1　数学的帰納法

整数とは,

$$\cdots, \quad -3, \quad -2, \quad -1, \quad 0, \quad 1, \quad 2, \quad 3, \quad \cdots$$

のひとつひとつのことである. 整数の全体からなる集合を $\mathbb{Z}$ で表す.

二つの整数 a, b に対して, それらの和 $a+b$, 差 $a-b$, 積 ab が定義されている.

二つの整数 a, b の間には順序関係 $\leq$ が定義されていて, $a \leq b$ か $b \leq a$ かのどちらか一方が必ず成り立つ. さらに, $a \leq b$ と $b \leq a$ とがともに成り立つとき, $a = b$ となる.

0 より大きい整数を**正**の整数といい, 0 より小さい整数を**負**の整数という.

また, 正の整数全体からなる集合を $\mathbb{Z}^+$ で表す:

$$\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}.$$

私たちは, 次の数学的帰納法の原理を以後の議論の前提とする:

定理 1.1 (数学的帰納法の原理). $\mathbb{Z}^+$ の部分集合 S が, 二つの条件

(i) $1 \in S$.

(ii) $n \in \mathbb{Z}^+$ とするとき, $n \in S \Longrightarrow n+1 \in S$.

を満たすと仮定する. このとき, $S = \mathbb{Z}^+$ となる.

定理 1.2 (数学的帰納法). 各々の $n \in \mathbb{Z}^+$ に対して命題 $P(n)$ が与えられたとし, それについて次の二つのことが示されたとする.

(i) $P(1)$ が成り立つ.

(ii) $P(n)$ が成り立つならば $P(n+1)$ が成り立つ.

このとき, すべての $n \in \mathbb{Z}$ に対して $P(n)$ は成り立つ.

証明. $S = \{n \in \mathbb{Z}^+ \mid P(n)$ が成り立つ $\}$ とおく.

条件 (i) より, $1 \in S$.

条件 (ii) より, $n \in \mathbb{Z}^+$ について, $n \in S$ ならば $n+1 \in S$ である.

ゆえに, すべての $n \in \mathbb{Z}^+$ に対して $n \in S$ となる.

すなわち, すべての $n \in \mathbb{Z}^+$ に対して命題 $P(n)$ が成り立つ. □

整数は, **整列性**と呼ばれる, 次の性質を持つ:

定理 1.3 (整列性). 任意の空でない $\mathbb{Z}^+$ の部分集合は最小元をもつ.

すなわち, S を $\mathbb{Z}^+$ の部分集合とすれば,

$$\exists n \in S \ \text{ s.t. } \forall x \in S,\ n \leq x$$

が成り立つ.

証明. S を $\mathbb{Z}^+$ の部分集合とし, $S \neq \emptyset$ とする.

$$T = \{n \in \mathbb{Z}^+ \mid \text{任意の } x \in S \text{ に対して } n \leq x \text{ が成り立つ}\}$$

とおく.

まず, 1 は $\mathbb{Z}^+$ における最小元であるから, $1 \in T$ が成り立つ.

次に, $S \neq \emptyset$ より, ある $x \in \mathbb{Z}^+$ が存在して $x \in S$ となる.

$x < x+1$ より,

$$x+1 \notin T.$$

よって,

$$T \neq \mathbb{Z}^+.$$

ゆえに, 定理 1.1 より,

$$m \in T \quad \text{かつ} \quad m+1 \notin T$$

なる $m \in \mathbb{Z}^+$ が存在する.

もし仮に $m \notin S$ ならば, すべての $x \in S$ に対して $m < x$, したがって $m+1 \leq x$ となる. これは $m+1 \notin T$ に反する.

したがって, $m \in S$ であって, m は S の最小元である. □

定理 1.4. $\mathbb{Z}^+$ の部分集合 S が, 二つの条件

(i) $1 \in S$.

(ii) $n \in \mathbb{Z}^+$ とするとき, $1 \leq k \leq n$ であるすべての $k \in \mathbb{Z}^+$ について $k \in S$ ならば, $n+1 \in S$.

を満たすと仮定する. このとき, $S = \mathbb{Z}^+$ となる.

証明. $T = \{x \in \mathbb{Z}^+ \mid x \notin S\}$ とおく. $T = \emptyset$ を示せばよい.

背理法を用いる. もし仮に $T \neq \emptyset$ とすると, 整列性によって T は最小元 n_0 をもつ. 仮定 (i) によって, $n_0 > 1$, ゆえに $n_0 - 1 \in \mathbb{Z}^+$ である. n_0 の最小性によって, $1 \leq k \leq n_0 - 1$ なるすべての $k \in \mathbb{Z}^+$ について $k \in S$ でなければならない. このとき, 仮定 (ii) によって $n_0 \in S$. これは $n_0 \in T$ に反する. □

次の定理は, 前述した数学的帰納法の強化版である. これもまた数学的帰納法と呼ぶ.

定理 1.5 (数学的帰納法). 各々の $n \in \mathbb{Z}^+$ に対して命題 $P(n)$ が与えられたとし, それについて次の二つのことが示されたとする.

(i) $P(1)$ が成り立つ.

(ii) $n \in \mathbb{Z}^+$ とするとき, $1 \leq k \leq n$ であるすべての $k \in \mathbb{Z}^+$ について $P(n)$ が成り立つならば $P(n+1)$ が成り立つ.

このとき, すべての $n \in \mathbb{Z}$ に対して $P(n)$ は成り立つ.

証明. $S = \{n \in \mathbb{Z}^+ \mid P(n) \text{ が成り立つ}\}$ とおく.

条件 (i) より, $1 \in S$.

条件 (ii) より, $n \in \mathbb{Z}^+$ について, $1 \leq k \leq n$ であるすべての $k \in \mathbb{Z}^+$ について $k \in S$ ならば $n+1 \in S$ である.

ゆえに, すべての $n \in \mathbb{Z}^+$ に対して $n \in S$ となる.

すなわち, すべての $n \in \mathbb{Z}^+$ に対して命題 $P(n)$ が成り立つ. □

定理 1.6 (除法の原理). $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ とする. このとき

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

を満たすような q, $r \in \mathbb{Z}$ がただ一組だけ存在する.

q, r を, それぞれ a を b で割ったときの**商**, **剰余** (または**余り**) という.

証明. まず, q, r の存在を示す.

$$r_1 = \min\{x \in \mathbb{Z}^+ \mid \text{ある } q \in \mathbb{Z} \text{ が存在して } a = bq + x \text{ が成り立つ}\}$$

とおく. 整列性より, このような r_1 の存在が保証される.

いま, $q_1 \in \mathbb{Z}$ が存在して

$$a = bq_1 + r_1$$

であるとする.

もし仮に $r_1 > b$ ならば,

$$0 < r_1 - b < r_1, \quad a = b(q_1 - 1) + (r_1 - b)$$

となって r_1 の最小性に反する. ゆえに $r_1 \leq b$ である.

$r_1 < b$ のとき, $q = q_1$, $r = r_1$ とおけばよい.

$r_1 = b$ のとき, $q = q_1 + 1$, $r = 0$ とおけばよい.

次に, 一意性を示す.

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

$$a = bq' + r', \quad 0 \leq r' < b$$

とする.

もし仮に $q \neq q'$ ならば,

$$b(q' - q) = r' - r.$$

よって,

$$b \leq b|q' - q| = |r' - r| \leq \max\{r, r'\} < b.$$

これは矛盾である.

したがって $q = q'$, $r = r'$ でなければならない. □

系 1.6.1. $a \in \mathbb{Z}$, b_1, b_2, …, $b_n \in \mathbb{Z}^+$ とする. このとき

$$\begin{aligned} &a = q_n b_1 b_2 \cdots b_n + r_{n-1} b_1 b_2 \cdots b_{n-1} + \cdots + r_1 b_1 + r_0, \\ &0 \leq r_i < b_{i+1} \quad (0 \leq i \leq n-1) \end{aligned}$$

を満たす q_n, r_0, …, $r_{n-1} \in \mathbb{Z}$ がただ一組だけ存在する.

証明. n に関する数学的帰納法により証明する.

$n = 1$ のときは上の定理より明らかである.

$n = k$ のとき, 主張が正しいと仮定すると,

$$\begin{aligned} &a = q_k b_1 b_2 \cdots b_k + r_{k-1} b_1 b_2 \cdots b_{k-1} + \cdots + r_1 b_1 + r_0, \\ &0 \leq r_i < b_{i+1} \quad (0 \leq i \leq k-1) \end{aligned}$$

を満たす q_k, r_0, …, $r_{k-1} \in \mathbb{Z}$ がただ一組だけ存在する. さらに,

$$q_k = q_{k+1} b_{k+1} + r_k, \quad 0 \leq r_k \leq b_{k+1}$$

を満たす組 q_{k+1}, $r_k \in \mathbb{Z}$ がただ一組だけ存在する. これを一つ上の式に代入すれば

$$a = q_{k+1} b_1 b_2 \cdots b_{k+1} + r_k b_1 b_2 \cdots b_k + \cdots + r_1 b_1 + r_0$$

が得られる. したがって, $n = k+1$ のときも主張は正しい.

