離散数学

宮本 暢子

April 9, 2022

Outline

自然数の公理（ペアノ公理)

(i) $1 \in \mathbb{N}$, 1 は自然数である
(ii) $x \in \mathbb{N}$ ならば，$x + 1 \in \mathbb{N}$ である
(iii) $x \in \mathbb{N}$ ならば，$x + 1 \neq 1$ である
(iv) $x + 1 = y + 1 (x, y \in \mathbb{N})$ ならば，$x = y$ である
(v) $1 \in M$ および $x \in M$ ならば $x + 1 \in M$ が満たされれば，$\mathbb{N} \subset M$ である

公理 (v) と数学的帰納法

数学的帰納法

$P(n)$ を自然数 n に関する命題とする．このとき

(i) $P(1)$ が成り立つ．

(ii) $P(n)$ が成り立つならば $P(n+1)$ も成り立つ

が成り立てば，すべての $n \in \mathbb{N}$ について $P(n)$ は成り立つ．

公理 1 整列原理

$\mathbb{N}$ の空でない部分集合には，最小の正の整数が存在する．

定理 1 (ユークリッドの性質)

任意の整数 a, 自然数 b ($b \neq 0$) に対して，

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

となるような整数の商 q と剰余 r が一意に存在する.

定義 1

a, b を共に零ではない整数とする.
このとき次の条件 (i) を満たすような d を a と b の**公約数**と呼び，条件 $(i), (ii)$ を満たす $d > 0$ を a と b の**最大公約数**と呼び，$\gcd(a, b)$ で表す.

(i) $d|a$ かつ $d|b$

(ii) $c|a$ かつ $c|b$ なるどんな整数 c も $c|d$ である.

整数 a, b が $\gcd(a, b) = 1$ の関係にあるとき，
a と b は**互いに素**であるという.

定理 2 (ユークリッドの互除法)

a,b を正の整数とする．
$a_0 = a$, $a_1 = b$ とおき, さらに $n \geq 1$ に対し，

$$a_{n-1} = a_n q_n + a_{n+1} \tag{1}$$

$$0 \leq a_{n+1} < a_n \tag{2}$$

で数列 $\{a_n\}$ を定義する．
このとき，ある自然数 N があって $a_{N+1} = 0$ となり

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

が成り立つ．

定理 3 (拡張ユークリッドアルゴリズム)

任意の整数 a,b に対して，$d = \gcd(a, b)$ とするとき

$$ax + by = d$$

を満たす整数 x, y が存在する．

問題 1

(1) $a = 72, b = 56$ とし $d = \gcd(a, b)$ を求め,
$ax + by = d$ を満たす整数 x, y を求めよ.

(2) $a = 6731, b = 4717$ とし $d = \gcd(a, b)$ を求め,
$ax + by = d$ を満たす整数 x, y を求めよ.

定理 4

a, b, c を整数とし，$a, b \neq 0$ とする.
このとき，方程式 $ax + by = c$ に対して，次が成り立つ.

(1) 整数解 x, y が存在することと $\gcd(a, b) | c$ であることは同値である.

(2) x_0, y_0 を１つの整数解とすると，任意の解はある整数 $m \in \mathbf{Z}$ により，
$x = x_0 - m(b/d), y = y_0 + m(a/d)$
と書ける.　ただし $d = \gcd(a, b)$ である.

問題 2

$72x + 56y = 16$ を満たす整数 x, y を 2 組求めよ.

定義 2

a, b を共に零ではない整数とする.
このとき次の条件 (i) を満たすような m を a と b の**公倍数**と呼び，条件 $(i), (ii)$ を満たす $m > 0$ を a と b の**最小公倍数**と呼び，$lcm(a, b)$ で表す.

(i) $a|m$ かつ　$b|m$

(ii) $a|c$ かつ $b|c$ なるどんな整数 c も $m|c$ である.

定理 5

a, b を整数とし，$a, b \neq 0$ とするとき，a, b の最小公倍数は一意に存在する.
また $lcm(a, b) = |ab| / \gcd(a, b)$ である.

定理 6 (一意因数分解の定理)

零でない任意の整数 n は，異なる素数 $p_1, p_2, \ldots$ と自然数 $e_1, e_2, \ldots$ で

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

と一意に表される．

上の定理において，素数 $p_1, \ldots, p_k$ を n の**素因数**といい，n を素因数の積として表すことを n の**素因数分解**という．

定理 7

素数は無限に存在する．

定義

1 より大きい自然数 m に対して，整数 a, b の差 $a-b$ が m の倍数であるとき，a と b は**法** m に関して**合同である**といい，

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

と表す．この式を**合同式**という．

定理 8 (mod 計算の性質)

(1) $a \equiv b \pmod{m}$ かつ $d|m$ のとき，

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

である．

(2) $a \equiv b \pmod{m}$ かつ $a \equiv b \pmod{n}$ のとき，

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

である．ただし $l = lcm(m, n)$.

