第 5 章　整数の合同

5.1　合同式

定義 5.1 $a, b, m \in \boldsymbol{Z}$ に対して，$a - b \in m\boldsymbol{Z}$ （すなわち $m|(a-b)$）であるとき，

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

と書き，a, b **は** m **を法として合同である**という． そうでないときは，$a \not\equiv b \pmod{m}$ と書く． このような式を一般に**合同式**という．

まず，$m \neq 0$ のとき，整数 a を m で割った余りを r とすると，$a \equiv r \pmod{m}$ が成り立つ． 実際，商を q とすれば

$$a = qm + r, \quad 0 \leq r < m$$

より $a - r = qm$ は m の倍数である． このことを使えば，

$$a \equiv b \pmod{m} \iff a, b \text{ それぞれを } m \text{ で割った余りは等しい}$$

と書き換えることができる． とくに，

$$a \equiv 0 \pmod{m} \iff m|a.$$

$m = 2$ ならば，任意の整数 a について，

$$a \equiv 0 \pmod{2}, \qquad a \equiv 1 \pmod{2}$$

のどちらか一方が成り立ち，それぞれ a が偶数，奇数であることを表している．
また，整数 $p > 1$ が素数であることは

$$1 < d < p \text{ である任意の } d \in \boldsymbol{Z} \text{ に対して } p \not\equiv 0 \pmod{d}$$

によって定義され，さらにその必要十分条件が

$$ab \equiv 0 \pmod{p} \text{ ならば，} \quad a \equiv 0 \pmod{p} \text{ または } b \equiv 0 \pmod{p}$$

であることを命題 4.2 は主張していることになる． このように，前出の定義や定理，証明などを合同式を用いて書き換えることは良い学習になる．

2013 年度「代数入門」講義資料（2013 年 10 月）ver.1031

さて，合同式の最も基本的な性質は，

- $a \equiv a \pmod{m}$,
- $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$,
- $a \equiv b,\ b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$

であるが，どれも定義から直ちにわかってしまうことである．これらは，合同式で表される関係が "同値関係" であることを示している．このことはいずれまた…….

次に，和，差，積と合同式の関係（割り算については次節で扱う）についての性質をまとめておく．

命題 5.2　$a,b,c,d,m \in \boldsymbol{Z}$ が $a \equiv b,\ c \equiv d \pmod{m}$ をみたすならば，

$$a+c \equiv b+d \pmod{m}, \quad a-c \equiv b-d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

がそれぞれ成り立つ．

証明　ええっと，まず $a = b+mx$, $c = d+my$ $(x,y \in \boldsymbol{Z})$ と書けることを確認してから，これらを足したり引いたり掛けたりという方針で…，あとは演習！ □

次の命題は，どんな場合に法が変化するかを示している．この証明も演習とする．

命題 5.3　$a,b,l,m,n \in \boldsymbol{Z}$ に対して次の (1), (2) が成り立つ．

(1) $m|n$ のとき，$a \equiv b \pmod{n}$ ならば $a \equiv b \pmod{m}$.

(2) $l \neq 0$ のとき，$a \equiv b \pmod{m} \Longleftrightarrow al \equiv bl \pmod{ml}$.

(1) の逆は成り立たないことに注意せよ．たとえば，$7 \equiv 1 \pmod{3}$ であるが $7 \not\equiv 1 \pmod{9}$ である．また，(2) と

$$\text{(誤)} \qquad l \neq 0 \text{ のとき，} \quad a \equiv b \pmod{m} \Longleftrightarrow al \equiv bl \pmod{m}$$

との違いに注意せよ．確かに "$\Longrightarrow$" は正しいのだが，逆は一般に正しくない．たとえば，$45 \equiv 15 \pmod{10}$ だが，両辺を 5 で割って $9 \equiv 3 \pmod{10}$ とはできない．一方，両辺を 3 で割れば，$15 \equiv 5 \pmod{10}$ という正しい合同式を得る．このように，割る数によっては正しい合同式が導かれることもある．どのような数で割ることができるかは，次節で詳しく述べる．

この節を終える前に，合同式の "極端" な場合の例をあげておく．

- $m = 1$ のとき，どんな $a,b \in \boldsymbol{Z}$ に対しても $a \equiv b \pmod{1}$ である．
- $m = 0$ のとき，"$x \in 0\boldsymbol{Z} \Leftrightarrow x = 0$" に注意すれば，$a \equiv b \pmod{0} \Leftrightarrow a = b$.
- $-m\boldsymbol{Z} = m\boldsymbol{Z}$ より，$a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{|m|}$.

したがって，ふつう m としては 2 以上の自然数を想定すればよい．

5.2　法に関する逆元

前節の命題 5.2 で見たように合同式と加減乗算の関係はカンタンであったが，割り算については状況が少し複雑である（命題 5.3 の直後の説明参照）．

定義 5.4　$a, m \in \boldsymbol{Z}$ に対して，$ax \equiv 1 \pmod{m}$ をみたす $x \in \boldsymbol{Z}$ が存在するとき，a は**法 m に関して可逆**であるといい，x を**法 m に関する a の逆元**という．

逆元はいつも存在するわけではないが，もし存在するならば m を法として一意的に定まる．すなわち，x, x' がともに a の法 m に関する逆元ならば，$x \equiv x' \pmod{m}$ が成り立つ．実際，$ax \equiv ax' \equiv 1 \pmod{m}$ から

$$x \equiv x \cdot 1 \equiv x(ax') \equiv (ax)x' \equiv 1 \cdot x' \equiv x' \pmod{m}$$