以上より, すべての n に関して主張は正しい. □

系 1.6.2. a, $b \in \mathbb{Z}^+$ とする. このとき, ある $m \in \mathbb{Z}^+$ が存在して,

$$a = r_m b^m + r_{m-1} b^{m-1} + \cdots + r_1 b + r_0, \quad 0 \leq r_i < b \quad (0 \leq i \leq m)$$

を満たす r_0, …, $r_m \in \mathbb{Z}$ が m に対してただ一組だけ定まる.

証明. まず,

$$a = b q_1 + r_0, \quad 0 \leq r_0 < b$$

を満たす q_1, $r_0 \in \mathbb{Z}$ がただ一組だけ存在する. さらに, $n \geq 1$ に対して,

$$q_n = b q_{n+1} + r_n, \quad 0 \leq r_n < b$$

を満たす q_{n+1}, $r_n \in \mathbb{Z}$ がただ一組だけ存在する.

このとき, $q_n \geq 0$ であるが, もしすべての $n \in \mathbb{Z}^+$ について $q_n > 0$ ならば, q_n の定め方から, 無限に続く減少列

$$a > q_1 > q_2 > \cdots > q_n > q_{n+1} > \cdots > 0$$

が得られる. これは a 以下の正の整数が有限個しかないことに反する.

したがって, ある番号 m が存在して, $q_{m+1} = 0$, $q_m = r_m$ となり,

$$\begin{aligned} a &= ((\cdots((r_m b + r_{m-1}) b + r_{m-2}) + \cdots) + r_1) + r_0 \\ &= r_m b^m + r_{m-1} b^{m-1} + \cdots + r_1 b + r_0, \\ &0 \leq r_i < b \quad (0 \leq i \leq m) \end{aligned}$$

となる. □

2　整数の整除

二つの整数の和, 差および積は整数である.
しかし, 二つの整数の商は必ずしも整数になるとは限らない.
$a, b \in \mathbb{Z}$ に対して, ある $q \in \mathbb{Z}$ が存在して

$$a = bq$$

が成り立つとき, a は b で**割り切れる**という. このことを記号で

$$b \mid a$$

と書く. またこのとき, a を b の**倍数**といい, b を a の**約数**という.

定理 2.1. *$a, b, c \in \mathbb{Z}^+$ について, 次の三つの条件が成り立つ:*

(i)　$a \mid a$.

(ii)　$a \mid b$, $b \mid a$ がともに成り立てば, $a = b$.

(iii)　$a \mid b$, $b \mid c$ がともに成り立てば, $a \mid c$.

証明.　(i)　$a = a \cdot 1$ より明らか.

(ii)　$a \mid b$ のとき, ある $q \in \mathbb{Z}^+$ が存在して $b = aq$ となる.
$q \geq 1$ より,

$$a \leq a + a(q-1) = aq = b.$$

同様にして $b \leq a$ もいえる.
したがって, $a \leq b$ と $b \leq a$ とがともに成り立つから, $a = b$.

(iii)　$a \mid b$ のとき, ある $q \in \mathbb{Z}^+$ が存在して $b = aq$ となる. 同様に, $b \mid c$ のとき, ある $q' \in \mathbb{Z}^+$ が存在して $c = bq'$ となる. よって,

$$c = bq' = aqq'.$$

$qq' \in \mathbb{Z}$ であるから, $c \mid a$. □

与えられた整数 $a_1, \ldots, a_n$ $(n \geq 2)$ に対して, これらをすべて割り切る整数のことを $a_1, \ldots, a_n$ の**公約数**という.
公約数 d が負でない整数であって, さらに, 条件

$$x \text{ を } a_1, \ldots, a_n \text{ の任意の約数とすれば, } x \mid d \text{ である.}$$

を満たすとき, d を $a_1, \ldots, a_n$ の**最大公約数**といい, 記号で

$$\gcd(a_1, \ldots, a_n)$$

と書く.

定理 2.2. $a_1, \ldots, a_n \in \mathbb{Z}$ とする.

$$d_2 = \gcd(a_1, a_2), \quad d_n = \gcd(d_{n-1}, a_n) \quad (n \geq 3),$$
$$d'_n = \gcd(a_1, a_2, \ldots, a_n) \quad (n \geq 2)$$

とおく. このとき,

$$d_n = d'_n \quad (n \geq 2)$$

が成り立つ.

証明. n に関する数学的帰納法によって証明する.
$d_2 = d'_2$ であるから, $n = 2$ のとき主張は正しい.
$n = k$ のとき, 主張が正しいと仮定すると,

$$d_{k+1} = \gcd(d_k, a_{k+1}) = \gcd(d'_k, a_{k+1}).$$

d'_{k+1} は $a_1, a_2, \ldots, a_k$ を割り切るから, d'_k を割り切る. さらに $d'_{k+1} \mid a_{k+1}$ より $d'_{k+1} \mid d_{k+1}$.
逆に, $d_{k+1} \mid d'_k$ より, d_{k+1} は $a_1, a_2, \ldots, a_k$ を割り切る. さらに $d_{k+1} \mid a_{k+1}$ より $d_{k+1} \mid d'_{k+1}$.
したがって, $d'_{k+1} \mid d_{k+1}$ かつ $d_{k+1} \mid d'_{k+1}$ より, $d_{k+1} = d'_{k+1}$. □

定理 2.3. $a, b, q, r \in \mathbb{Z}$ とする.

$$a = bq + r$$

ならば

$$\gcd(a, b) = \gcd(b, r)$$

が成り立つ.

証明. $d = \gcd(a, b)$, $d' = \gcd(b, r)$ とおく.
$r = a - bq$, $d \mid a$, $d \mid b$ より, $d \mid r$. ゆえに $d \mid d'$.
逆に, $a = bq + r$, $d' \mid b$, $d' \mid r$ より, $d' \mid a$. ゆえに $d' \mid d$.
したがって, $d \mid d'$ と $d' \mid d$ とから, $d = d'$ がいえる. □

系 2.3.1 (Euclid の互除法). $a, b \in \mathbb{Z}^+$ とし, $b < a$ とする.

$$r_0 = a, \quad r_1 = b$$

とおき, $n \geq 2$ に対して, $r_{n-1} > 0$ である限り, r_n を

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}$$

によって定義する.
このとき, ある番号 m が存在して

$$r_m = 0$$

となる. さらにこのとき

$$r_{m-1} = \gcd(a, b)$$

が成り立つ.

証明. まず, $r_m = 0$ となる番号 m が存在することを背理法で証明する.

$r_m = 0$ となる番号 m が存在しないと仮定すると, r_n の定め方から, 無限に続く減少列

$$a = r_0 > r_1 > r_2 > \cdots > r_{n-2} > r_{n-1} > r_n > \cdots > 0$$

が得られる. ところがこれは, a 以下の正の整数が有限個しかないことに反する.

したがって, $r_m = 0$ となる番号 m は存在する.

$r_m = 0$ となるとき, 上の定理を繰り返し用いれば,

$$\begin{aligned} r_{m-1} &= \gcd(r_{m-1},\, r_m) \\ &= \gcd(r_{m-2},\, r_{m-1}) \\ &= \cdots\cdots \\ &= \gcd(r_0,\, r_1) \\ &= \gcd(a,\, b) \end{aligned}$$

となる. □

$m \in \mathbb{Z}$ に対して, m の倍数全体からなる集合を $m\mathbb{Z}$ とおく:

$$m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}.$$

定理 2.4. $a_1, \ldots, a_n \in \mathbb{Z}$ とし,

$$I = \{a_1x_1 + \cdots + a_nx_n \mid x_i \in \mathbb{Z}\}$$

とおく. このとき, ある $d \in \mathbb{Z}^+$ が存在して,

$$I = d\mathbb{Z}$$

が成り立つ.

さらに, d は $a_1, \ldots, a_n$ の最大公約数である.

証明. I に属する正整数のうちで最小のものを d とする. このとき, $u_1, \ldots, u_n \in \mathbb{Z}$ が存在して

$$d = a_1u_1 + \cdots + a_nu_n$$

と書ける.

$I = d\mathbb{Z}$ を示せばよいが, $d\mathbb{Z} \subseteq I$ は明らかなので, $I \subseteq d\mathbb{Z}$ を示せば十分である.