定理 8 (mod 計算の性質) の続き

(3) $a \equiv c \pmod{m}$ かつ $b \equiv d \pmod{m}$ のとき，

$$a + b \equiv c + d \pmod{m},$$

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

$$ab \equiv cd \pmod{m}$$

である．

(4) $ab \equiv ac \pmod{m}$ のとき，

$$b \equiv c \pmod{m/d}$$

である．ただし $d = \gcd(a, m)$ である．

定理 9

$d = \gcd(a, m)$ とおくと，次のことが成り立つ．

(1) 次の $(a), (b)$ は同値である．
   (a) $ax \equiv b \pmod{m}$ は解をもつ．
   (b) $d|b$ が成り立つ．

(2) $ax \equiv b \pmod{m}$ の解の１つを x_1 とし，$m' = m/d$ とおくと，合同式の解全体は $\{x_1 + m'k : k \in \mathbb{Z}\}$ で与えられる．

(3) m を法としての解の個数は d である．

系 10

$\gcd(a, m) = 1$ ならば，$ax \equiv b \pmod{m}$, $a \not\equiv 0 \pmod{m}$ の解は，m を法としてただ１つである．

合同式　$ax \equiv b \pmod{m}$ を解くアルゴリズム

(1) $0 \le a \le m$ でなければ，$a = a'm + r$ $(0 \le r < m)$ として，$a := r$ に置き換える．

(2) a, m に対して拡張ユークリッドの互除法を用い $au + mv = d$, $d = \gcd(a, m)$ となる d, u, v を求める．

(3)
   (i) $d \nmid b$ なら解は存在しない．
   (ii) $d|b$ なら $x = u(b/d)$ が解の１つである．

問題 9

次の合同式が解をもつか答えよ. また解を持つ場合は求めよ.

(1) $4x \equiv 1 \pmod{5}$

(2) $8x \equiv 5 \pmod{12}$

(3) $9x \equiv 6 \pmod{15}$

(4) $72x \equiv 8 \pmod{56}$

(5) $66x \equiv 18 \pmod{42}$

定理 11 (中国人の剰余定理)

$m_1, m_2, \ldots, m_k$ を互いに素な整数 (> 1) とするとき，次の連立合同式

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

には $M = m_1 m_2 \cdots m_k$ を法としてただ１つの解が存在する．

連立合同式の解の求め方

$M_i = M/m_i, (i = 1, \ldots, k)$ とおく．

$$M_i x_i \equiv a_i \pmod{m_i}\ (i = 1, \ldots, k)$$

を満たす解 $u_i, (i = 1, \ldots, k)$ を用いて

$$x = M_1 u_1 + M_2 u_2 + \cdots + M_k u_k$$

が唯一つの解となる．

問題 10

次の連立合同式の解を求めよ.

(1) $\begin{cases} 3x \equiv 1 \pmod{5} \\ 4x \equiv 5 \pmod{7} \end{cases}$ (2) $\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$

定理 11 の派生

$m_1, m_2, \ldots, m_k$ を互いに素な整数 (> 1) とするとき，次の連立合同式

$$\begin{aligned} t_1 x &\equiv a_1 \pmod{m_1} \\ t_2 x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ t_k x &\equiv a_k \pmod{m_k} \end{aligned}$$

には $M = m_1 m_2 \cdots m_k$ を法としてただ１つの解が存在する．

$$M_i t_i x_i \equiv a_i \pmod{m_i}\ (i = 1, \ldots, k)$$

を満たす解 $u_i, (i = 1, \ldots, k)$ を用いて

$$x = M_1 u_1 + M_2 u_2 + \cdots + M_k u_k$$

が唯一つの解となる．

解の求め方

解の求め方 $M_i = M/m_i, (i = 1, \ldots, k)$ とおく．

$$M_i x_i \equiv a_i \pmod{m_i} \ (i = 1, \ldots, k)$$

を満たす解 $u_i, (i = 1, \ldots, k)$ を用いて

$$x = M_1 u_1 + M_2 u_2 + \cdots + M_k u_k$$

が唯一つの解となる．

$$\begin{aligned} t_i x &\equiv t_i\{M_1 u_1 + M_2 u_2 + \cdots + M_k u_k\} \\ &\equiv t_i\{M_i u_i\} \\ &\equiv a_i \pmod{m_i} \end{aligned}$$

二項関係

定義

空でない集合 A, B に対して，

$$A \times B = \{(x, y) : x \in A, y \in B\}$$

を A と B の直積といい，$A \times B$ で表す．
特に同じ集合の直積 $A \times A$ を A^2, n 個の A の直積を A^n で表す．また，A と B の直積の部分集合 $R \subseteq A \times B$ を A と B の二項関係という．

