

---

## 4. 整数論

# 約数と倍数

任意の整数を $a$ とし、任意の正整数を $b$ とすると、

$$a = bq + r, \quad 0 \leq r \leq b - 1$$

を満たす $q, r$ が一意的に存在する。このとき、 $q$ を商、 $r$ を剰余という。

$r = 0$  即ち、 $a = bq$  のとき、 $a$ は $b$ の倍数、 $b$ は $a$ の約数という。

**公約数** (common divisor) : 任意の2つの整数の共通の約数

**最大公約数** (greatest common divisor) : 公約数の中で最大の数

整数 $a, b$ の最大公約数を以下で表現

$$(a, b) \text{ または } \text{GCD}(a, b)$$

$(a, b) = 1$  の時、 $a$ と $b$ は互いに素であるという。

**公倍数** (common multiple) : 任意の2つの整数の共通の倍数

**最小公倍数** (least common multiple) : 公倍数の中で最小の数

整数 $a, b$ の最小公倍数を以下で表現

$$\text{LCM}(a, b)$$

# 約数に関する定理

**定理1** 任意の整数 $a$ ( $\neq 0$ 。以降も同じ)に対して、 $a$ は $a$ の約数、 $1$ は $a$ の約数

**定理2**  $a$ が $b$ の約数、 $b$ が $c$ の約数ならば、 $a$ は $c$ の約数

**定理3**  $a$ が $b$ の約数、 $b$ が $a$ の約数ならば、 $b = \pm a$

**証明**  $b = qa, a = q'b$  ( $q, q'$  は整数)

$$a = q'qa$$

$$a \neq 0 \text{ 故、} q'q = 1, q' = q = \pm 1 \quad \therefore b = \pm a$$

**補遺**  $a$ が $b$ の約数、 $c$ が $d$ の約数ならば、 $ac$ は $bd$ の約数

**定理4**  $a$ が $b$ と $c$ の公約数ならば、 $a$ は $b \pm c$ の約数

**証明**  $b = qa, c = q'a$  ( $q, q'$  は整数)

$$b \pm c = qa \pm q'a = (q \pm q')a$$

$q \pm q'$  は整数故、 $a$ は $b \pm c$ の約数

# 最大公約数に関する定理

**定理5**  $a < b$  の時、 $q$  を整数とすると、 $(a, b) = (a, b - qa)$

**証明**

$d = (a, b)$ ,  $d' = (a, b - qa)$  とおく

$d$  は  $qa$  の約数 従って、 $d$  は  $qa$  と  $b$  の公約数

$\therefore$  定理4より  $d$  は  $b - qa$  の約数

$\therefore d$  は  $a$  と  $b - qa$  の公約数

$d'$  は  $a$  と  $b - qa$  の最大公約数故、 $d \leq d' \cdots \textcircled{1}$

逆に、 $d'$  は  $a$  と  $b - qa$  の公約数

$d'$  は  $qa$  の約数

$\therefore d'$  は  $(b - qa) + qa$  の約数 即ち、 $d'$  は  $b$  の約数

$\therefore d'$  は  $a$  と  $b$  の公約数

$d$  は  $a$  と  $b$  の最大公約数故、 $d' \leq d \cdots \textcircled{2}$

式 $\textcircled{1}$ 、 $\textcircled{2}$ より、 $d = d'$  即ち、 $(a, b) = (a, b - qa)$

**例**  $(6, 15) = (6, 15 - 2 \cdot 6) = (6, 3)$

# ユークリッドの互除法

a と b の最大公約数 (a, b) を求める

$a < b$  とすると、 $b = q_1 a + r_1$  とおける

定理5より  $(a, b) = (a, b - q_1 a) = (a, r_1) = (r_1, a) \quad r_1 < a$

$$b = q_1 a + r_1$$

$$a = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

...