$z \in I$ とする. ある $q, r \in \mathbb{Z}$ が存在して

$$z = dq + r, \quad 0 \leq r < d$$

となる. 適当な $x_1, \ldots, x_n \in \mathbb{Z}$ をとって

$$z = a_1x_1 + \cdots + a_nx_n$$

と書けば,

$$r = a_1(x_1 - u_1q_1) + \cdots + a_n(x_n - u_nq_n) \in I.$$

ところが, d の最小性により $r = 0$ でなければならない. ゆえに $I \in d\mathbb{Z}$.

$a_1, \ldots, a_n \in I = d\mathbb{Z}$ より, d は $a_1, \ldots, a_n$ の公約数である.
また, x を $a_1, \ldots, a_n$ の公約数とすれば,

$$x \mid (a_1u_1 + \cdots + a_nu_n) = d.$$

ゆえに d は $a_1, \ldots, a_n$ の最大公約数である. □

系 2.4.1. $a_1, \ldots, a_n$ の最大公約数を d とすれば, 適当な $u_1, \ldots, u_n$ によって

$$d = a_1u_1 + \cdots a_nu_n$$

と書ける.

証明. 主張は $d \in I$ と同値であるが, これは定理より明らかである. □

系 2.4.2. $a_1, \ldots, a_n, b \in \mathbb{Z}$ とし, $a_1, \ldots, a_n$ の最大公約数を d とする.
方程式

$$a_1x_1 + \cdots + a_nx_n = b$$

が整数解 $x_1, \ldots, x_n$ をもつための必要十分条件は, b が d で割り切れることである.

証明. 方程式が整数解をもつ $\iff b \in I \iff b \in d\mathbb{Z} \iff d \mid b.$ □

系 2.4.3. $m \in \mathbb{Z}^+$ とするとき,

$$\gcd(ma_1, \ldots, ma_n) = m \cdot \gcd(a_1, \ldots, a_n).$$

証明. $d = \gcd(a_1, \ldots, a_n)$, $d' = \gcd(ma_1, \ldots, ma_n)$ とおく.
適当な $u_1, \ldots, u_n \in \mathbb{Z}$ をとって

$$d = a_1u_1 + \cdots + a_nu_n$$

と書き, 両辺に m を掛けると,

$$md = (ma_1)u_1 + \cdots + (ma_n)u_n.$$

ゆえに $d' \mid md$.
逆に, 適当な $u_1', \ldots, u_n' \in \mathbb{Z}$ をとって

$$d' = (ma_1)u_1' + \cdots + (ma_n)u_n'$$

と書けば,

$$d' = m(a_1u_1' + \cdots + a_nu_n').$$

$a_1u_1' + \cdots + a_nu_n'$ は d で割り切れるから, $md \mid d'$. したがって $d' = md$. □

a, b を整数とする．$\gcd(a, b) = 1$ が成り立つとき，a と b とは**互いに素**であるという．

定理 2.5. $a, b, c \in \mathbb{Z}$ とし，$\gcd(a, b) = 1$ とする．このとき，$a \mid bc$ ならば $a \mid c$ である．

証明. $\gcd(a, b) = 1$ より，ある $x, y \in \mathbb{Z}$ が存在して

$$ax + by = 1.$$

両辺に c を掛ければ，

$$acx + bcy = c.$$

$a \mid bc$ であるから，この左辺は a の倍数である．ゆえに $a \mid c$. □

系 2.5.1. $a, b, c \in \mathbb{Z}$ とする．このとき

$$\gcd(a, b) = \gcd(a, c) = 1 \Longleftrightarrow \gcd(a, bc) = 1.$$

証明. ($\Rightarrow$) $\gcd(a, b) = \gcd(a, c) = 1$ を仮定して $\gcd(a, bc) = 1$ を証明する．

$d = \gcd(a, bc)$ とおくと，$d \mid a$, $d \mid bc$.

もし仮に $\gcd(d, b) > 1$ ならば，$d \mid a$ より $\gcd(a, b) > 1$ となる．これは $\gcd(a, b) = 1$ に反する．よって $\gcd(d, b) = 1$.

したがって上の定理より $d \mid c$.

ところが，$d \mid a$ より d は a, c の公約数である．仮定より $\gcd(a, c) = 1$ であったから，$d = 1$ でなければならない．

($\Leftarrow$) $\gcd(a, b) > 1$ ならば $\gcd(a, bc) > 1$ となることは明らかである．$\gcd(a, c) > 1$ ならば $\gcd(a, bc) > 1$ となることも同様に明らかである．よって，

$$\gcd(a, b) > 1 \text{ または } \gcd(a, c) > 1 \Longrightarrow \gcd(a, bc) > 1.$$

対偶をとれば

$$\gcd(a, bc) = 1 \Longrightarrow \gcd(a, b) = \gcd(a, c) = 1$$

となる． □

与えられた整数 $a_1, \ldots, a_n$ $(n \geq 2)$ に対して，これらすべての倍数であるような整数のことを $a_1, \ldots, a_n$ の**公倍数**という．

公倍数 l が負でない整数であって，さらに，条件

$$x \text{ を } a_1, \ldots, a_n \text{ の任意の倍数とすれば，} l \mid x \text{ である．}$$

を満たすとき，l を $a_1, \ldots, a_n$ の**最小公倍数**といい，記号で

$$\mathrm{lcm}(a_1, a_2, \ldots, a_n)$$

と書く．

定理 2.6. $a_1, \ldots, a_n \in \mathbb{Z}$ とする.

$$l_2 = \mathrm{lcm}(a_1, a_2), \quad l_n = \mathrm{lcm}(l_{n-1}, a_n) \quad (n \geq 3),$$
$$l'_n = \mathrm{lcm}(a_1, a_2, \ldots, a_n) \quad (n \geq 2)$$

とおく. このとき,

$$l_n = l'_n \quad (n \geq 2)$$

が成り立つ.

証明. n に関する数学的帰納法によって証明する.
$l_2 = l'_2$ であるから, $n = 2$ のとき主張は正しい.
$n = k$ のとき, 主張が正しいと仮定すると,

$$l_{k+1} = \mathrm{lcm}(l_k, a_{k+1}) = \mathrm{lcm}(l'_k, a_{k+1}).$$

$a_1, a_2, \ldots, a_k$ は l'_{k+1} を割り切るから, l'_k は l'_{k+1} を割り切る. さらに $a_{k+1} \mid l'_{k+1}$ より $l_{k+1} \mid l'_{k+1}$.
逆に, $l'_k \mid l_{k+1}$ より, $a_1, a_2, \ldots, a_k$ は l_{k+1} を割り切る. さらに $a_{k+1} \mid l_{k+1}$ より $l'_{k+1} \mid l_{k+1}$.
したがって, $l_{k+1} \mid l'_{k+1}$ かつ $l'_{k+1} \mid l_{k+1}$ より, $l_{k+1} = l'_{k+1}$. □

定理 2.7. $a, b \in \mathbb{Z}^+$ の最大公約数を d, 最小公倍数を l とする. このとき

$$ab = dl$$

が成り立つ.

証明. $a = a'd, b = b'd$ とおく. このとき

$$\gcd(a', b') = \frac{\gcd(a, b)}{d} = 1.$$

l は a の倍数であるから, ある $k \in \mathbb{Z}^+$ が存在して

$$l = ak = a'kd.$$

l は $b = b'd$ の倍数でもあるから, $d \neq 0$ より $b' \mid a'k$ が得られる. $\gcd(a', b') = 1$ であるから, $b' \mid k$ である. したがって, ある $t \in \mathbb{Z}^+$ が存在して $k = b't$. このとき,

$$l = ak = ab't = a'db't = a'bt.$$

ゆえに,

$$\frac{l}{t} = ab_1 = ba_1.$$

したがって l/t は a, b の公倍数である. l の最小性より $t = 1$ でなければならない. ゆえに $ab = ld$ が得られる. □

3　素因数分解

$n \in \mathbb{Z}$, $n > 1$ とする.

n の正の約数が 1 と n だけであるとき, n は**素数**であるといい, そうでないとき, n は**合成数**であるという.

素数全体からなる集合を $\mathbb{P}$ とおく.

定理 3.1.　$p \in \mathbb{P}$, a, $b \in \mathbb{Z}$ とする. このとき

$$p \mid ab \Longrightarrow p \mid a \text{ または } p \mid b.$$

証明.　任意の $n \in \mathbb{Z}^+$ に対して,

$$\gcd(p, n) = 1 \Longleftrightarrow p \nmid n$$

が成り立つことに注意する.

$$\gcd(p, a) = \gcd(p, b) = 1 \Longrightarrow \gcd(p, ab) = 1$$

なので

$$p \nmid a \text{ かつ } p \nmid b \Longrightarrow p \nmid ab.$$

対偶をとれば

$$p \mid ab \Longrightarrow p \mid a \text{ または } p \mid b.$$

□

系 3.1.1.　$p \in \mathbb{P}$, a_1, ..., $a_n \in \mathbb{Z}^+$ とする.