同値関係

定義 3

A 上の同値関係 E とは，次の条件を満たす二項関係 $E \subseteq A \times A$ である．

(1) $\forall x \in A$ に対し，$(x, x) \in E$ である．(反射律)

(2) $(x, y) \in E$ ならば，$(y, x) \in E$ である．(対称律)

(3) $(x, y) \in E$ かつ $(y, z) \in E$ ならば，$(x, z) \in E$ である．(推移律)

同値類

$x \in A$ に対して，x と同値関係 E にあるすべての要素の集合

$$[x]_\sim = \{y \in A : y \sim x\}$$

を**同値類**といい，そのときの x を**代表元**という．集合 A のすべての同値類の集合を $A/\sim = \{[x]_\sim : x \in A\}$ と書き，A の同値関係 $\sim$ に関する**商集合**と呼ぶ．

定理 12

m を正の整数とする．
このとき $\mathbf{Z}$ 上の二項関係 $\sim$ を

$$x \sim y \Leftrightarrow x \equiv y \pmod m$$

と定義するとき，$\sim$ は $\mathbf{Z}$ 上の同値関係である．

$\mathbf{Z}$ は同値類の集合（商集合）

$$\mathbf{Z}/\sim = \mathbf{Z}_m = \{[0]_\sim, [1]_\sim, \cdots, [m-1]_\sim\}$$

に類別される．
この同値類を**剰余類**と呼び，各同値類の代表元も m で割ったときの余りとすることが多く，$\mathbf{Z}_m = \{0, 1, \cdots, m-1\}$ と表すことができる．

問題 5

$\mathbb{Z}$ 上に次の二項関係 $\sim$ を定義する．

$x \sim y \Leftrightarrow x - y$ が 3 の倍数　$(x \equiv y \pmod 3)$

$\sim$ が同値関係となることを示し，同値類を求めよ．

代数系

代数系

ある集合 G が G 上で定義されるある演算 $\circ$ に関して閉じている，すなわち

$$a, b \in G \quad \text{ならば} \quad a \circ b \in G$$

であるとき，G と演算 $\circ$ の組 $(G, \circ)$ を代数系という．

群

定義 4(群)

代数系 $(G, \circ)$ が次の性質を満たすとき，$(G, \circ)$ は群であるという．

(1) 任意の $a, b, c \in G$ に対して，
$(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ．(結合法則)

(2) ある元 $e \in G$ が存在して，任意の元 $a \in G$ に対して $e \circ a = a \circ e = a$ が成り立つ．
（e を単位元という）

(3) 任意の元 $a \in G$ に対して，ある元 a^{-1} が存在して $a \circ a^{-1} = a^{-1} \circ a = e$ が成り立つ．
（a^{-1} を a の逆元という）

$\mathbb{Z}, \mathbb{Q}$について

- $(\mathbb{Z}, +)$について
  - (0) 任意の$a, b \in \mathbb{Z}$に対して, $a + b \in \mathbb{Z}$ は成り立つか？
  - (1) 任意の$a, b, c \in \mathbb{Z}$に対して, $(a + b) + c = a + (b + c)$は成り立つか？
  - (2) 任意の元$a \in \mathbb{Z}$に対して, $e + a = a + e = a$が成り立つある元$e \in \mathbb{Z}$が存在するか？
  - (3) 任意の元$a \in \mathbb{Z}$に対して, $a + a^{-1} = a^{-1} + a = e$が成り立つある元$a^{-1} \in \mathbb{Z}$が存在するか？

$\mathbb{Z}$, $\mathbb{Q}$について

- $(\mathbb{Q}, +)$ について
  (0) 任意の $a, b \in \mathbb{Q}$ に対して, $a + b \in \mathbb{Q}$ は成り立つか？
  (1) 任意の $a, b, c \in \mathbb{Q}$ に対して, $(a + b) + c = a + (b + c)$ は成り立つか？
  (2) 任意の元 $a \in \mathbb{Q}$ に対して, $e + a = a + e = a$ が成り立つある元 $e \in \mathbb{Q}$ が存在するか？
  (3) 任意の元 $a \in \mathbb{Q}$ に対して, $a + a^{-1} = a^{-1} + a = e$ が成り立つある元 $a^{-1} \in \mathbb{Q}$ が存在するか？