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n + 0$$

$$b > a > r_1 > r_2 > \dots > r_n > 0$$

$$(a, b) = (r_1, a) = (r_2, r_1) = \dots = (r_n, r_{n-1}) = (0, r_n) = r_n$$

例: (85, 204) を求める

$$85 = 0 \cdot 204 + 85$$

$$204 = 2 \cdot 85 + 34$$

$$85 = 2 \cdot 34 + 17$$

$$34 = 2 \cdot 17 + 0$$

最大公約数は17

例: (3, 11) を求める

$$11 = 3 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

最大公約数は1

# オイラーの関数

素数: 1より大きい整数で、1とその整数以外の約数を持たない数

合成数: 1とその整数以外にも、約数を持つ正整数

(注) 1は素数でも合成数でもない

定理6 合成数は素数の積で表される(素因数分解)

定理7 合成数を素数の積で表す仕方は1通りである(積の順序は対象外)

オイラーの関数  $\phi(n)$ : 正整数  $n$  に対し、 $1 \leq i \leq n$  で、 $(n, i) = 1$  を満たす  $i$  の総数

例:  $n=12$  のとき、 $1 \leq i \leq 12$  を満たす集合  $Z_{12}$  は

$$Z_{12} = \{1, 2, 3, \dots, 12\}$$

$(12, i) = 1$  を満たす  $i$  の集合  $Z_{12}^* = \{1, 5, 7, 11\}$  故、 $\phi(n)=4$

# 合同式

日	月	火	水	木	金	土
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

日:  $x \bmod 7 = 4$

月:  $x \bmod 7 = 5$

火:  $x \bmod 7 = 6$

水:  $x \bmod 7 = 0$

木:  $x \bmod 7 = 1$

金:  $x \bmod 7 = 2$

土:  $x \bmod 7 = 3$

2つの整数  $a, b$  が同じ曜日を表すということは、7で割った余りが同一ということ  
このことを以下のように記述し、「 $a$  は7を法として  $b$  に合同である」という

合同式  $a \equiv b \bmod 7$

反射律  $a \equiv a \bmod n$  但し、 $n$  は自然数

対称律  $a \equiv b \bmod n$  ならば  $b \equiv a \bmod n$

推移律  $a \equiv b \bmod n$  かつ  $b \equiv c \bmod n$  ならば  $a \equiv c \bmod n$

例:  $3 \equiv 10 \bmod 7$  かつ  $10 \equiv 17 \bmod 7$  ならば  $3 \equiv 17 \bmod 7$

# 合同式の算法(1)

**定理8**  $a \equiv b \pmod{n}$ 、 $c \equiv d \pmod{n}$  のとき、

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}$$

$$ac \equiv bd \pmod{n}$$

**証明**  $a = pn + r$     $b = qn + r$     $c = sn + u$     $d = tn + u$

$$a+c = (p+s)n + \underline{(r+u)} \qquad b+d = (q+t)n + \underline{(r+u)}$$

同一なので、 $n$ で割った余りも同じ

$$a-c = (p-s)n + \underline{(r-u)} \qquad b-d = (q-t)n + \underline{(r-u)}$$

同一なので、 $n$ で割った余りも同じ

$$ac = (psn + pu+rs)n + \underline{ru} \qquad bd = (qtn+qt+rt)n + \underline{ru}$$

同一なので、 $n$ で割った余りも同じ



## 合同式の算法(2)

**定理9**  $a \equiv b \pmod{n}$  ならば  $a^k \equiv b^k \pmod{n}$

$$\begin{array}{l} \text{証明} \qquad a \equiv b \pmod{n} \\ \qquad \qquad a \equiv b \pmod{n} \\ \qquad \qquad \dots \\ \qquad \qquad a \equiv b \pmod{n} \end{array} \left. \vphantom{\begin{array}{l} a \equiv b \pmod{n} \\ a \equiv b \pmod{n} \\ \dots \\ a \equiv b \pmod{n} \end{array}} \right\} k\text{個}$$

両辺を掛け合わせると

$$a^k \equiv b^k \pmod{n}$$

**定理10**  $(c, n) = 1$  ならば

$ac \equiv bc \pmod{n}$  の時、 $a \equiv b \pmod{n}$

$$\begin{array}{l} \text{証明} \qquad ac - bc \equiv 0 \pmod{n} \\ \qquad \qquad (a - b)c \equiv 0 \pmod{n} \end{array}$$

$(c, n) = 1$  故、 $a - b \equiv 0 \pmod{n}$

即ち、 $a \equiv b \pmod{n}$

# 剰余類

剰余類 $R(a)$ : 自然数  $n$  と整数  $a$  に対して、 $n$  を法として  $a$  と合同な整数の集合

完全剰余系 $R_n$ : 各剰余類 $R(i)$  ( $i=0,1,\dots,n-1$ ) それぞれの要素から成る整数集合

既約剰余系 $R_n^*$ : 完全剰余系 $R_n$  の整数のうち、 $n$  と互いに素となる ( $(n, a_i)=1$ ) 整数 $a_i$ の集合

例:  $n=10$  を法とする剰余類

$$R(0) = \{ \dots, -20, -10, 0, 10, 20, \dots \}$$

$$R(1) = \{ \dots, -19, -9, 1, 11, 21, \dots \}$$

...

