2　整数と剰余類

2.1　整数

群の剰余類の一つの応用として，整数に関する，重要な定理を証明する。その前に，整数に関するいくつかの定義を行う。

定義 2.1　(1) a を 0 ではない整数とする。$a = km$ となる整数 k と m が存在する時，k と m は a の**約数** (*divisor*) であると言い，$k|a$, $m|a$ と書く。

またこの時，a は k や m の**倍数** (*multiple*) であると言う。

k, m は 1 や a 自身でも良い。$a \neq 0$ なので，0 が約数となることはない。

(2) a, b を 0 ではない整数とする。ある整数 k があって，$k|a$, $k|b$ となる時，k を a と b の**公約数** (*common divisor*) という。

(3) a, b を 0 ではない整数とする。k が a と b の公約数なら，$-k$ も公約数である。a と b の公約数の中で，最大のものを**最大公約数** (*GCD: Greatest Common Divisor*) と言い，(a, b) という記号で表す。1 は必ず公約数となるので，$(a, b) \geqq 1$ である。

(4) a, b を 0 ではない整数とする。$(a, b) = 1$ となる時，a と b は**互いに素** (*relatively prime*) であると言う。

(5) a, b を 0 ではない整数とする。ある整数 m があって，$a|m$, $b|m$ となる時，m を a と b の**公倍数** (*common multipul*) という。

m が a と b の公倍数なら，$-m$ も公倍数である。kab という形の整数は全て公倍数となるが，公倍数がこのような形になるとは限らない。正の公倍数の中で最小のものを，a と b の**最小公倍数**)(*LCM: Least Common Multiple*) と言う。

(6) 自分自身と 1 以外に約数を持たない自然数を**素数** (*prime number*) という。素数ではない自然数を**合成数** (*composite number*) という。

定理 2.2　$p_1, \cdots, p_n$ を 1 と 0 ではない整数とし，1 以外の共通の約数を持たないとする。すなわち，ある 0, 1 ではない整数 d で $d|p_1, \cdots, d|p_n$ となるようなものは存在しないとする。

この時，ある整数 $k_1, \cdots, k_n$ が存在して，

$$k_1 p_1 + \cdots + k_n p_n = 1$$

となる。

証明

$$H = \{\ m_1 p_1 + \cdots + m_n p_n \mid m_i \in \mathbb{Z}\ (i = 1, \cdots, n)\ \}$$

とおく。すなわち，これは $p_1, \cdots, p_n$ の整数倍の和を全て集めたもので，$\mathbb{Z}$ の部分群になる。

定理 1.35 より，この H は巡回群であるので，ある正の整数 m があって，$H = m\mathbb{Z}$ となっている。

これは，H の全ての元は m の整数倍になるということを意味している。すなわち，$p_1, \cdots, p_n$ は全て m の整数倍となる。仮定より，$p_1, \cdots, p_n$ は 1 以外の共通の約数を持たないので，$m = 1$ でなければならない。

$H = \mathbb{Z}$ となるので，$1 \in H$ である。すなわち，$k_1p_1 + \cdots + k_np_n = 1$ となるような整数 $k_1, \cdots, k_n$ が存在する。 ∎

この定理は，特に $n = 2$ の場合が，良く使われる。

定理 2.3 p_1, p_2 を互いに素な２つの整数とすると，

$$k_1p_1 + k_2p_2 = 1$$

を満たす整数 k_1, k_2 が存在する。

注意： $k_1p_1 + k_2p_2 = 1$ を満たす整数 k_1, k_2 は，一意的に決まるわけではない。例えば，m を任意の整数とした時，

$$1 = k_1p_1 + k_2p_2 = k_1p_1 + k_2p_2 + mp_1p_2 - mp_1p_2 = (k_1 + mp_2)p_1 + (k_2 - mp_1)p_2$$

である。すなわち，

$$k_1' = k_1 + mp_2 \qquad k_2' = k_2 - mp_1$$

も同じ性質を持つ。

逆に，$k_1p_1 + k_2p_2 = 1$, $k_1'p_1 + k_2'p_2 = 1$ を満たす整数 k_1, k_2, k_1', k_2' があったとすると，$(k_1' - k_1)p_1 + (k_2' - k_2)p_2 = 0$ であるから，

$$(k_1' - k_1)p_1 = -(k_2' - k_2)p_2$$

である。p_1 と p_2 は互いに素であるから，$p_2|(k_1' - k_1)$, $p_1|(k_2' - k_2)$ でなければならない。すなわち，ある整数 m_1, m_2 があって，$k_1' - k_1 = m_1p_2$, $k_2' - k_2 = m_2p_1$ となっている。

$$(k_1 + m_1p_2)p_1 + (k_2 + m_2p_1)p_2 = 1$$

であるが，$k_1p_1 + k_2p_2 = 1$ より，$m_1p_2p_1 + m_2p_1p_2 = (m_1 + m_2)p_1p_2 = 0$ であるから，$m_1 = -m_2$ でなければならない。