$\mathbb{Z}$, $\mathbb{Q}$について

- $(\mathbb{Z} \setminus \{0\}, \cdot)$について
  (0) 任意の $a, b \in \mathbb{Z}$ に対して, $a \cdot b \in \mathbb{Z}$ は成り立つか？
  (1) 任意の $a, b, c \in \mathbb{Z}$ に対して, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ は成り立つか？
  (2) 任意の元 $a \in \mathbb{Z}$ に対して, $e \cdot a = a \cdot e = a$ が成り立つある元 $e \in \mathbb{Z}$ が存在するか？
  (3) 任意の元 $a \in \mathbb{Z}$ に対して, $a \cdot a^{-1} = a^{-1} \cdot a = e$ が成り立つある元 $a^{-1} \in \mathbb{Z}$ が存在するか？

$\mathbb{Z}$, $\mathbb{Q}$について

- $(\mathbb{Q} \setminus \{0\}, \cdot)$ について
  - (0) 任意の $a, b \in \mathbb{Q}$ に対して, $a \cdot b \in \mathbb{Z}$ は成り立つか？
  - (1) 任意の $a, b, c \in \mathbb{Q}$ に対して, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ は成り立つか？
  - (2) 任意の元 $a \in \mathbb{Q}$ に対して, $e \cdot a = a \cdot e = a$ が成り立つある元 $e \in \mathbb{Z}$ が存在するか？
  - (3) 任意の元 $a \in \mathbb{Q}$ に対して, $a \cdot a^{-1} = a^{-1} \cdot a = e$ が成り立つある元 $a^{-1} \in \mathbb{Q}$ が存在するか？

問題 6

次の各二項演算 $\circ$ は結合法則を満たすか答えよ.

(1) $\mathbb{Z}$ において，$a \circ b = a - b$ と定義する.

(2) $\mathbb{N}$ において，$a \circ b = 2^{ab}$ と定義する.

問題 7

$G = \mathbb{R} \setminus \{-1\}$ として二項演算 $\circ$ を $a \circ b = a + b + ab$ と定義する.

(1) $(G, \circ)$ は代数系であるか答えよ.

(2) $(G, \circ)$ が群であるか確かめよ.

可換群

可換群

群が次の条件を満たすとき，可換群という．

(4) 任意の $a, b \in G$ に対して，$a \circ b = b \circ a$ が成り立つ．(交換法則)

例

- $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ は可換群
- $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ は可換群

対称群

- 集合 $\{1, 2, \ldots, n\}$ 上の全単射写像を n 次の置換という．
- 一般に n 次の置換全体を S_n で表し，S_n は写像の積（合成）に関して群をなし，n 次の対称群と呼ばれる．
- 任意の S_n の置換 σ, τ に対し，合成写像 $\sigma \circ \tau$ は，各元 i, $i = 1, \ldots, n$ を $\sigma \circ \tau(i) = \sigma(\tau(i))$ にうつす写像である．

3 次の対称群

問題 8

3 次の対称群 $S_3 = \{\epsilon, \sigma_1, \sigma_2, \sigma_3, \psi_1, \psi_2\}$ を考える.

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \psi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \psi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

(1) 演算表を作り，S_3 が群であるか確かめよ。

(2) S_3 の真の部分集合で，群となるものを一つ挙げよ。

環

Definition

次の性質を満たす２つの二項演算子 $+, \cdot$ を持つ代数系 $(R, +, \cdot)$ を環という．

(1) $(R, +)$ は可換群である．

(2) $(R \setminus \{0\}, \cdot)$ は逆元の存在を除いては，乗法群の定義を満たす．ここで 0 は加法単位元とする．

(3) 分配法則を満たす．すなわち任意の $a, b, c \in R$ に対して，

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

かつ

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

が成り立つ．

乗法について可換な環は可換環と呼ばれる．

例

$(\mathbb{Z}, +, \cdot)$ は環である．

- $(\mathbb{Z}, +)$ は可換群
- $(\mathbb{Z} \setminus \{0\}, \cdot)$ は群の定義の (1), (2) を満たす
  - (1) 結合法則
  - (2) 単位元の存在
- 交換法則

環

定理 13

任意の整数 $m \geq 2$ に対し，$(\mathbb{Z}_m, +_m, \cdot_m)$ は可換環である．ただし，$+_m, \cdot_m$ は $\mod m$ での加法，乗法とする．

問題 9

$\mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5$ を考える.

(1) それぞれの加法 $+_m$ と乗法 $\cdot_m$ の演算表を作れ.
(2) 加法に関して，単位元および各元の逆元が存在するか答えよ.
(3) 乗法に関して，単位元および各元の逆元が存在するか答えよ.

