

3 整数と剰余類

3.1 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 3.1 (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、 $(a, b) \geq 1$ 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 multiple) 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。 a と b の最小公倍数は $[a, b]$ で表す。

(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。

演習問題 3.1 a, b を正の整数とする。このとき最大公約数と最小公倍数の積は ab である事、即ち $(a, b) \cdot [a, b] = a \cdot b$ が成立することを示せ。

定理 3.2 p_1, \dots, 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 $d|p_1, \dots, d|p_n$ 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, \dots, k_n が存在して、

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

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 1.32 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、 $k_1 p_1 + \cdots + k_n p_n = 1$ 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 3.3 p_1, p_2 を互いに素な 2 つの整数とすると、

$$k_1 p_1 + k_2 p_2 = 1$$

を満たす整数 k_1, k_2 が存在する。

注意： $k_1 p_1 + k_2 p_2 = 1$ 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、

$$1 = k_1 p_1 + k_2 p_2 = k_1 p_1 + k_2 p_2 + m p_1 p_2 - m p_1 p_2 = (k_1 + m p_2) p_1 + (k_2 - m p_1) p_2$$

である。すなわち、

$$k'_1 = k_1 + m p_2 \quad k'_2 = k_2 - m p_1$$

も同じ性質を持つ。

逆に、 $k_1 p_1 + k_2 p_2 = 1$, $k'_1 p_1 + k'_2 p_2 = 1$ 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、 $p_2 \mid (k'_1 - k_1)$, $p_1 \mid (k'_2 - k_2)$ 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、 $k'_1 - k_1 = m_1 p_2$, $k'_2 - k_2 = m_2 p_1$ となっている。

$$(k_1 + m_1 p_2) p_1 + (k_2 + m_2 p_1) p_2 = 1$$

であるが、 $k_1 p_1 + k_2 p_2 = 1$ より、 $m_1 p_2 p_1 + m_2 p_1 p_2 = (m_1 + m_2) p_1 p_2 = 0$ 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 3.4 p_1, p_2 を互いに素な 2 つの整数とし、 k_1, k_2 を

$$k_1 p_1 + k_2 p_2 = 1$$

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、

$$k'_1 = k_1 + m p_2 \quad k'_2 = k_2 - m p_1$$

となっている。

演習問題 3.2

- (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) $k_1 79 + k_2 89 = 1$ を満たす k_1, k_2 を 1 組見つけよ。

3.2 剰余類の積

整数全体 \mathbb{Z} は和に関して群になるが、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。

その前に、重要なので整数の合同類 (剰余類) について復習しておく。

整数全体の集合を \mathbb{Z} とすると和という演算に関して群である。 n を正の整数とし、1 つ固定して考える。このとき $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ は \mathbb{Z} の部分群である。このとき \mathbb{Z} の $n\mathbb{Z}$ による剰余類全体の集合を \mathbb{Z}_n と書くと \mathbb{Z}_n は和に関して群をなす。具体例で見よう。 $n = 4$ とする。0 を含む剰余類 $[0]$ は 4 で割った余りが 0 である整数の全体なので

$$[0] = \{4k + 0 \mid k \in \mathbb{Z}\} = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

である。同様に他の剰余類は

$$[1] = \{4k + 1 \mid k \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$[2] = \{4k + 2 \mid k \in \mathbb{Z}\} = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$[3] = \{4k + 3 \mid k \in \mathbb{Z}\} = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

である。このとき $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ である。

$[2]$ と $[3]$ の和は $[2]$ と $[3]$ から任意に元を選ぶ。 $n_1 \in [2], [n_2] \in [3]$ として $n_1 + n_2$ を求める。例えば $n_1 = 6, n_2 = 7$ とすると、 $n_1 + n_2 = 13$ となる。13 が属する剰余類は $[13]$ であるが、 $[13] = [1]$ なので $[2] + [3] = [1]$ となる。和を計算するとき 6 と 7 を選んだが、他の元でもかまわない。例えば $n_1 = 2, n_2 = 3$ を選ぶと $n_1 + n_2 = 5$ となるので $[2] + [3] = [5]$ となるが、 $[5] = [1]$ なので $[2] + [3] = [1]$ となる。即ち和を定義する方法は元の選び方によらない。