が得られる．

例 5.5 (1)　$7 \cdot 2 = 14 \equiv 1 \pmod{13}$ より，7 は 13 を法として可逆であり，逆元として 2 がとれる．一方，$7 \cdot 8 = 56 \equiv 1 \pmod{11}$ なので，8 は法 11 に関する 7 の逆元である．
(2)　14 未満のすべての自然数 x に対して $7x \equiv 0$ または $7 \pmod{14}$ が確かめられ，したがって 7 は法 14 に関して可逆ではない．

整数 a, b の最大公約数が 1 のとき，a, b は**互いに素**であるという．次の命題は，法 m と互いに素な整数による割り算が可能なことを示している．

命題 5.6 互いに素な整数 a, m について次が成り立つ．

(1)　a は法 m に関して可逆である．

(2)　$b, c \in \boldsymbol{Z}$ が $ab \equiv ac \pmod{m}$ をみたすならば，$b \equiv c \pmod{m}$ が成り立つ．

証明　(1)　$\gcd(a, m) = 1$ より $ax + my = 1$ $(x, y \in \boldsymbol{Z})$ と書けるが，これより $ax - 1 = -my$ は m の倍数，すなわち $ax \equiv 1 \pmod{m}$ であるから a は可逆である．
(2)　$ab \equiv ac \pmod{m}$ の両辺に，a の法 m に関する逆元 x を掛ければよい．　□

さて，a が法 m に関して可逆ならば，逆元 x を用いて $ax = 1 + my$ $(y \in \boldsymbol{Z})$ と書けるが，このことは定理 3.2 より $\gcd(a, m) = 1$ を意味する．上の命題とあわせれば，法 m に関する a の逆元が存在するためには，a, m が互いに素であることが必要十分であることがわかる．式で書けば，

$$\gcd(a, m) = 1 \quad \Longleftrightarrow \quad ax \equiv 1 \pmod{m} \text{ をみたす } x \in \boldsymbol{Z} \text{ が存在する．}$$

とくに，p が素数のときは，$a \not\equiv 0 \pmod{p}$ である任意の整数 a に対して，法 p に関する逆元が存在する．

一般に，a, m が互いに素のとき，ax に $x = 1, 2, \cdots$ を順々に代入していって m で割った余りが 1 になるものを探すことで a の法 m に関する逆元が求まる．しかし，大きな m に対しては，この方法は効率が悪い．そこで，ユークリッドの互除法を用いる．第 2 章の最後で計算したように，ユークリッドの互除法から $ax + my = 1$ をみたす整数 x, y が求まり，上の証明からもわかるように，このときの x が a の法 m に関する逆元になるわけである．

例 5.7 (1)　法 2013 に関する 1031 の逆元を求めてみよう．そのために，$1031x$ に $x = 2, 3, \cdots$ を順に代入して 2013 で割り算して余りを求めていくと，いつまで経っても余り 1 が現れず，お腹は空くし恋人も逃げる．そこで，2013, 1031 に対してユークリッドの互除法を適用すると

$$2013 = 1 \cdot 1031 + 982, \quad 1031 = 1 \cdot 982 + 49, \quad 982 = 20 \cdot 49 + 2, \quad 49 = 24 \cdot 2 + 1$$

であり，これらから $986 \cdot 1031 - 505 \cdot 2013 = 1$ と計算される．よって，法 2013 に関する 1031 の逆元として 986 が求まり恋人にも尊敬される．
(2)　一方，法 2013 に関する 1101 の逆元を求めようとすると，これらはともに 3 の倍数であって互いに素ではないから，逆元は存在せず，恋人に軽蔑されるのがオチ．

定義 5.8　$a, m \in \boldsymbol{Z}$（ただし $|m| \geq 2$）とする．$az \equiv 0 \pmod{m}$ かつ $z \not\equiv 0 \pmod{m}$ をみたす $z \in \boldsymbol{Z}$ が存在するとき，a は**法** m **に関する零因子**であるという．

たとえば，$2 \cdot 3 \equiv 0 \pmod{6}$，$2, 3 \not\equiv 0 \pmod{6}$ なので，2 と 3 はどちらも法 6 に関する零因子である．なお，0 はどんな法 $m \geq 2$ に対しても零因子であることに注意せよ（だって $0 \cdot 1 = 0,\ 1 \not\equiv 0 \pmod{m}$ だもん）．

定理 5.9　$a, m \in \boldsymbol{Z}$ $(m \geq 2)$ に対して次は同値である．

(i) a, m は互いに素である．
(ii) a は法 m に関して可逆である．
(iii) a は法 m に関する零因子ではない．

証明　<u>(i) ⇒ (ii):</u> すでに命題 5.6 で示されている．
<u>(ii) ⇒ (iii):</u> 整数 x を法 m に関する a の逆元とする．いま，a が零因子であるとすると，$az \equiv 0,\ z \not\equiv 0 \pmod{m}$ をみたす整数 z がとれるが，

$$z \equiv 1 \cdot z \equiv (ax)z \equiv x(az) \equiv x \cdot 0 \equiv 0 \pmod{m}$$

となって矛盾する．よって a は零因子ではない．
<u>(iii) ⇒ (i):</u> $d = \gcd(a, m)$ とおき，対偶を示すために $d > 1$ と仮定する．$a = a'd,\ m = m'd$ とすれば，$d > 1$ より $m' \not\equiv 0 \pmod{m}$．一方，$am' = a'm \equiv 0 \pmod{m}$ だから，a は法 m に関する零因子である．□