このとき, $p \mid (a_1 \cdots a_n)$ ならば, p はいずれかの a_i を割り切る.

証明.　n に関する数学的帰納法によって証明する.

$n = 2$ のときは上の定理より明らか.

$n = k$ のとき主張が成り立つと仮定する.

$p \mid (a_1 \cdots a_k a_{k+1})$ ならば, 上の定理より, $p \mid (a_1 \cdots a_k)$ または $p \mid a_{k+1}$ である.

$p \mid a_{k+1}$ ならば, これ以上すべきことはない.

$p \nmid a_{k+1}$ ならば $p \mid (a_1 \cdots a_k)$ である. 帰納法の仮定により p は a_1, ... a_k のうちのいずれかを割り切る.

したがって, p は a_1, ... a_k, a_{k+1} のいずれかを割り切る.

以上より, すべての n について系の主張が成り立つことが示された.　□

定理 3.2.　$n \in \mathbb{Z}$, $n > 1$ とする.

n は素数の積として表せる. しかもその表し方は積の順序を除いて一意的である.

証明. まず, n が素数の積として表せることを, n に関する数学的帰納法によって証明する.

$n = 2$ のとき, 2 は素数である.

$2 \leq k \leq n$ であるようなすべての $k \in \mathbb{Z}$ について, k が素数の積として表せると仮定する.

$n+1$ が素数ならば, これ以上すべきことはない.

$n+1$ が合成数ならば, 適当な $l, m \in \mathbb{Z}^+$ をとって

$$n+1 = lm, \quad 2 \leq l < n+1, \quad 2 \leq m < n+1$$

と書ける. 帰納法の仮定から, l, m はそれぞれ素数の積で表せる. したがって $n+1$ も素数の積で表せる.

以上より, すべての $n \in \mathbb{Z}$, $n > 1$ について, n が素数の積として表せることが示された.

次に, 表し方の一意性を証明する.

上に述べたことから, $n \in \mathbb{Z}$, $n > 1$ なる任意の n に対して, ある $k \in \mathbb{Z}^+$ が存在して, n は k 個の素数の積で表すことができる:

$$n = p_1 p_2 \cdots p_k.$$

そこで, k に関する数学的帰納法によって, 表し方の一意性を証明する.

n が素数のとき, $n = p_1 p_2 \cdots p_k$ (p_i は素数) と書けたとすると, $k = 1$, $p_1 = n$ でなければならない.

n が少なくとも k 個の素数の積で書けるならば, 表し方は一意的であると仮定する.

$$n = p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_l, \quad p_i, q_j \text{ は素数}$$

のとき, 帰納法の仮定から $k+1 \leq l$ である. $p_1 \mid (q_1 q_2 \cdots q_l)$ より, ある i について $p_1 \mid q_i$. 積の順序を考えなければ, $p_1 \mid q_1$ としてもよい. q_1 は素数だから, $p_1 = q_1$. よって

$$\frac{n}{p_1} = p_2 \cdots p_{k+1} = q_2 \cdots q_l.$$

帰納法の仮定より, $l = k+1$, $p_i = q_i$ でなければならない.

以上より, すべての k に関して, 表し方の一意性が証明された.

したがって, すべての $n \in \mathbb{Z}$, $n > 1$ について, n の素数の積での表し方は一意的である. □

整数 n ($n > 1$) を素数の積として表すことを, n の**素因数分解**という.

また, n を割り切る素数を n の**素因数**という.

定理 3.3. 素数は無限に存在する.

証明. 背理法により証明する.

いま, 素数が有限個しかないと仮定し, p_1, p_2, ..., p_k が素数のすべてであるとする.

$$n = p_1 p_2 \cdots p_k + 1$$

とおく.

n は素因数分解できる. よって n は素数の約数を持つ.

ところが, p_1, p_2, ..., p_k はすべて n を割らない. これは n が素数の約数を持つことに反する.

したがって素数は無限に存在する. □

4　法 m に関する剰余類

$a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ とする.

$$m \mid (a-b)$$

となるとき, a と b とは m を法として**合同**であるといい, 記号で

$$a \equiv b \pmod{m}$$

と書く.

また, $\equiv$ の入った式を**合同式**という.

例えば,

$$3 \equiv 1 \pmod{2}$$

や, 未知数 x の入った式

$$7x \equiv 3 \pmod{10}$$

は合同式である.

定理 4.1. $a, b, c \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ とする.

(i) $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$.

(iii) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ がともに成り立てば, $a \equiv c \pmod{m}$.

証明. (i) 任意の $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ に対して,

$$a - a = 0 = m \cdot 0.$$

よって $m \mid (a-a)$. したがって $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m}$ のとき, ある $t \in \mathbb{Z}$ が存在して

$$a - b = mt.$$

このとき

$$b - a = m(-t).$$

ゆえに $m \mid (b-a)$. したがって $b \equiv a \pmod{m}$.

(iii) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ がともに成り立つとき, ある $s, t \in \mathbb{Z}$ が存在して

$$a - b = ms, \quad b - c = mt.$$

このとき

$$a - c = (a-b) + (b-c) = m(s+t).$$

ゆえに $m \mid (a-c)$. したがって $a \equiv c \pmod{m}$. □

$m \in \mathbb{Z}^+$ を一つ固定する. $a \in \mathbb{Z}^+$ に対して

$$C(a) = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

とおく. $C(a)$ を法 m に関する**剰余類**という.
またこのとき, a を剰余類 $C(a)$ の**代表元**という.

定理 4.2. *$a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ とする. $C(*)$ は法 m に関する剰余類を表すものとする.*

(i) $a \equiv b \pmod{m} \Longrightarrow C(a) = C(b)$.

(ii) $a \not\equiv b \pmod{m} \Longrightarrow C(a) \cap C(b) = \emptyset$.

証明. (i) $x \in C(a)$ とすれば, $x \equiv a \pmod{m}$. これと $a \equiv b \pmod{m}$ という仮定から, $x \equiv b \pmod{m}$ がいえる. ゆえに $x \in C(b)$. したがって $C(a) \subseteq C(b)$.
同様に $C(b) \subseteq C(a)$ もいえる. よって $C(a) = C(b)$.

(ii) $C(a) \cap C(b) \neq \emptyset$ と仮定すると, ある $x \in \mathbb{Z}$ が存在して,

$$x \in C(a) \text{ かつ } x \in C(b).$$

すなわち,

$$x \equiv a \pmod{m} \text{ かつ } x \equiv b \pmod{m}.$$

このことから

$$a \equiv b \pmod{m}$$

が導かれる. したがって

$$C(a) \cap C(b) \neq \emptyset \Longrightarrow a \equiv b \pmod{m}.$$

あとは, この対偶をとればよい. □

$m \in \mathbb{Z}^+$ に対して, 法 m に関する剰余類の全体からなる集合を $\mathbb{Z}/m\mathbb{Z}$ とおく:

$$\mathbb{Z}/m\mathbb{Z} = \{C(a) \mid a \in \mathbb{Z}\} = \{C(0), C(1), \ldots, C(m-1)\}.$$

$\mathbb{Z}/m\mathbb{Z}$ は m 個の元からなる有限集合である.

定理 4.3. *$a, a', b, b' \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ とする.*

$$a \equiv a' \pmod{m}, \quad b \equiv b' \pmod{m}$$

がともに成り立つとき, 次のことが成り立つ:

(i) $a + b \equiv a' + b' \pmod{m}$.

(ii) $a - b \equiv a' - b' \pmod{m}$.

(iii) $ab \equiv a'b' \pmod{m}$.

証明. (i) $(a+b)-(a'+b')=(a-a')+(b-b')$ よりわかる.

(ii) $(a-b)-(a'-b')=(a-a')-(b-b')$ よりわかる.

(ii) $ab-a'b'=a(b-b')+b'(a-a')$ よりわかる. □

$\mathbb{Z}/m\mathbb{Z}$ の二つの元 $C(a)$ と $C(b)$ との和 $C(a)+C(b)$, 差 $C(a)-C(b)$, 積 $C(a)C(b)$ を次のように定義する:

$$C(a)+C(b)=C(a+b),\quad C(a)-C(b)=c(a-b),\quad C(a)C(b)=C(ab).$$

この定義は, 剰余類の代表元の選び方に依存しない.

定理 4.4. $a,\ b,\ c\in\mathbb{Z},\ c\neq 0,\ m\in\mathbb{Z}^+$ とする.

$$ca\equiv cb\pmod{m}$$

が成り立つとき, $d=\gcd(c,\ m)$ とおけば

$$a\equiv b\pmod{\frac{m}{d}}$$

が成り立つ.