以上から，次のことがわかった。

命題 2.4 p_1, p_2 を互いに素な２つの整数とし，k_1, k_2 を

$$k_1p_1 + k_2p_2 = 1$$

を満たす整数とする。ある整数 k_1', k_2' で $k_1'p_1 + k_2'p_2 = 1$ となるならば，ある整数 m があって，

$$k_1' = k_1 + mp_2 \qquad k_2' = k_2 - mp_1$$

となっている。

演習問題 2.1

(1) 1680 の正の約数をすべて求めよ。　(2) 240 と 360 の最大公約数を求めよ。

(3) 240 と 360 の最小公倍数を求めよ。　(4) 589 と 703 の最大公約数を求めよ。

(5) $k_1 179 + k_2 89 = 1$ を満たす k_1, k_2 を 1 組見つけよ。

2.2 合同類の積

整数全体 $\mathbb{Z}$ は和に関して群であったが，積に関しては群にならない。整数の範囲で考えると，積に関しては，1 以外の整数は逆元を持たないからである。しかし，合同類で考えると，積という演算に関しても，群になる場合があるのである。

定義 2.5 n を自然数とし，$\mathbb{Z}_n$ を剰余群とする。$\mathbb{Z}_n$ 上の積を次のように定義する。

$$[a] \cdot [b] = [ab]$$

剰余群 $\mathbb{Z}_n$ 上の演算は加法 $+$ であったから，このように定義した積は，集合 $\mathbb{Z}_n$ 上の全く新しい演算となるべきものだが，まず最初に，そもそも，これが演算として正しく定義されていることを証明する必要がある。

命題 2.6 この積は $\mathbb{Z}_n$ 上の２項演算になる。

証明: $\mathbb{Z}_n$ 上の演算として定義可能であることを示す。

具体的には，$\mathbb{Z}_n$ の元として $[a] = [a']$, $[b] = [b']$ である時，$\mathbb{Z}_n$ の元として $[ab] = [a'b']$ であることを示せば良い。

$[a] = [a']$, $[b] = [b']$ であるから，$a - a' \in n\mathbb{Z}$, $b - b' \in n\mathbb{Z}$ である。すなわち，ある $k, k' \in \mathbb{Z}$ があって，$a = a' + kn$, $b = b' + k'n$ となっている。

$$ab = (a' + kn)(b' + k'n) = a'b' + ak'n + b'kn + kk'n^2 = a'b' + n(ak' + b'k + kk'n)$$

であるから，$ab - a'b' \in n\mathbb{Z}$ となり，$[ab] = [a'b']$ であることが示された。□

a と a' が $\mathbb{Z}_n$ の同じ同値類に入っていることを

$$a \equiv a' \mod n \quad \text{または} \quad a \equiv a' \pmod{n}$$

と書いた。上の命題をこの記号を使って書き直すと，

命題 2.7 $a \equiv a' \pmod{n}$ であり $b \equiv b' \pmod{n}$ ならば $ab \equiv a'b' \pmod{n}$ である。

となる。

例えば，$a \equiv 1 \pmod{n}$ ならば，任意の整数 b に対して $ab \equiv b \pmod{n}$ となる。

この $\mathbb{Z}_n$ 上の積は結合律を満たすことは明らかであり，さらに，[1] が単位元であることも明らかである。もし，全ての元に逆元があれば，群になるのだが，それは成り立たない。

[0] は，他の元との積をとると常に [0] となり，[1] となることはない。すなわち，逆元を持たない。

それでは [0] 以外の元は逆元を持つだろうか？ すなわち，[0] を $\mathbb{Z}_n$ から除いてしまえば群になるだろうか？

これについても，一般には成立しない。[0] を除いてしまえば，積が定義されない場合があるからである。例えば，$n = 4$ の場合，

$$\mathbb{Z}_4 - \{[0]\} = \{1, 2, 3\}$$

を考えると，

$$2 \cdot 2 \equiv 0 \pmod 4$$

であるから，0 がなければ，積が定義されない。しかし，$\mathbb{Z}_n - \{[0]\}$ が群になる場合もあるのである。

定理 2.8 p を素数とし，$\mathbb{Z}_p^* = \mathbb{Z}_p - \{[0]\}$ とすると，これは積に関して群になる。

証明: $\mathbb{Z}_p^*$ が積に関して逆元を持つことを言えば良い。

以下では代表元で考えて，$[q] \in \mathbb{Z}_p$ を単に q と書くことにする。

$$\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$$

である。

$q \in \mathbb{Z}_p^*$ を任意の元とすると，p は素数なので，p と q は互いに素である。定理 2.2 より，ある整数 k_1, k_2 があって，$k_1 p + k_2 q = 1$ となる。

k_2 を p で割ると，ある整数 m と，$0 \leqq r \leqq p-1$ となる整数 r があって，$k_2 = mp + r$ となっている。ここで $r = 0$ ならば，$k_2 = mp$ なので，$k_1 p + mpq = (k_1 + mq)p = 1$ となり，1 より大きい整数 p に他の整数をかけて 1 となることはあり得ないので矛盾である。従って，$1 \leqq r \leqq p-1$ である。