整域

定義 6

可換環 R の要素 $a \neq 0$ に対し，もし $ab = 0$ となるような $b \neq 0$ が R に存在すれば，a を**零因子**という．零因子をもたない可換環を**整域**と呼ぶ．

体

定義 7

次の条件を満たす代数系 $(F, +, \cdot)$ を**体**という．

(1) $(F, +, \cdot)$ は可換環である．

(2) 任意の $x \in F (x \neq 0)$ に対し，逆元 x^{-1} が存在する．

F が有限集合で $(F, +, \cdot)$ が体となるとき，F を**有限体**または**ガロア体**と呼ぶ．有限体 F の元の数を F の**位数**と呼び，位数 q の有限体を $\mathrm{GF}(q)$ と書く．

例

- $\mathbb{Z}$ は整域である
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は可換体である.

問題 10

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ を考える.

(1) 加法に関して，単位元および各元の逆元が存在するか答えよ.

(2) 乗法に関して，単位元および各元の逆元が存在するか答えよ.

(3) 零元以外の零因子をもつか答えよ.

問題 11

$\mathbb{Z}_6, \mathbb{Z}_7$ を考える．各元の乗法逆元が存在するか答えよ．また存在するならば，その元を示せ．

定義 8

環 $(R,+,\cdot)$ の部分集合 I が加法群として R の部分群 $(a, b \in I$ ならば，$a - b \in I$ が成り立つ$)$ で，

(1) $r \in R, a \in I$ ならば，$r \cdot a \in I$

を満たすとき，I を R の左イデアルといい，

(2) $r \in R, a \in I$ ならば，$a \cdot r \in I$

を満たすとき，I を R の右イデアルという.
また，I が条件 (1)，(2) を共に満たすとき，I を R の両側イデアルまたはイデアルという.

イデアル

一般に，環 R の部分集合 $\{0\}$ と R 自身は R のイデアルである．この $\{0\}$ と R を環 R の自明なイデアルといい，そうでないイデアルを真のイデアルという．イデアル $\{0\}$ は (0) で表すことが多い．

イデアル

問題 12

6 の倍数の全体の集合 $6\mathbb{Z}$ が $\mathbb{Z}$ のイデアルであることを示せ.

イデアル

問題 13

$\mathbb{Z}_{12}$ の真のイデアルを一つ答えなさい.

イデアル

定義 9

R のイデアル I が $I = xR = \{xy : y \in R\}$ と 1 つの元で生成されるとき，I を**単項イデアル**という.
また，すべてのイデアルが単項イデアルとなる整域を**単項イデアル整域**という.

イデアル

定理 14

I を環 R のイデアルとする. このとき R 上の二項関係 $\sim$ を

$$x \equiv y \mod I \Leftrightarrow x - y \in I$$

と定義するとき，$\sim$ は R 上の同値関係である.

イデアル

この同値類の間に加法と乗法の演算 $+, \cdot$ を, 環 R の加法と乗法の演算算 $+, \cdot$ を用いて，次のように定義することができる.
$r \in R$ を含む同値類 $[r]$ と $s \in R$ を含む同値類 $[s]$ に対して，

$$[r] + [s] = [r + s],$$

$$[r] \cdot [s] = [r \cdot s]$$

と定義する.

イデアル

定理 15

I を環 R のイデアルとする. I を法とする剰余類全体の集合 R/I に対して，上記のように加法と乗法を定義するとき，これらの演算に関して，剰余類の全体 R/I は環になる.

上の定理で得られた環 R/I を I を法とする R の**剰余環**と呼ぶ.

剰余環 R/I の零元は $[0] = I$ で，単位元は $[1] = 1 + I$ である.

イデアル

定義 10

可換環 R のイデアル I が $ab \in I$ ならば，$a \in I$ または $b \in I$ を満たすとき，I は R の素イデアルという．

定義 11

可換環 R のイデアル I が，$I \neq R$ で，I を真に含むようなイデアルが R だけのとき，I は R の極大イデアルという．

イデアル

例 1

素数 p で生成されるイデアル $p\mathbb{Z} = \{py : y \in \mathbb{Z}\}$ は，$\mathbf{Z}$ の素イデアルであり，極大イデアルでもある．

イデアル

定理 16

可換環 R のイデアル I が素イデアルとなることと，剰余環 R/I が整域となることは同値である.

定理 17

可換環 R のイデアル I が極大イデアルとなることと，剰余環 R/I が体となることは同値である.

定理 18

可換環 R の極大イデアルは素イデアルである.

