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しよう．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（各自考えてみよ）．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，差の表を作ってみればすぐにわかるが，$a, b \in R_j$ $(j = 0, 1, 2)$ 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 に属することがいえる．

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．このような式を一般に**合同式**という．

以下において合同式の性質を列挙するが，その前に “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．

合同式の最も基本的な性質は，

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

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…….

いま，$m \neq 0$ 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（どして？）．したがって，

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

と書き換えることができる．とくに，

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

次に和，差，積と合同式の関係を述べよう（割り算については次節で扱う）．

命題 5.2 $a, b, c, m \in \boldsymbol{Z}$ 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！　□

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．たとえば

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

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

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

と書き直すことができる． 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．

次の命題は，どんな場合に法が変化するかを示している． 証明は演習とする．

命題 5.3 (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，$a \equiv b \pmod m \iff ad \equiv bd \pmod{md}$.

(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）．

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．

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 5.4 互いに素な整数 a, m について次が成り立つ．
(1) $ax \equiv 1 \pmod m$ をみたす $x \in \boldsymbol{Z}$ が存在する．
(2) $b, c \in \boldsymbol{Z}$ に対して，$ab \equiv ac \pmod m$ ならば $b \equiv c \pmod m$.

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 $ax \equiv 1 \pmod m$.
(2) $ab \equiv ac \pmod m$ の両辺に (1) の x を掛ければよい. □

上の命題の (1) をみたす整数 x を，**法 m に関する a の逆元**という． 逆元は一意的に定まるわけではないが，x, x' がともに a の法 m に関する逆元ならば，$x \equiv x' \pmod m$ が確かめられる（各自確かめよ）． つまり，**法 m に関する逆元は（もし存在するならば）一意的に定まる**.

例 5.5 (1)　$7 \cdot 2 = 14 \equiv 1 \pmod{13}$ より，2 は法 13 に関する 7 の逆元である．一方，$7 \cdot 8 = 56 \equiv 1 \pmod{11}$ なので，法 11 に関する 7 の逆元として 8 がとれる．
(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 に関する逆元をもたない．

上の命題は，整数 a, m が互いに素ならば，法 m に関する a の逆元が存在することを示している．逆に，法 m に関する a の逆元 x が存在すれば $ax = 1 + my$ $(y \in \boldsymbol{Z})$ 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．すなわち，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．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．

以下，$|m| \neq 1$ 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 5.6 $a, m \in \boldsymbol{Z}$ $(|m| \neq 1)$ に対して次は同値である．

(i) a, m は互いに素である．

(ii) 法 m に関する a の逆元が存在する．

(iii) a は法 m に関する零因子ではない．

証明　(i) と (ii) が同値であることは上で示されているので，以下，(ii) と (iii) の同値性を示す．
(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) ⇒ (ii): すべての整数は 0 以上 $|m|$ 未満のある整数と m を法として合同だから，$a^k \equiv a^l \pmod{m}$ をみたす自然数 $k < l$ の組が存在する．このとき，

$$a^k(a^{l-k} - 1) \equiv 0 \pmod{m}$$

であるが，仮定より a は法 m に関する零因子でないから，$a^{l-k} - 1 \equiv 0 \pmod{m}$ でなければならない．したがって，$a^{l-k} \equiv 1 \pmod{m}$ であり，法 m に関する a の逆元として整数 a^{l-k-1} がとれることがわかる．　□