ であることを考えると，以下のように c は $a_i x \equiv b_i \pmod{m_i}$ の解となっている．

$$\begin{aligned} a_i c &\equiv a_i(M_1 c_1 b_1 + M_2 c_2 b_2 + \cdots + M_k c_k b_k) \pmod{m_i} \\ &\equiv a_i M_i c_i b_i \pmod{m_i} \\ &\equiv b_i \pmod{m_i} \end{aligned}$$

(一般解) 解が少なくとも一つ存在することはすでに示した．解の 1 つを c とする．このとき $x \equiv c \pmod{M}$ が一般解を与えることを示す．

最初に，$x \equiv c \pmod{M}$ が解を与えること，すなわち，任意の整数 t に対し $c + tM$ も解となることを示す．これは，各 i で，$a_i(c + tM) \equiv a_i c \equiv b_i \pmod{m_i}$ となることから示せる．

次に，M を法とした解の一意性を示す．c' を c と異る連立合同方程式の解とする．このとき，各 i で $a_i c \equiv b_i \pmod{m_i}$ かつ $a_i c' \equiv b_i \pmod{m_i}$．辺々引くと $a_i(c - c') \equiv 0 \pmod{m_i}$．$(a_i, m_i) = 1$ なので定理 7.4(5) より $c - c' \equiv 0 \pmod{m_i}$．すなわち，$m_i \mid c - c'$．よって，$M \mid c - c'$ となるので，$c \equiv c' \pmod{M}$．

以上より，$x \equiv c \pmod{M}$ は一般解を与える． □

上記の証明より直ちに次のアルゴリズムを得る．

アルゴリズム 7.13 定理 7.12 で取り扱った連立合同方程式を考える．また，定理 7.12 の条件 (1),(2) も成立するとする．このとき，この連立合同方程式の一般解は次のように計算できる．

(1) $M = m_1 m_2 \cdots m_k$ と $M_i = \frac{M}{m_i}$ $(i = 1, 2, \ldots, k)$ を計算．
(2) 各 i に対し，合同方程式 $a_i M_i x_i \equiv 1 \pmod{m_i}$ の特殊解 c_i を アルゴリズム 7.9 を用いて求める．
(3) $c = M_1 c_1 b_1 + M_2 c_2 b_2 + \cdots + M_k c_k b_k$ を計算．
(4) $x \equiv c \pmod{M}$ を出力 (c の代りに $c \bmod M$ を用いた方が綺麗かも)． □

NOTE: 中国人の剰余定理が何故そう呼ぶれるかというと，中国の古い数学書『孫子算経』に以下の問題とその解法が記述されていたことに由来する．

今有物不知其数	今，ここに物が有るが其の数を知らない
三三数之剰二	其の数を 3 つずつ数えれば 2 余り
五五数之剰三	其の数を 5 つずつ数えれば 3 余り
七七数之剰二	其の数を 7 つずつ数えれば 2 余る
問物幾何	ここに物は何個あるか？

なお，この問題は『百五減算』と言う名前でも知られている．では何故 “百五” なのであろうか？それはこの問題を解いてみれば自ずと分かるであろう (演習課題に加えておく)．

NOTE: 『孫子算経』は紀元 3–5 世紀頃に中国 (西晋-東晋？) で成立したとされている．著者は明らかではない．日本には遣唐使によって伝えられた．なお，養老 2 年 (西暦 718 年) に制定された養老律令 (大宝律令 (大宝 1 年, 西暦 701 年) の改訂版) において，大学寮 (官吏養成の為の教育機関) には算博士 2 人と算生 30 人を置く事と定めてあり，その教科書の一つとして孫子算経は採用されている．

演習課題

問 7.1 $7x \equiv 5 \pmod{13}$ を解け．

問 7.2 『百五減算』を連立合同方程式の概念を用いて定式化し，さらにその解答を与えよ．

問 7.3 例 7.5 を参考にして，与えられた整数が 11 の倍数であるかどうかを簡単に判定する方法を考案せよ．また，考案した方法で 1234321 が 11 の倍数であるかどうかを判定せよ．