剰余群を代表元で表す方法もある。各剰余類から代表元を 1 つ選ぶ。例えば $0 \in [0], 1 \in [1], 2 \in [2], 3 \in [3]$ とすると、 $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ と考える。このとき例えば $2 + 3$ は $4\mathbb{Z}$ には入らないので整数の和ではなく、 $\text{mod } 4$ で考える。即ち 4 で割った余りを考える。 $2 + 3 = 5 \equiv 1 \pmod{4}$ なので 2 と 3 の和は 1 と考える。この 2 つの考え方は同等であることが分かる。

定義 3.5 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 3.6 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

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

と書いた。上の命題をこの記号を使って書き直すと,

命題 3.7 $a \equiv a' \pmod{n}$ 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。

積が定義できたので, 積の性質について確認しておく。

命題 3.8 $[a], [b], [c] \in \mathbb{Z}_n$ とする。

- (1) $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$ (結合法則)
- (2) $[1] \cdot [a] = [a] \cdot [1] = [a]$ (単位元の存在)
- (3) $[a] \cdot [b] = [b] \cdot [a]$ (交換法則)
- (4) $[0] \cdot [a] = [0]$

命題 3.8 を合同の記号を使って書き直すと次のようになる。 $a, b, c \in \mathbb{Z}$ とする。

- (1) $(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{n}$
- (2) $a \cdot 1 \equiv 1 \cdot a \equiv a \pmod{n}$
- (3) $a \cdot b \equiv b \cdot a \pmod{n}$
- (4) $0 \cdot a \equiv 0 \pmod{n}$

もし, 全ての元に積に関する逆元があれば, 積に関しても群になるのだが, 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, $\mathbb{Z}_n - \{[0]\}$ が積に関して群になる場合もある。

$\mathbb{Z}_7^* = \mathbb{Z}_7 - \{[0]\} = \{[1], [2], [3], [4], [5], [6]\}$ とする。 $[2]^2 = [2] \cdot [2] = [4]$, $[2]^3 = [4] \cdot [2] = [8] = [1]$ なので $[2] \cdot [4] = [1]$ となり $[2]$ の逆元は $[4]$ である。即ち $[2]^{-1} = [4]$ である。また $[4]^{-1} = [2]$ でもある。

$[3]^2 = [9] = [2]$, $[3]^3 = [2] \cdot [3] = [6]$, $[3]^4 = [6] \cdot [3] = [18] = [4]$, $[3]^5 = [4] \cdot [3] = [12] = [5]$, $[3]^6 = [5] \cdot [3] = [15] = [1]$ より $[3] \cdot [5] = [1]$ となり $[3]^{-1} = [5]$, $[5]^{-1} = [3]$ となる。

$[6]^2 = [36] = [1]$ なので $[6]^{-1} = [6]$ である。よって \mathbb{Z}_7^* に関しては乗法の逆元がすべて存在するので, 乗法に関しても群になる。一般に次が成立する。

定理 3.9 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。

$[q] \in \mathbb{Z}_p^*$ 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 3.2 より, ある整数 k_1, k_2 があって, $k_1p + k_2q = 1$ となる。

k_2 を p で割ると, ある整数 m と, $0 \leq r \leq p-1$ 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, $k_1p + mpq = (k_1 + mq)p = 1$ 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, $1 \leq r \leq p-1$ 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, \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 3.10 [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。このとき $[a] \in \mathbb{Z}_p^*$ である。

定理 3.9 より, \mathbb{Z}_p^* は積に関して群であり, $|\mathbb{Z}_p^*| = p-1$ である。 $[a]$ の位数を k とすると $[a]^k = [1]$ であり, 定理 1.30 より, k は $p-1$ の約数なのである整数 m を用いて $p-1 = km$ と書ける。

$$[a^{p-1}] = [a]^{p-1} = [a]^{km} = ([a]^k)^m = [1]^m = [1]$$

が成立する。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,

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

(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,

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

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