証明. $ca\equiv cb\pmod{m}$ のとき, ある $t\in\mathbb{Z}$ が存在して,

$$c(a-b)=mt.$$

$c=dc',\ m=dm'$ とおくと,

$$c'(a-b)=m't.$$

よって

$$m'\mid c'(a-b).$$

$\gcd(c',\ m')=1$ であるから, $m'\mid(a-b)$ でなければならない. ゆえに

$$a\equiv b\pmod{m'}.$$

□

法 m に関する剰余類は m 個ある.

その各々から 1 つずつ代表元をとって作った m 個の整数の組を, 法 m に関する**完全剰余系**という.

例えば $m=7$ のとき,

$$0,\quad 1,\quad 2,\quad 3,\quad 4,\quad 5,\quad 6$$

や

$$-3,\quad -2,\quad -1,\quad 0,\quad 1,\quad 2,\quad 3$$

は完全剰余系である.

一般に, 完全剰余系の選び方は無数にある.

定理 4.5. $m \in \mathbb{Z}^+$, $c \in \mathbb{Z}$ とし, $\gcd(c, m) = 1$ とする. $a_1, a_2, \ldots, a_m$ を法 m に関する完全剰余系とすれば, $ca_1, ca_2, \ldots, ca_m$ もまた法 m に関する完全剰余系である.

証明. ある番号 i, j が存在して

$$ca_i \equiv ca_j \pmod{m}$$

であるとする. 仮定 $\gcd(c, m) = 1$ より,

$$a_i \equiv a_j \pmod{m}.$$

したがって,

$$C(a_i) = C(a_j).$$

完全剰余系の定義の仕方から, $i = j$ でなければならない.

よって, $ca_1, ca_2, \ldots, ca_m$ は別々の剰余類に属する. □

定理 4.6. $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ とする. $d = \gcd(a, m)$ とおく.

合同式

$$ax \equiv b \pmod{m}$$

が整数解を持つための必要十分条件は, d が b を割り切ることである.

さらに, m を法として考えたとき, 上の合同式の整数解の個数は d である.

証明. 上の合同式が整数解 x_0 を持つと仮定すると, ある $t \in \mathbb{Z}$ が存在して

$$ax - b = mt.$$

ゆえに

$$d \mid (ax - mt) = b.$$

逆に, d が b を割り切ると仮定すると, 方程式

$$ax + my = b$$

は解 $x, y \in \mathbb{Z}$ を持つ. このとき,

$$ax \equiv b \pmod{m}$$

となっている. よって, 与えられた合同式は解 $x \in \mathbb{Z}$ を持つ.

さらに, $x_0 \in \mathbb{Z}$ を与えられた合同式の解の一つとし,

$$a = a'd, \quad m = m'd, \quad b = b'd$$

とおく. 与えられた合同式の任意の解 $x \in \mathbb{Z}$ に対して,

$$a'x \equiv b' \pmod{m'}, \quad a'x_0 \equiv b' \pmod{m'}$$

であるから,

$$a'x \equiv a'x_0 \pmod{m'}.$$

$\gcd(a', m') = 1$ であるから,

$$x \equiv x_0 \pmod{m'}.$$

したがって, x は m を法として

$$x_0, \quad x_0 + m', \quad x_0 + 2 \cdot m', \quad \ldots, \quad x_0 + (d-1) \cdot m'$$

の d 個のうちのいずれかと合同である.

逆に, これらの d 個はすべて与えられた合同式の解である.

したがって, 与えられた合同式の解は m を法としてちょうど d 個ある. □

定理 4.7. $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{Z}^+$ とする. 連立合同式

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}$$

が整数解を持つための必要十分条件は, $d = \gcd(m_1, m_2)$ とおくとき,

$$a_1 \equiv a_2 \pmod{d}$$

が成り立つことである.

さらに, 上の連立合同式が整数解を持つとき, その解は m_1, m_2 の最小公倍数を法として一意的である.

証明. 上の連立合同式が解 $x \in \mathbb{Z}$ を持つとする:

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}.$$

m_1, m_2 はともに d で割り切れるから,

$$x \equiv a_1 \pmod{d}, \quad x \equiv a_2 \pmod{d}.$$

ゆえに

$$a_1 \equiv a_2 \pmod{d}.$$

逆に, $a_1 \equiv a_2 \pmod{d}$ が成り立つと仮定すると, 合同式

$$m_1 t \equiv a_2 - a_1 \pmod{m_2}$$

は解 $t \in \mathbb{Z}$ を持つ. このとき,

$$x = a_1 + m_1 t$$

とおけば,

$$x \equiv a_1 \pmod{d}, \quad x \equiv a_2 \pmod{d}$$

となる.

最後に, 解の一意性を証明する.

もし, $x_1, x_2 \in \mathbb{Z}$ がともに与えられた連立合同式の解であるとすると,

$$\begin{aligned} x_1 &\equiv a_1 \pmod{m_1}, \quad x_1 \equiv a_2 \pmod{m_2}, \\ x_2 &\equiv a_2 \pmod{m_1}, \quad x_2 \equiv a_2 \pmod{m_2}. \end{aligned}$$

よって,

$$x_1 \equiv x_2 \pmod{m_1}, \quad x_1 \equiv x_2 \pmod{m_2}.$$

言い換えると,

$$m_1 \mid (x_1 - x_2), \quad m_2 \mid (x_1 - x_2).$$

したがって, $l = \mathrm{lcm}(m_1, m_2)$ とおくと, 最小公倍数の性質から,

$$l \mid (x_1 - x_2).$$

すなわち,

$$x_1 \equiv x_2 \pmod{l}.$$

□

系 4.7.1 (中国剰余定理). $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, $m_1, m_2, \ldots, m_n \in \mathbb{Z}^+$, $n \geq 2$ とする.
$i \neq j$ のとき, $\gcd(m_i, m_j) = 1$ と仮定する.
このとき, 連立合同式

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots, \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

は, 積 $m_1 m_2 \cdots m_n$ を法としてただ一つの整数解を持つ.

証明. 合同式の個数 n に関する数学的帰納法によって証明する.
$n = 2$ のときは, 上の定理より明らかである.
$n = k$ のとき, 主張が正しいと仮定すると, 連立合同式

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots, \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

は解 $b_0 \in \mathbb{Z}$ を持ち, すべての整数解 x は

$$x \equiv b_0 \pmod{m_1 m_2 \cdots m_k}$$

を満たす. ここで, $i \neq j$ のとき $\gcd(m_i, m_j) = 1$ という仮定から, $m_1, m_2, \ldots, m_k$ の最小公倍数が積 $m_1 m_2 \cdots m_k$ になることに注意する.
さらに合同式 $x \equiv a_{k+1} \pmod{m_{k+1}}$ を追加したとき, $k+1$ 個の合同式

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots, \\ x &\equiv a_k \pmod{m_k}, \\ x &\equiv a_{k+1} \pmod{m_{k+1}} \end{aligned}$$

の整数解 x は, 連立合同式

$$x \equiv b_0 \pmod{m_1 m_2 \cdots m_k}, \quad x \equiv a_{k+1} \pmod{m_{k+1}}$$

の解である. そして上の定理より, この連立方程式は解 $b_0' \in \mathbb{Z}$ を持ち, すべての整数解 x' は

$$x' \equiv b_0' \pmod{m_1 m_2 \cdots m_k m_{k+1}}$$

を満たす. したがって $k+1$ のときも主張は正しい. □

5 Euler の関数

整数 1, 2, ..., n のうち n と互いに素なものの個数を $\varphi(n)$ と書く．これにより定まる $\mathbb{Z}^+$ から $\mathbb{Z}^+$ 自身への写像 φ を **Euler の関数**という.

定理 5.1. n が r 個の異なる素数 $p_1, p_2, \ldots, p_r$ で割れるとき，1, 2, ..., n の中で $p_1, p_2, \ldots, p_r$ と互いに素なものの個数を $\varphi_r(n)$ とすれば

$$\varphi_r(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

が成り立つ.

証明. r に関する数学的帰納法により証明する.

$r = 1$ のとき．1, 2, ..., n の中で p_1 と互いに素でないものは p_1 の倍数

$$p_1, \quad 2p_1, \quad \ldots, \quad \frac{n}{p_1} \cdot p_1$$

であり，個数は n/p_1 である．これらを除いたものが p_1 と互いに素になる．よって

$$\varphi_1(n) = n - \frac{n}{p_1} = n\left(1 - \frac{1}{p_1}\right).$$

r まで正しいとして，$r+1$ の場合を考える.

そのために, $\varphi_r(n) - \varphi_{r+1}(n)$ の値を考える．この値は $p_1, p_2, \ldots, p_r$ と互いに素な数の個数から $p_1, p_2, \ldots, p_{r+1}$ と互いに素な数の個数を引いたものである.