$$R(9) = \{ \dots, -11, -1, 9, 19, 29, \dots \}$$

$$\text{完全剰余系 } R_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\text{既約剰余系 } R_{10}^* = \{1, 3, 7, 9\}$$

$$\text{オイラーの関数 ( } R_n^* \text{ の要素数 ) } \phi(10) = 4$$

# 既約剰余系の乗算

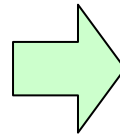
完全剰余系  $R_{10} : \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

乗算結果

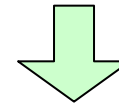
	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

既約剰余系  $R_{10}^* : \{1, 3, 7, 9\}$

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1



- ・任意の2つの数の乗算結果は元の既約剰余系の要素
- ・乗算表の行や列には、すべての要素が繰り返なしで現れる



乗算の対応は1対1

# 既約剰余系の乗算対応

**定理11**  $\text{mod } n$  の既約剰余系  $R_n^* = \{a_1, a_2, \dots, a_{\phi(n)}\}$  の各要素  $x$  に、 $R_n^*$  のうちの1つの要素  $a_i$  を掛けて

$$x \rightarrow a_i x$$

という対応を考えると、この対応は1対1である。

**証明**

$(a_i, n) = 1, (x, n) = 1$  故、 $(a_i x, n) = 1$

従って、 $a_i x$  は既約剰余系  $R_n^*$  に属する

また、 $x_1 \rightarrow a_i x_1, x_2 \rightarrow a_i x_2$

で、 $a_i x_1 \equiv a_i x_2 \pmod{n}$

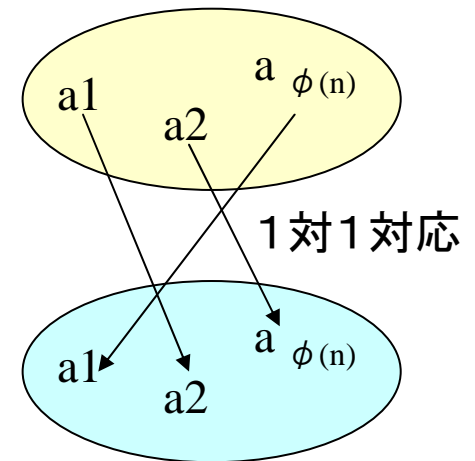
ならば、定理8より  $a_i(x_1 - x_2) \equiv 0 \pmod{n}$

即ち、 $n$  は  $a_i(x_1 - x_2)$  の約数

ここで、 $(a_i, n) = 1$  故、 $n$  は  $(x_1 - x_2)$  の約数

即ち、 $x_1 \equiv x_2 \pmod{n}$

従って、対応は1対1



# オイラーの定理

**定理12** 自然数 $n$ 、整数 $a$ に対し、 $(a, n) = 1$  ならば、以下の式が成立

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

**証明**  $R_n^* = \{a_1, a_2, \dots, a_{\phi(n)}\}$  の各要素を $x$ 、 $R_n^*$ のうちの1つの要素 $a_i$ とした場合

$x \rightarrow a_i x$  は1対1対応

即ち、 $\{a_1, a_2, \dots, a_{\phi(n)}\}$  と  $\{a_i a_1, a_i a_2, \dots, a_i a_{\phi(n)}\}$  は要素の並び順を除いては、同一の集合

従って、その積は同一。即ち、

$$a_1 a_2 \cdots a_{\phi(n)} \equiv (a_i a_1)(a_i a_2) \cdots (a_i a_{\phi(n)}) \pmod{n}$$

$$a_1 a_2 \cdots a_{\phi(n)} \equiv a_i^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$$