定理 19

可換環 $\mathbb{Z}_m$ の要素 a が乗法逆元をもつための必要十分条件は，

$$\gcd(a, m) = 1$$

である．

定理 20

p が素数のとき $\mathbb{Z}_p$ は体となる．

補題 21

p を素数，a, b, x を $\mathbb{Z}_p$ の要素とし，$x \neq 0$ とすると，$a \neq b$ ならば $ax \neq bx$ である．

定理 22 (フェルマーの小定理)

p を素数とする．a を $p \nmid a$ なる整数とすると，

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

である．

問題 14

$\mathbb{Z}_5$ の 0 以外の各元に対して，フェルマーの小定理が成り立つことを確認せよ．

問題 15

(1) 2^{100} を 101 で割った余りを求めよ．

(2) 3^{100} を 13 で割った余りを求めよ．

オイラーの ϕ 関数

整数 $n > 0$ に対して，$\phi(n)$ を n と互いに素な $1 \leq m \leq n$ なる整数 m の個数とする．
このとき ϕ を**オイラーの ϕ 関数**という．
素数 p に対して，$\phi(p) = p - 1$ となる．

定理 23

$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ $(p_1, p_2, \ldots, p_k$ は異なる素数) とすると，

$$\begin{aligned}\phi(n) &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) \\ &= (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1}) \cdots (p_k^{e_k} - p_k^{e_k - 1})\end{aligned}$$

である．

補題

p_1, p_2：異なる素数とする. $n = p_1 p_2$ のとき,

$$\begin{aligned}\phi(n) &= \phi(p_1)\phi(p_2)\\ &= (p_1 - 1)(p_2 - 1)\end{aligned}$$

補題

p_1：素数とする. $n = p^e$ のとき,

$$\phi(n) = p^e - p^{e-1}$$

例えば $n = 2 \cdot 3 \cdot 5 = 30$ のとき，$2, 3, 5$ の 30 以下の倍数は

$$
\begin{aligned}
\text{因子 2 を持つ数} &: \quad D_2 = \{2, 4, 6, 8, 10, 12, 14, 16, 18, \\
&\qquad\qquad 20, 22, 24, 26, 28, 30\} \\
\text{因子 3 を持つ数} &: \quad D_3 = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\} \\
\text{因子 5 を持つ数} &: \quad D_5 = \{5, 10, 15, 20, 25, 30\}
\end{aligned}
$$

であり，

$$
\begin{aligned}
\phi(30) = 30 &- |D_2| - |D_3| - |D_5| \\
&+ |D_2 \cap D_3| + |D_2 \cap D_5| + |D_3 \cap D_5| - |D_2 \cap D_3 \cap D_5|
\end{aligned}
$$

0 から 1 までの分母が 12 の既約分数の数はいくつあるか？

$$\begin{aligned}\phi(12) &= \phi(2^2 \cdot 3)\\ &= \phi(2^2)\phi(3)\\ &= (2^2 - 2)(3 - 1)\\ &= 2 \cdot 2 = 4\end{aligned}$$

$$\frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}$$

補題 24

$\mathbb{Z}_m$ の中で m と互いに素な整数の集合を $M = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ とすると，この集合は $\mod m$ での乗法に関して群をなす．

[考え方]

(0) M が演算 $\cdot_m$ について閉じているか？

(1) 結合法則が成り立つことは，明らか．

(2) 単位元の存在: $1 \in M$ であるか？

(3) 逆元の存在： 任意の $r_i \in M$ に対して，定理 (拡張ユークリッドアルゴリズム) より，$r_i x + my = 1$ なる整数 x, y が存在することを用いる．

問題 17

$\mathbf{Z}_8$ 上において，上の補題を確認せよ．

定理 25(オイラーの定理)

m を正整数とする．もし $\gcd(a, m) = 1$ ならば，

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

である．

補題 26

G を群とし，$a \in G$ とする．

$$< a >= \{a^n : n \in \mathbb{Z}\}$$

は G の部分群になる．

ここで a^n は $n > 0$ のときは，a の n 個の積を表し，$n < 0$ のときは a の逆元の $-n$ 個の積 $(a^{-1})^{-n}$ を表す．$a^0 = e$ とする．
$< a >$ を a で生成された**巡回群**といい，a を巡回群の**生成元**という．
また，群の元 a に対し $a^n = e$ を満たす最小の自然数 n を元 a の**位数**といい，order(a) と書く

問題 18

乗法群 $(\mathbb{Z}_7 \setminus \{0\}, \cdot)\}$ を考える．

(1) $2, 3 \in \mathbb{Z}_7$ に対して，それらを生成元とする巡回群 $< 2 >, < 3 >$ を求めよ．

(2) $\mathbb{Z}_7 \setminus \{0\}$ の各元の位数を求めよ．

問題 19

$\mathbb{Z}_8$ の中で 8 と互いに素な整数の集合を $\mathbb{Z}_8^*$ とする.

(1) $\mathbb{Z}_8^*$ の各元の位数を求めよ.

(2) $(\mathbb{Z}_8^*, \cdot)$ が巡回群であるか答えよ.

補題 27

G を群とし，$a \in G$ とする．$a^k = e$ ならば k は，order(a) の倍数である

補題 28

G を群とし，$a, b \in G$, $\mathrm{order}(a) = n$, $\mathrm{order}(b) = m$ とする．

(i) 自然数 l に対して，$\mathrm{order}(a^l) = n/\gcd(l, n)$.