つまり, $\varphi_r(n) - \varphi_{r+1}(n)$ は $p_1, p_2, \ldots, p_r$ と互いに素であって，p_{r+1} で割り切れる数の個数である.

p_{r+1} で割り切れる数は

$$p_{r+1}, \quad 2p_{r+1}, \quad \ldots, \quad \frac{n}{p_{r+1}} \cdot p_{r+1}$$

である．この中で $p_1, p_2, \ldots, p_r$ と互いに素な数の個数は

$$1, \quad 2, \quad \ldots, \quad \frac{n}{p_{r+1}} \tag{1}$$

の中で $p_1, p_2, \ldots, p_r$ と互いに素なものの個数に等しい．なぜなら，p_{r+1} で割っても $p_1, p_2, \ldots, p_r$ と互いに素か否かという関係は変わらないからである.

(1) の中で $p_1, p_2, \ldots, p_r$ と互いに素なものの個数は $\varphi_r(n/p_{r+1})$ である．
n/p_{r+1} が $p_1, p_2, \ldots, p_r$ で割り切れることに注意すると，帰納法の仮定から

$$\varphi_r\left(\frac{n}{p_{r+1}}\right) = \frac{n}{p_{r+1}} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \tag{2}$$

となる．(2) は $\varphi_r(n) - \varphi_{r+1}(n)$ に等しいから

$$\begin{aligned}
\varphi_{r+1}(n) &= \varphi_r(n) - (\varphi_r(n) - \varphi_{r+1}(n)) \\
&= \varphi_r(n) - \varphi_r\left(\frac{n}{p_{r+1}}\right) \\
&= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_r}\right) - \frac{n}{p_{r+1}} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\
&= n \prod_{i=1}^{r+1} \left(1 - \frac{1}{p_i}\right).
\end{aligned}$$

したがって $r+1$ の場合も正しい． □

系 5.1.1. $n \in \mathbb{Z}^+$ とする．このとき

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

が成り立つ．ただし p は n の素因数全体を動く．

証明. n の素因数の個数を r とする．n と互いに素な整数とは，n のどの素因数とも互いに素な整数のことであるから，$\varphi(n) = \varphi_r(n)$．したがって定理 5.1 より上の等式は正しい． □

系 5.1.2. $p \in \mathbb{P}$，$e \in \mathbb{Z}^+$ とする．このとき

$$\varphi(p^e) = p^{e-1}(p-1).$$

証明. 系 5.1.1 において，n の素因数が一つしかない場合である． □

系 5.1.3. $m, n \in \mathbb{Z}^+$ とし, $\gcd(m\,n) = 1$ とする．このとき

$$\varphi(m)\varphi(n) = \varphi(mn).$$

証明. 系 5.1.1 により

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right), \qquad \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

と表せる．ただし p は素数である．

$\gcd(m, n) = 1$ より m の素因数と n の素因数とで一致するものはないから,

$$\begin{aligned}\varphi(m)\varphi(n) &= m\prod_{p|m}\left(1-\frac{1}{p}\right)\cdot n\prod_{p|n}\left(1-\frac{1}{p}\right)\\ &= mn\prod_{p|mn}\left(1-\frac{1}{p}\right)\\ &= \varphi(mn)\end{aligned}$$

となる. □

定理 5.2. n を正の整数とする. このとき

$$\sum_{d|n}\varphi(d) = n$$

が成り立つ. ただし d は n の正の約数全体を動く.

証明. 1, 2, ..., n のどの数も n との最大公約数が n の約数になる. ゆえに,

$$N_d = \{x \in \mathbb{Z}^+ \mid 1 \le x \le n,\ \gcd(x, n) = d\}$$

とおけば,

$$\{1, 2, \ldots, n\} = \bigcup_{d|n} N_d \quad (\text{集合の直和}) \tag{3}$$

となる. ただし, d は n の正の約数全体を動く.

n の正の約数 d を一つ固定する. $n = d'd$ とおくと, N_d の元 x は

$$x = x'd, \quad 1 \le x' \le d', \quad \gcd(x', d') = 1$$

と書ける.

x' は,

$$d, \quad 2d, \quad 3d, \quad \ldots, \quad d'd = n$$

を d で割った

$$1, \quad 2, \quad 3, \quad \ldots, \quad d'$$

のうち, d' と互いに素になるもの全体を動く.

したがって, n の各々の約数 d に対して x' は $\varphi(d')$ 個ある.

一方,

$$N_d = \{x'd \mid 1 \le x' \le d',\ \gcd(x', d') = 1\}$$

であるから, N_d の元 x の個数もまた $\varphi(d')$ である.

ゆえに, (3) において, 集合の個数を比較すれば,

$$n = \sum_{d|n}\varphi(d')$$

が得られる.

$$N = \{d \in \mathbb{Z}^+ \mid d \text{ は } m \text{ の約数 }\},$$
$$N' = \left\{\frac{n}{d} \in \mathbb{Z}^+ \mid d \text{ は } m \text{ の約数}\right\}$$

とおくと, $N = N'$ が成り立つ. したがって,

$$\sum_{d|n} \varphi(d) = \sum_{d \in N} \varphi(d) = \sum_{d' \in N'} \varphi(d') = \sum_{d|n} \varphi(d') = n.$$

□

$m \in \mathbb{Z}^+$ を一つ固定する.

法 m に関する剰余類 $C(a)$ $(a \in \mathbb{Z})$ について, $C(a)$ のある一つの元が m と互いに素ならば, $C(a)$ に属するすべての元は m と互いに素である.

代表元 a が m と互いに素であるとき, 剰余類 $C(a)$ を**既約剰余類**という.

各々の既約剰余類からそれぞれ一つずつ代表元をとって作った $\varphi(m)$ 個の整数の組を, 法 m に関する**既約剰余系**という.

完全剰余系から, m と互いに素なものだけを選んで並べたものは既約剰余系になる.

定理 5.3. $m \in \mathbb{Z}^+$, $c \in \mathbb{Z}$ とし, $\gcd(c, m) = 1$ とする. $a_1, a_2, \ldots, a_r$ $(r = \varphi(m))$ を法 m に関する既約剰余系とすれば, $ca_1, ca_2, \ldots, ca_r$ もまた法 m に関する既約剰余系である.

証明. ある番号 i, j が存在して

$$ca_i \equiv ca_j \pmod{m}$$

であるとすれば,

$$m \mid c(a_i - a_j).$$

仮定 $\gcd(c, m) = 1$ より,

$$m \mid (a_i - a_j).$$

ゆえに

$$a_i \equiv a_j \pmod{m}.$$

したがって

$$C(a_i) = C(a_j).$$

既約剰余系の定義の仕方から, $i = j$ でなければならない.

よって, $ca_1, ca_2, \ldots, ca_r$ は別々の剰余類に属する.

仮定より,

$$\gcd(c, m) = 1, \quad \gcd(a_1, m) = \cdots = \gcd(a_r, m) = 1.$$

ゆえに,

$$\gcd(ca_1, m) = \cdots = \gcd(ca_r, m) = 1.$$

すなわち, $ca_1, ca_2, \ldots, ca_r$ はすべて既約剰余類の代表元である. □

定理 5.4 (Euler の定理). $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ とし, $\gcd(a, m) = 1$ とする. このとき,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

が成り立つ.

証明. $x_1, \ldots, x_r$ $(r = \varphi(m))$ を法 m に関する既約剰余系とする. このとき, $ax_1, \ldots, ax_r$ もまた法 m に関する既約剰余系である.

したがって, $x_1, \ldots, x_r$ の順序を適当に並べかえたものを $x_{i_1}, \ldots, x_{i_r}$ として,

$$\begin{aligned} ax_1 &\equiv x_{i_1} \pmod{m}, \\ ax_2 &\equiv x_{i_2} \pmod{m}, \\ &\cdots\cdots, \\ ax_r &\equiv x_{i_r} \pmod{m} \end{aligned}$$

となるようにできる. これら r 個の合同式の両辺をそれぞれ掛け合わせれば,

$$a^r x_1 \cdots x_r \equiv x_{i_1} \cdots x_{i_r} = x_1 \cdots x_r \pmod{m}.$$

$x_1 \cdots x_r$ と m とは互いに素だから, 両辺を $x_1 \cdots x_r$ で割れば,

$$a^r \equiv 1 \pmod{m}$$

が得られる. □

定理 5.5 (Fermat の定理). $p \in \mathbb{P}$, $a \in \mathbb{Z}$ とし, $\gcd(a, p) = 1$ とする. このとき,

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

が成り立つ.

証明. $\varphi(p) = p - 1$ より明らか. □

6 Legendre 記号

$p \in \mathbb{P} \setminus \{2\}$, $a \in \mathbb{Z}$ とする.
合同式

$$x^2 \equiv a \pmod{p}$$

が解を持つとき, a を p の**平方剰余**といい, 解を持たないとき**平方非剰余**という. $\gcd(a, p) = 1$ であるとき,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ が平方剰余のとき} \\ -1, & a \text{ が平方非剰余のとき} \end{cases}$$

と定める. (a/p) を **Legendre 記号**と呼ぶ.

