第5章　整数の合同

5.1　合同式

偶数と偶数を加えると偶数になり，偶数と奇数を加えると奇数になる．加法だけでなく減法や乗法についても，こういった性質を書き下すことができる．

$$\text{偶} \pm \text{偶} = \text{偶}, \qquad \text{偶} \pm \text{奇} = \text{奇}, \qquad \text{奇} \pm \text{奇} = \text{偶}$$
$$\text{偶} \times \text{偶} = \text{偶}, \qquad \text{偶} \times \text{奇} = \text{偶}, \qquad \text{奇} \times \text{奇} = \text{奇}$$

偶数とは 2 の倍数のことであるが，今度は 3 の倍数についても同様のことを考えてみる．奇数は “偶数でない” と一言で特徴づけられるが，3 の倍数でない数は 2 種類に分けられることに注意する．すなわち，3 で割って 1 余る数と 2 余る数である．これらをそれぞれ R_1, R_2 と書くことにする（ここだけの記法！）．ついでに 3 の倍数は余りが 0 の数だから R_0 と書こう（つまり $R_0 = 3\boldsymbol{Z}$）．このとき，たとえば “3 で割って 1 余る数ふたつを加えると余りが 2 の数になる” ことは，$R_1 + R_1 = R_2$ と表すことができるであろう．このようにして R_0, R_1, R_2 の間の和，積の性質が次の表のように書ける．

$+$	R_0	R_1	R_2
R_0	R_0	R_1	R_2
R_1	R_1	R_2	R_0
R_2	R_2	R_0	R_1

$\times$	R_0	R_1	R_2
R_0	R_0	R_0	R_0
R_1	R_0	R_1	R_2
R_2	R_0	R_2	R_1

差についても作表できるのだが，順序の説明が面倒なので省略する（各自作ってみよ）．上で，3 で割って 1 余る数を R_1 と書くなどと説明したが，実際には，そのような整数全体の集合が R_1 だと考えるべきである．すなわち，各 $j = 0, 1, 2$ について

$$R_j = \left\{ n \in \boldsymbol{Z} \;\middle|\; n \text{ を } 3 \text{ で割った余りは } j \right\}$$

であって，上の表はこれらの間に和と積を “自然に定義” したものとみなす．たとえば，$R_1 + R_2 = R_0$ の意味は，$x \in R_1, y \in R_2$ ならばいつでも $x + y \in R_0$ となっていることをさすわけである．この “いつでも” というのが大切である．つまり，j の組合せだけで性質が決まり，それぞれの R_j の元 x, y の選び方によらない，同じ R_j に属している 2 つの整数は同じ性質をもつことが大切なのである．ところで，$a, b \in R_j$ $(j = 0, 1, 2)$ ならば $a - b$ は 3 の倍数であり，逆に $a - b \in 3\boldsymbol{Z}$ ならば a, b は同じ R_j に属している．以上をふまえて次の定義から始めよう．

定義 5.1 $a, b, m \in \boldsymbol{Z}$ に対して，$a - b \in m\boldsymbol{Z}$ （すなわち $m \mid (a-b)$）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，$a \equiv r \pmod{m}$ が成り立つことに注意する（どしてかな？）．したがって，

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

とくに，

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

この章のはじめに述べたことは，3 を法とする合同式で表現することができる．すなわち

$$R_j = \left\{ n \in \boldsymbol{Z} \;\middle|\; n \equiv j \pmod{3} \right\} \qquad (j = 0, 1, 2)$$

であり，たとえば，性質 $x \in R_1, y \in R_2$ ならばいつでも $x + y \in R_0$ は，

$$x \equiv 1 \pmod{3}, \quad y \equiv 2 \pmod{3} \text{ ならば } x + y \equiv 0 \pmod{3}$$

と書き表すことができる．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．

以下に，合同式の基本的な性質をまとめておく．初めの命題は，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，後の命題は，どんな場合に法が変化するかが述べられている．どの証明も定義からすぐに導かれるので演習とする．

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．

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

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

(2) $d \neq 0$ のとき，$a \equiv b \pmod{m} \Longleftrightarrow ad \equiv bd \pmod{md}$.

(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（このような例をたくさん考えてみよう）．

この節を終える前に，合同式の “極端” な例をあげておく．

- $m = 1$ 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．

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． □

とくに，素数 p に対して $p \mid a$ でない整数 a はすべて法 p に関して可逆である．

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 法 2012 に関する 1113 の逆元を求めてみよう．そのために，$1113x$ に $x = 2, 3, \cdots$ を順に代入して 2012 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，$2012, 1113$ に対してユークリッドの互除法を適用すると

$$2012 = 1 \cdot 1113 + 899, \quad 1113 = 1 \cdot 899 + 214, \quad 899 = 4 \cdot 214 + 43,$$
$$214 = 4 \cdot 43 + 42, \qquad 43 = 1 \cdot 42 + 1$$

であり，これらから $-47 \cdot 1113 + 26 \cdot 2012 = 1$ と計算される．よって，法 2012 に関する 1113 の逆元として -47 が求まり恋人にも尊敬される．さらに $-47 \equiv 2012 - 47 \equiv 1965 \pmod{2012}$ なので，1965 も逆元だよねとそっと囁けば，恋人との絆はさらに深まる（はず）．

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 はいつで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　(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，

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

となって矛盾する．よって a は零因子ではない．
(iii) ⇒ (i): 対偶を示すために，$\gcd(a, b) = d > 1$ 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．　□