(ii) a, b が可換で，$\gcd(m, n) = 1$ ならば，$\mathrm{order}(ab) = mn$

問題 20

乗法群 $(\mathbb{Z}_{11} \setminus \{0\}, \cdot)\}$ を考える．

(1) 上の補題を用いて，$\mathbb{Z}_{11} \setminus \{0\}$ の各元の位数を求めよ．

(2) 生成元をすべて求めよ．

定理 29　(巡回群の性質)

G を位数 n の巡回群，a をその生成元とするとき，以下が成り立つ.

(i) d を n の正の約数とするとき，G には位数 d の元が必ず存在する.

(ii) G には位数 d の元が $\phi(d)$ 個ある.

(iii) $\sum_{d|n} \phi(d) = n$ である.

同型

２つの代数系 $(F_1, +_1, \cdot_1)$ と $(F_2, +_2, \cdot_2)$ に対して，全単射 $f\colon F_1 \to F_2$ が存在し，任意の要素 $a, b \in F_1$ に対し，

$$\begin{cases} f(a +_1 b) & = & f(a) +_2 f(b) \\ f(a \cdot_1 b) & = & f(a) \cdot_2 f(b) \end{cases}$$

が成り立つとき，この２つの代数系は**同型**であるという．

定理 30

p, q を異なる素数とする．$\mathbb{Z}_{pq}$ は $\mathbb{Z}_p \times \mathbb{Z}_q$ と同型である．

$n = pq$ とおく．$x \in \mathbb{Z}_n$ に対して，

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

を求め，Z_m から $\mathbb{Z}_p \times \mathbb{Z}_q$ への写像

$$f: \ x \mapsto (a, b)$$

を考える．このとき f は同型写像となる．

例

$$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$$

$\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ と $\mathbb{Z}_3 \times \mathbb{Z}_5 = \{(0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (1, 0), (1, 1), (1, 2), (1, 3), (1, 4), (2, 0), (2, 1), (2, 2), (2, 3), (2, 4)\}$ に対して，以下のような写像 f は同型写像である．

$$\begin{array}{ccc} f: \quad x & \mapsto & (a, b) \\ \hline 0 & \mapsto & (0, 0) \\ 1 & \mapsto & (1, 1) \\ 2 & \mapsto & (2, 2) \\ 3 & \mapsto & (0, 3) \\ 4 & \mapsto & (1, 4) \end{array}$$

定理 31

p, q を異なる素数とし，$\lambda = \mathrm{lcm}(p-1, q-1)$ とする．そのとき $\mathbb{Z}_{pq}$ の任意の要素 c に対し，

$$c^{\lambda+1} \equiv c \pmod{n}$$

が成り立つ．ただし $n = pq$ とする．

考え方
定理 30 より $\mathbb{Z}_{pq}$ は $\mathbb{Z}_p \times \mathbb{Z}_q$ と同型なので，$c \in \mathbb{Z}_n$ に対して，

$$\begin{aligned} c &\equiv a \pmod{p} \\ c &\equiv b \pmod{q} \end{aligned}$$

なる $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$ が存在する．a, b は共に 0 でないとする．(c は n と互いに素である．)

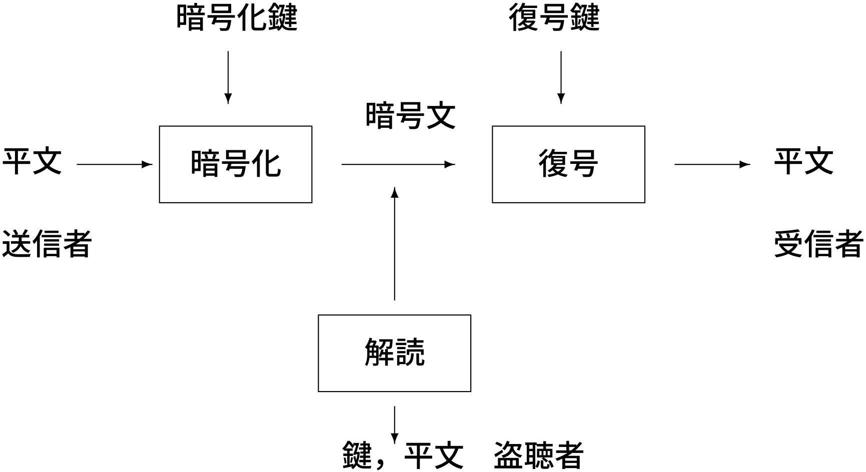
$$(a, b)^0 = (1, 1),\ (a, b),\ (a, b)^2 = (a^2, b^2), \ldots$$