定理 6.1. $p \in \mathbb{P} \setminus \{2\}$，$a,\, b \in \mathbb{Z}$ とし，$\gcd(a,\, p) = \gcd(b,\, p) = 1$ とする．このとき

$$a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

が成り立つ．

特に，p の平方剰余と合同なものはまた平方剰余であり，平方非剰余と合同なものはまた平方非剰余である．

証明. $a \equiv b \pmod{p}$ ならば，合同式 $x^2 \equiv a \pmod{p}$ が解を持つことと合同式 $x^2 \equiv b \pmod{p}$ が解を持つこととは同値である． □

p の平方剰余は $1,\, 2,\, \ldots,\, p-1$ の平方のいずれかと p を法として合同な整数である．

$$x^2 \equiv (p-x)^2 \pmod{p}$$

だから，p の平方剰余はすべて $1,\, 2,\, \ldots,\, (p-1)/2$ の平方のいずれかに p を法として合同である．

$x,\, y \in \mathbb{Z}$ に対して，

$$\begin{aligned} x^2 \equiv y^2 \pmod{p} &\Longrightarrow (x-y)(x+y) \equiv 0 \pmod{p} \\ &\Longrightarrow x-y \equiv 0 \pmod{p} \text{ または } x+y \equiv 0 \pmod{p}. \end{aligned}$$

$x,\, y$ の範囲を考慮して，$1 \leq x \leq (p-1)/2$, $1 \leq y \leq (p-1)/2$ とすれば,

$$x^2 \equiv y^2 \pmod{p} \Longrightarrow x \equiv y \pmod{p} \Longrightarrow x = y$$

となる．ゆえに $1,\, 2,\, \ldots,\, (p-1)/2$ の平方はどの 2 つも p を法として合同ではない．

したがって, $1,\, 2,\, \ldots,\, p-1$ のうち，p の平方剰余，平方非剰余はそれぞれ $(p-1)/2$ 個ずつある．

定理 6.2 (Euler の規準). $p \in \mathbb{P} \setminus \{2\}$，$a \in \mathbb{Z}$ とし，$\gcd(a,\, p) = 1$ とする．このとき

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

が成り立つ．

証明. $1 \leq x \leq p-1$ となる x に対し，$\gcd(x,\, p) = 1$ であるから,

$$xy \equiv a \pmod{p}, \quad 1 \leq y \leq p-1$$

となる $y \in \mathbb{Z}$ がただ一つ存在する．この y を a に関する x の配偶と呼ぶことにする．このとき,

$$a \text{ が平方剰余} \Longleftrightarrow x \in \mathbb{Z} \text{ が存在して, } x \text{ 自身が } a \text{ に関する } x \text{ の配偶になる.}$$

と言いかえることができる．

a が平方剰余のとき，合同式 $x^2 \equiv a \pmod{p}$ の解を x_0 $(1 \leq x_0 \leq p-1)$ とする．

$$(p-x_0)^2 = p^2 - 2px_0 + x_0^2 \equiv x_0^2 \equiv a \pmod{p}$$

であるから，$p - x_0$ も解となり，$1 \leq p - x_0 \leq p-1$ である．

p は奇数だから, $p - x_0 \neq x_0$ である.

よって, 1 から $p-1$ までの中で x_0 と $p - x_0$ の 2 つだけが自分自身を配偶に持ち，他は自分と異なる配偶を持つ.

1 から $p-1$ までを並び替えて

$$x_0, \quad p - x_0, \quad x_1, \quad \ldots, \quad x_{(p-3)/2}, \quad y_1, \quad y_2, \quad \ldots, \quad y_{(p-3)/2}$$

とする．ただし y_i は a に関する x_i の配偶である．すると,

$$\begin{aligned}(p-1)! &= x_0(p-x_0)(x_1 \cdot y_1)(x_2 \cdot y_2) \cdots (x_{(p-3)/2} \cdot y_{(p-3)/2}) \\ &\equiv x_0(-x_0) \cdot a \cdot \cdots \cdot a \\ &\equiv -a^{\frac{p-1}{2}} \pmod{p}.\end{aligned}$$

特に $a = 1$ のとき，a は平方剰余であるから

$$(p-1)! \equiv -1 \pmod{p} \tag{4}$$

となる．この式を再び上の式に代入すると

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

を得る.

a が平方非剰余のときは，自分自身を配偶に持つ整数はない. そこで, 1 から $p-1$ までの数を並べ替えて

$$x_1, \quad x_2, \quad \ldots, \quad x_{(p-1)/2}, \quad y_1, \quad y_2, \quad \ldots, \quad y_{(p-1)/2}$$

とおく．ただし y_i は a に関する x_i の配偶である．このとき,

$$\begin{aligned}(p-1)! &= (x_1 \cdot y_1)(x_2 \cdot y_2) \cdots (x_{(p-1)/2} \cdot y_{(p-1)/2}) \\ &\equiv a \cdot \cdots \cdot a \pmod{p} \\ &\equiv a^{\frac{p-1}{2}} \pmod{p}\end{aligned}$$

となる．よって (4) より

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

が得られる. □

系 6.2.1 (Wilson の定理). $n \in \mathbb{Z}$, $n > 1$ とするとき

$$n \text{ は素数である} \iff (n-1)! \equiv -1 \pmod{n}.$$

証明. ($\Rightarrow$) n が奇素数の場合は，Euler の規準を証明する途中で既に示されている．$n = 2$ のときは明らか.

($\Leftarrow$) n が合成数であるとすると，ある $b, c \in \mathbb{Z}$ によって

$$n = bc, \qquad 1 < b < n$$

と表せる．b は $(n-1)!$ の約数である．よって b は $(n-1)! + 1$ の約数ではない．n は b の倍数だから $(n-1)! + 1$ を割り切ることができない. □

系 6.2.2. $p \in \mathbb{P} \setminus \{2\}$，$a,\ b \in \mathbb{Z}$ とし，$\gcd(a,\ p) = \gcd(b,\ p) = 1$ とする．このとき

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

証明. Euler の規準により

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

両辺とも ± 1 であり，$1 \not\equiv -1 \pmod{p}$ であるから等号が成り立つ． □

定理 6.3 (Gauss の補題). $p \in \mathbb{P} \setminus \{2\}$，$a \in \mathbb{Z}$ とし，$\gcd(a,\ p) = 1$ とする．このとき

$$1 \cdot a, \quad 2 \cdot a, \quad \ldots, \quad \frac{p-1}{2} \cdot a$$

を p で割ったときの剰余の中に $p/2$ よりも大きいものが n 個あったとすれば

$$\left(\frac{a}{p}\right) = (-1)^n.$$

証明.

$$\pm 1, \quad \pm 2, \quad \ldots, \quad \pm\frac{p-1}{2}$$

の $p-1$ 個の整数は法 p に関する既約剰余系である．

$\gcd(a,\ p) = 1$ だから，

$$\pm 1 \cdot a, \quad \pm 2 \cdot a, \quad \ldots, \quad \pm\frac{p-1}{2} \cdot a$$

もまた法 p に関する既約剰余系である．

xa $(1 \leq x \leq (p-1)/2)$ を p で割ったときの剰余が $p/2$ より大きいということは，xa が -1, -2, …, $-(p-1)/2$ のいずれかと p を法として合同なことと同値である．

そこで, $1 \cdot a$, $2 \cdot a$, …, $(p-1)/2 \cdot a$ のうち -1, -2, …, $-(p-1)/2$ のいずれかと合同なものの個数を n とする．このとき,

$$(1 \cdot a) \cdot (2 \cdot a) \cdot \cdots \cdot \left(\frac{p-1}{2} \cdot a\right) \equiv (-1)^n \cdot 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} \pmod{p}.$$

$1 \cdot 2 \cdot \cdots \cdot (p-1)/2$ と p とは互いに素であるから，両辺を $1 \cdot 2 \cdot \cdots \cdot (p-1)/2$ で割ると

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

Euler の規準により,

$$\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$$

となる． □

系 6.3.1 (第一補充法則). $p \in \mathbb{P} \setminus \{2\}$ とするとき,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

証明. Gauss の補題における $a = -1$ の場合を考える.
$-1, -2, \ldots, -(p-1)/2$ はすべて p で割ったときの剰余が $p/2$ 以上になる.
よって, Gauss の補題により求める式が得られる. □

系 6.3.2 (第二補充法則). $p \in \mathbb{P} \setminus \{2\}$ とするとき,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

証明. Gauss の補題における $a = 2$ の場合を考える.