$(mp + r)q = (-k_1)p + 1$ であるから，$rq = (-mq - k_1)p + 1$ であり，これは $rq \equiv 1 \pmod p$ であることを示している。$r \in \mathbb{Z}_p^*$ とみなすと，これは r が q の逆元であることを示している。□

$|\mathbb{Z}_p^*| = p-1$ であるから，定理 1.39 より，$\mathbb{Z}_p^*$ の任意の元 a に対し，$\mathbb{Z}_p^*$ 上の積に関して，$a^{p-1} = 1$ が成り立つ。

これが，初等整数論において有名な次の定理である。

定理 2.9 (フェルマーの小定理) 素数 p と $(p, a) = 1$ となる自然数 a に対して次が成り立つ。

$$a^{p-1} \equiv 1 \pmod p$$

証明: p を素数とし，a を $(p,a)=1$ となる自然数とする。

整数の剰余定理より，ある整数 q と $0 \leqq r \leqq p-1$ となる r があって，$a=qp+r$ となる。

もし $r=0$ なら，a は p の倍数であり，$a \neq 0$ なので，$(p,a)=p \neq 1$ となって，$(p,a)=1$ に矛盾する。従って，$1 \leqq r \leqq p-1$ である。

$\mathbb{Z}_p$ において $[a]=[r]$ であるから，$[a^{p-1}]=[a]^{p-1}=[r]^{p-1}=[r^{p-1}]$ である。

定理 2.8 より，$\mathbb{Z}_p^*$ は積に関して群であるから，定理 1.39 より，$\mathbb{Z}_p^*$ においては，$[r]^{p-1}=1$ である。すなわち，$[a^{p-1}]=1$ である。これは，

$$a^{p-1} \equiv 1 \pmod{p}$$

を意味する。□

注意： **(1)** 素数 p に対して，$a \in \mathbb{Z}$ が $(p,a)=1$ すなわち，p と a が互いに素であるということは，a が p の倍数になっていない，ということである。

(2) $a^{p-1} \equiv 1 \pmod{p}$ の両辺に a をかけて，

$$a^p \equiv a \pmod{p}$$

という形で使われることもある。

例： **(1)** $p=5$, $a=4$ とすると $(5,4)=1$ である。

$$4^{5-1}=4^4=256 \equiv 1 \pmod{5}$$

(2) $p=11$, $a=12$ とすると $(11,12)=1$ である。

$$12^{11-1}=12^{10}=61917364224=5628851293*11+1 \equiv 1 \pmod{11}$$

(3) 例題： $2^{1,000,000} \pmod{7}$ を求めよ。

解： $(2,7)=1$ であり 7 は素数だから，フェルマーの小定理から $2^6 \equiv 1 \pmod{7}$ である。$1,000,000=166666*6+4$ であるから，

$$\begin{aligned} 2^{1,000,000} &= 2^{166666*6+4} = 2^{166666*6}2^4 = \left(2^6\right)^{166666}2^4 \\ &\equiv 2^4 \pmod{7} \equiv 2 \pmod{7} \end{aligned}$$

(4) 例題： $1234^{1,000,000,000} \pmod{997}$ を求めよ。

解： $(1234,997)=1$ であり 997 は素数だから，フェルマーの小定理から $1234^{996} \equiv 1 \pmod{997}$ である。

$1,000,000,000=1004016*996+64$ であるから，

$$\begin{aligned} 1234^{1,000,000,000} &= 1234^{1004016*996+64} = 1234^{1004016*996}1234^{64} \\ &= \left(1234^{996}\right)^{1004016}1234^{64} \\ &\equiv 1234^{64} \pmod{997} \end{aligned}$$

となり，$1234^{64} \pmod{997}$ を求める問題に帰着された。あとは，$1234 = 237 \pmod{997}$ なので，

$$1234^{64} \equiv 237^{64} \pmod{997}$$

となる。

$$237^2 = 56169 \equiv 337 \pmod{997}$$

なので，

$$237^{64} = 56169^{32} \equiv 337^{32} \pmod{997}$$

というプロセスにより，$\log_2 64$ の回数で指数を 0 にできる。