# 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，$a$ **は** $m$ **を法として** $b$ **と合同である**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**といい，$m$ をその合同式の**法**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，$a \equiv r \pmod{m}$ が成り立つことに注意しよう． 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，$m \neq 0$ のとき

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

と書き換えることができる． とくに，

$$a \equiv 0 \pmod{m} \quad \Longleftrightarrow \quad m|a.$$

次に，“極端” な場合，つまり $m = 0, 1$ のときを考える．

- $m = 1$ 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,「$a \equiv b \pmod{0} \Leftrightarrow a - b \in 0\boldsymbol{Z} \Leftrightarrow a - b = 0 \Leftrightarrow a = b$」.

これらは例外的に扱われることが多い． また，$-m\boldsymbol{Z} = m\boldsymbol{Z}$ 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．

$m = 2$ 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，さらに命題 4.2 は，$p>1$ が素数であるための必要十分条件が

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

であることを主張している． 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．

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 (はずである (と思う (と信じたい)))． 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（Wikipedia で調べてみ……）．

次に，和，差，積（足し算，引き算，掛け算）と合同式の関係についての性質をまとめておく（商，つまり割り算については次節で扱う）．

**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，まず仮定から $a=b+mx,\ c=d+my$ $(x,y\in\boldsymbol{Z})$ と書けるから，これらを足したり引いたり掛けたりという方針で…，あとは任せた！ □

次の命題は，どんな場合に法が変化するかを示している． この証明もやってみて．

**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，$3|9$ だけど，$7\equiv 1 \pmod{3}$ かつ $7\not\equiv 1 \pmod{9}$ 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が，一般には正しくない． 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．

## 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．

**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．“$m$ を法として一意的” とは，$x$ と $x'$ がともに $a$ の法 $m$ に関する逆元ならば，$x \equiv x' \pmod{m}$ が成り立つことを意味する．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 $7 \pmod{14}$ であることを確かめよ．このことから，7 は法 14 に関して可逆ではないことがわかる．

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 $ax + my = 1$ をみたす $x, y \in \boldsymbol{Z}$ がとれるが，これより $ax \equiv 1 \pmod{m}$ 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 3.3 より $\gcd(a, m) = 1$ を意味する．上の命題とあわせれば，$a$ が法 $m$ に関して可逆であるためには，$a, m$ 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，

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

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，$\gcd(a, m) = 1$ 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 $m$ に関する逆元のひとつが求まる．実際に，

計算苦手な私でも $m < 20$ くらいならばこの方法は実用的である（若い皆さんなら計算力もあるから $m < 100$ くらいまで大丈夫？）．しかし，大きな $m$ に対しては効率が悪い．命題 5.6 の証明をみると，$ax + my = 1$ $(x, y \in \boldsymbol{Z})$ のとき，$x$ が $a$ の法 $m$ に関する逆元になっているので，ユークリッドの互除法を用いて $x, y$ を求めれば効率よく計算できる．

**例 5.7** (1) 法 2019 に関する 1963 の逆元を求めてみよう．そのために，$1963x$ に $x = 2, 3, \cdots$ を順に代入して 2019 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 が現れない．そこで，$2018, 1963$ に対してユークリッドの互除法を適用すると，

$$2019 = 1 \cdot 1963 + 56, \quad 1963 = 35 \cdot 56 + 3, \quad 56 = 18 \cdot 3 + 2, \quad 3 = 1 \cdot 2 + 1$$

であり，これらから

$$-666 \cdot 2019 + 685 \cdot 1963 = 1$$

と計算され（ホントかな？），法 2019 に関する 1963 の逆元として 685 が求まる．
(2) 一方，法 2015 に関する 1963 の逆元を求めようとして，ユークリッドの互除法を適用すると，最大公約数は 13 となって互いに素ではないから逆元は存在せず，なんだかなあ〜という気分になるので，逆元を求めるときは注意が必要である．

**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，$4 \cdot 3 \equiv 0 \pmod{6}$，$4 \not\equiv 0 \pmod{6}$，$3 \not\equiv 0 \pmod{6}$ なので，4 と 3 はどちらも法 6 に関する零因子である．なお，どんな法 $m \geq 2$ に対しても，0 は法 $m$ に関する零因子であることに注意せよ（理由を考えてごらん）．

**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** (i) ⇒ (ii): すでに命題 5.6 で示されている．
(ii) ⇒ (iii): 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，

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

となって矛盾する．よって $a$ は零因子ではない．
(iii) ⇒ (i): $d = \gcd(a, m)$ とおき，$a = a'd,\ m = m'd$ のように整数 $a', m'$ をとっておく．いま $d > 1$ と仮定すると，$m' \not\equiv 0 \pmod{m}$．一方，

$$am' = (a'd)m' = a'(m'd) = a'm \equiv 0 \pmod{m}$$

だから，$a$ は法 $m$ に関する零因子となって矛盾．したがって $d = 1$．　□