$$1 \cdot 2, \quad 2 \cdot 2, \quad \ldots, \quad \frac{p-1}{2} \cdot 2 = p - 1$$

のうち, $p/2$ より大きいものの個数を n とする. これは,

$$1 = p - \frac{p-1}{2} \cdot 2, \quad 3 = p - \frac{p-3}{2} \cdot 2, \quad 5 = p - \frac{p-5}{2} \cdot 2,$$
$$\ldots, \quad p-4 = p - 2 \cdot 2, \quad p-2 = p - 1 \cdot 2$$

のうち, $p/2$ より小さいものの個数に一致する.
すなわち, n は奇数 1, 3, 5, ..., $p-2$ のうち, $p/2$ より小さいものの個数に一致する.
よって, $(p-1)/2$ が奇数のとき,

$$n \equiv 1 + 3 + 5 + \cdots + \frac{p-1}{2} \pmod 2,$$

$(p-1)/2$ が偶数のとき,

$$n \equiv 1 + 3 + 5 + \cdots + \frac{p-3}{2} \pmod 2.$$

いずれにせよ,

$$\begin{aligned} n &\equiv 1 + 2 + 3 + \cdots + \frac{p-1}{2} \pmod 2 \\ &= \frac{1}{2} \cdot \frac{p-1}{2} \left(\frac{p-1}{2} + 1\right) \\ &= \frac{p^2-1}{8}. \end{aligned}$$

したがって Gauss の補題から求める式を得る. □

定理 6.4 (平方剰余の相互法則). $p, q \in \mathbb{P} \setminus \{2\}$ とし, $p \neq q$ とする. このとき,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

証明. 集合 S の元の個数を $|S|$ で表すことにする.

$$\begin{aligned} A &= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 1 \leq x \leq (p-1)/2,\ 1 \leq y \leq (q-1)/2\}, \\ B &= \{qx - py \mid (x, y) \in A\}, \\ B_1 &= \{qx - py \mid (x, y) \in A,\ qx - py < -p/2\}, \\ B_2 &= \{qx - py \mid (x, y) \in A,\ -p/2 < qx - py < 0\}, \\ B_3 &= \{qx - py \mid (x, y) \in A,\ 0 < qx - py < q/2\}, \\ B_4 &= \{qx - py \mid (x, y) \in A,\ q/2 < qx - py\} \end{aligned}$$

とおく.

Step 1　まず,

$$B = B_1 \cup B_2 \cup B_3 \cup B_4 \quad (\text{集合の直和})$$

を証明する. そのためには, $0 \notin B$ を証明すれば十分である.

$(x, y) \in \mathbb{Z} \times \mathbb{Z}$ が存在して

$$qx - py = 0$$

が成り立つとすると, $\gcd(p, q) = 1$ より,

$$x \equiv 0 \pmod{p}, \quad y \equiv 0 \pmod{q}$$

が得られる. よって $(x, y) \notin A$. したがって, $0 \notin B$ が示された.

Step 2　次に,

$$|B| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

を証明する.

$(x, y), (x', y') \in \mathbb{Z} \times \mathbb{Z}$ について,

$$qx - py = qx' - py'$$

が成り立つとすると,

$$q(x - x') = p(y - y').$$

$\gcd(p, q) = 1$ より,

$$x \equiv x' \pmod{p}, \quad y \equiv y' \pmod{q}.$$

よって, $qx - py$ の値は $(x, y) \in A$ ごとに異なる. ゆえに

$$|B| = |A| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Step 3　次に,

$$|B_1| = |B_4|$$

が成り立つ. このことは, 写像

$$\begin{aligned} B_1 \longrightarrow B_4, \quad qx - py \longmapsto & q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right) \\ & = \frac{q-p}{2} - (qx - py) \end{aligned}$$

が, 逆写像

$$\begin{aligned} B_4 \longrightarrow B_1, \quad qx' - py' \longmapsto & q\left(\frac{p+1}{2} - x'\right) - p\left(\frac{q+1}{2} - y'\right) \\ & = \frac{q-p}{2} - (qx' - py') \end{aligned}$$

を持つことからわかる.

Step 4

$$C_2 = \{x \in \mathbb{Z} \mid 1 \le x \le (p-1)/2,$$
$$\exists y \in \mathbb{Z} \text{ s.t. } 1 \le y \le (q-1)/2, \quad -p/2 < qx - py < 0 \},$$
$$C_2' = \{x \in \mathbb{Z} \mid 1 \le x \le (p-1)/2,$$
$$qx \text{ は } p \text{ を法として } -1, -2, \ldots -(p-1)/2 \text{ のいずれかと合同 } \}$$

とおく.

Step 4-1　まず, $|B_2| = |C_2|$ を証明する.
$1 \le x \le (p-1)/2$ なる $x \in \mathbb{Z}$ に対して, $y \in \mathbb{Z}$ がただ一つ存在して

$$-\frac{p}{2} < qx - py < \frac{p}{2}$$

となる.
実際, qx を p で割ったとき,

$$qx = py_1 + r_1, \quad 0 \le r_1 < p$$

を満たすような組 $y_1, r_1 \in \mathbb{Z}$ がただ一つ存在する.
$\gcd(qx, p) = 1$ より, $r_1 \neq 0$.
$0 < r_1 < p/2$ のとき, $y = y_1$ とおく.
$p/2 < r_1 < p$ のとき, $y = y_1 + 1$ とおく.
以上より, 求める y が得られる.
このことから $|B_2| \le |C_2|$ が得られる.

$(x, y), (x', y') \in A$ について

$$qx - py = qx' - py'$$

であるとすれば,

$$q(x - x') = p(y - y').$$

$\gcd(p, q) = 1$ より,

$$x \equiv x' \pmod{p}, \ y \equiv y' \pmod{q}$$

が得られる. よって, 逆の不等号 $|C_2| \le |B_2|$ も成り立つ.

以上より, $|B_2| \le |C_2|$ と $|C_2| \le |B_2|$ とがともに成り立つから, $|B_2| = |C_2|$.

Step 4-2　次に, $|C_2| = |C_2'|$ を証明する.
$1 \le x \le (p-1)/2$ なる $x \in \mathbb{Z}$ について, ある $y \in \mathbb{Z}$ が存在して

$$-\frac{p}{2} < qx - py < 0$$

が成り立つとき, qx は p を法として $-1, -2, \ldots, -(p-1)/2$ のいずれかに合同である. すなわち, $C_2 \subseteq C_2'$.
逆に, $1 \le x \le (p-1)/2$ なる $x \in \mathbb{Z}$ について, qx が p を法として $-1, -2, \ldots, -(p-1)/2$ のいずれかと合同であるとする. このとき, $y \in \mathbb{Z}$ が存在して

$$-\frac{p}{2} < qx - py < 0$$

でなければならない. さらに,

$$y < \frac{1}{2} + \frac{q}{p}x \leq \frac{1}{2} + \frac{q}{p} \cdot \frac{p-1}{2} < \frac{q+1}{2}$$

および

$$y > \frac{q}{p}x \geq \frac{q}{p} > 0$$

より,

$$1 \leq y \leq \frac{q-1}{2}$$

が得られる. すなわち, $C_2' \subseteq C_2$.

$C_2 \subseteq C_2'$ と $C_2' \subseteq C_2$ とがともに成り立つから, $C_2 = C_2'$ となる.

以上より,

$$|B_2| = |C_2| = |C_2'|$$

が示された.

よって, $n = |B_2|$ とおけば, Gauss の補題より

$$\left(\frac{q}{p}\right) = (-1)^n$$

が成り立つ.

Step 5 $m = |B_3|$ とおけば, $1 \leq y \leq (q-1)/2$ なる $y \in \mathbb{Z}$ に対して Step 4 と同様の議論を行うことによって

$$\left(\frac{p}{q}\right) = (-1)^m$$

が得られる.

以上より,

$$\begin{aligned}\frac{p-1}{2} \cdot \frac{q-1}{2} &= |B| = |B_1| + |B_2| + |B_3| + |B_4| \\ &= 2|B_1| + n + m \\ &\equiv n + m \pmod 2.\end{aligned}$$

さらに,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^n(-1)^m = (-1)^{n+m} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

となる. □

記 号

$\mathbb{Z}$: 整数全体からなる集合
$\mathbb{Z}^+$: 正の整数全体からなる集合
$\mathbb{P}$: 素数全体からなる集合
$\mathbb{P} \setminus \{2\}$: 2 以外の素数全体からなる集合
$m\mathbb{Z}$: m の倍数全体からなる集合
$\mathbb{Z}/m\mathbb{Z}$: 法 m に関する剰余類全体からなる集合
$b \mid a$: a は b で割りきれる
gcd: 最大公約数
lcm: 最小公倍数
$C(a)$: a を代表元とする剰余類
φ: Euler の関数
(a/p): Legendre 記号

索 引