$$a_1 a_2 \cdots a_{\phi(n)} (a_i^{\phi(n)} - 1) \equiv 0 \pmod{n}$$

$a_1 a_2 \cdots a_{\phi(n)}$  は  $n$  と互いに素故、

$$a_i^{\phi(n)} - 1 \equiv 0 \pmod{n}$$

$$a_i^{\phi(n)} \equiv 1 \pmod{n}$$

## 付. オイラーの定理の例

**定理12** 自然数 $n$ 、整数 $a$ に対し、 $(a, n) = 1$  ならば、以下の式が成立

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

例

$n=12$  のとき、 $(a, 12) = 1$  を満たす既約剰余系 $R_{12}^* = \{1, 5, 7, 11\}$

オイラーの関数  $\phi(12) = 4$

$$1^4 \equiv 1 \pmod{12}$$

$$5^4 = 25^2 \equiv 1 \pmod{12}$$

$$7^4 = 49^2 \equiv 1 \pmod{12}$$

$$11^4 = 121^2 \equiv 1 \pmod{12}$$

$$ab \pmod{p} = (mp+r)b \pmod{p} = (mpb+rb) \pmod{p} = rb \pmod{p}$$

$ab$ に対する剰余は  $(a$ に対する剰余) $\cdot b$  に対する剰余に等しい

# フェルマーの小定理

**定理13** 整数 $a$  に対し、 $p$  が素数で、 $(a, p) = 1$  ならば、以下の式が成立

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

$\because$   $p$ が素数故、オイラー関数  $\phi(p) = p - 1$

例  $p = 5$  のとき

$$a = 1, 2, 3, 4$$

$$p - 1 = 4$$

$$1^4 \equiv 1 \pmod{5}$$

$$2^4 = 16 \equiv 1 \pmod{5}$$

$$3^4 = 81 \equiv 1 \pmod{5}$$

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

# 逆数

素数 $p$ の既約剰余系  $R_p^* = \{1, 2, \dots, p-1\}$  の任意の要素  $a$  に対して

$$ab \equiv 1 \pmod{p}$$

となる $b$ が存在する。

$b = a^{p-2}$  を選べばよい

$b$  を $a$  の逆数(逆元)といい、 $a^{-1}$ で表す。

## フェルマーの小定理

$p$ が素数で、 $(a, p) = 1$  ならば、以下の式が成立

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

$a$  の逆数は唯一に定まる。

証明

$$\begin{aligned} ab &\equiv 1 \pmod{p} \\ ab' &\equiv 1 \pmod{p} \end{aligned}$$

$$\text{とすると、} a(b-b') \equiv 0 \pmod{p}$$

$$(a, p) = 1 \text{ 故、} b-b' \equiv 0 \pmod{p}$$

$$\text{即ち、} b \equiv b' \pmod{p}$$

ある数の逆数の逆数はその数自身  $(a^{-1})^{-1} = a$



# 逆数の計算(1)

例 mod 11での既約剰余系の逆数

$b = a^{p-2}$  を計算

$$1^{-1} \equiv 1^{11-2} = 1^9 \equiv 1$$

$$2^{-1} \equiv 2^{11-2} = 2^9 = 512 \equiv 6$$

$$3^{-1} \equiv 3^{11-2} = 3^9 = (3^3)^3 = 27^3 \equiv 5^3 = 125 \equiv 4$$

$$4^{-1} \equiv 3$$

$$5^{-1} \equiv 5^{11-2} = 5^9 = (5^3)^3 = 125^3 \equiv 4^3 = 64 \equiv 9$$

$$6^{-1} \equiv 2$$

$$7^{-1} \equiv 7^{11-2} = 7^9 = (7^3)^3 = 343^3 \equiv 2^3 = 8$$

$$8^{-1} \equiv 7$$

$$9^{-1} \equiv 5$$

$$10^{-1} \equiv 10^{11-2} = 10^9 = (10^3)^3 = 1000^3 \equiv 10^3 = 1000 \equiv 10$$

## 逆数の計算(2)

例  $3b \equiv 1 \pmod{11}$ における $b$ (3の逆数)の計算

ユークリッドの互除法の利用

$$3b \equiv 1 \pmod{11} \quad (1)$$

$$\text{恒等的に成り立つ式} \quad 11b \equiv 0 \pmod{11} \quad (2)$$

11と3にユークリッドの互除法を適用

$$11 = 3 \cdot 3 + 2 \quad (3)$$

$$3 = 1 \cdot 2 + 1 \quad (4)$$

$$2 = 2 \cdot 1$$

$$(3) \text{より、} \times 3 \text{ が必要} \quad 3 \equiv 3 \pmod{11} \quad (5)$$

$$(1) \times (5) \quad 9b \equiv 3 \pmod{11} \quad (6)$$

$$(2) - (6) \quad 2b \equiv -3 \pmod{11} \quad (7)$$

$$(4) \text{より、} (1) - (7) \quad b \equiv 4 \pmod{11}$$