を考える．

$a \in \mathbb{Z}_p$ の位数は $p-1$ の約数なので, a^{p-1},$a^{2(p-1)}$,... はすべて 1 となる．
同様に b^{q-1}, $b^{2(q-1)}$,... はすべて 1 となる．
さらに $(p-1)|\lambda$, $(q-1)|\lambda$ なので $(a^\lambda, b^\lambda) = (1, 1)$ である．したがって

$$(a, b)^{\lambda+1} = (a^{\lambda+1}, b^{\lambda+1}) = (a, b)$$

が成り立つ．
$a \neq 0$, $b = 0$ とする．(c は q の倍数である.)
$(a, b)^{p-1} = (a, 0)^{p-1} = (a^{p-1}, 0) = (1, 0)$ となる．
$(p-1)|\lambda$ なので，$(a, 0)^\lambda = (1, 0)$ となり，$(a, b)^{\lambda+1} = (a, b)$ が成り立つ．


暗号化鍵
復号鍵
暗号文
平文
暗号化
復号
平文
送信者
受信者
解読
鍵，平文
盗聴者

暗号

対称鍵暗号系　暗号化鍵と復号鍵のいずれか一方から他方を簡単に求められる暗号系

- **ブロック暗号**　あるまとまったブロック情報を単位として暗号化
- **ストリーム暗号**　ビットなどの情報要素を逐次的に暗号化

非対称鍵暗号系　簡単に求められない暗号系

- **公開鍵暗号系**　暗号化鍵から復号鍵を簡単に求められないもの．暗号化鍵を公開しても情報の秘密を保つことができる．
  RSA 暗号、ElGamal 暗号など

RSA暗号

受信者の準備

(a1) 受信者（アリス）は2つの大きな素数 p, q を選び，$n = pq$ と $\phi(n) = (p-1)(q-1)$ を計算する．(n は 10^{200}〜10^{600} 程度)

(a2) アリスは $\lambda = lcm(p-1, q-1)$ を計算し，λ と互いに素な整数 e をランダムに選び，

$$ed \equiv 1 \pmod{\lambda}$$

となる d を求める．

(a3) アリスは e と n を公開し (公開鍵)，p, q, d はアリスだけが知っている秘密鍵とする．

暗号化と復号化

(b1) ボブがアリスに暗号化してメッセージを送りたいものとする．まずアリスによって公開された e と n を得る．

(b2) ボブは平文 $x \in \mathbf{Z}_n$ に対して，暗号文 c を次のように計算し，アリスに送信する．

$$x^e \equiv c \pmod{n}$$

(b3) アリスは暗号文 c を受け取り，次の方法で復号化する．

$$c^d \equiv x \pmod{n}$$

(a2) の代わりに (a2') として次のようにしても良い．

(a2') アリスは $\phi(n)$ と互いに素な整数 e をランダムに選び

$$ed \equiv 1 \pmod{\phi(n)}$$

となる d を求める．

問題

$p = 5, q = 11$ として上の手順に従って暗号化鍵，復号化鍵を定めよ．また，平文 3 を送るものとし，暗号化メッセージと復号化の手順を記せ．

ElGamal暗号

受信者の準備

(a1) 受信者（アリス）は素数 p を選び，乗法群 $\mathbf{Z}_p^*$ での原始元 α を求める．次に整数 a $(1 \leq a \leq p-2)$ を定め，

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

を計算する．

(a2) アリスは p, α, y を公開し (公開鍵)，a はアリスだけが知っている秘密鍵とする．

ElGamal暗号

暗号化と復号化

(b1) ボブがアリスに暗号化してメッセージを送りたいものとする．まずアリスによって公開された p, α, y を得る．

(b2) ボブは平文 $x \in \mathbf{Z}_p$ に対して，整数 k $(1 \leq k \leq p-2)$ を任意に定めて（乱数を発生させて）暗号文 (c_1, c_2) を次のように計算し，アリスに送信する．

$$
\begin{aligned}
c_1 &\equiv \alpha^k \pmod p \\
c_2 &\equiv y^k x \pmod p
\end{aligned}
$$

ElGamal 暗号

暗号化と復号化

(b3) アリスは暗号文 (c_1, c_2) を受け取り，次の方法で復号化する．

$$c_2/c_1^a \equiv x \pmod{p}$$

離散対数問題

$\mathbf{Z}_p$ 上で，$\alpha^a \equiv y \pmod{p}$ の関係があるとき，a を y の (α を底とする) 離散対数と呼び，$\log_\alpha y$ で表す．
このシステムの安全性は，y と α が与えられたとき，$y = \alpha^a$ なる a がどのくらい速く計算できるかにかかっている．この問題を**離散対数問題**という．

問題

$p = 13$ として上の手順に従って公開鍵，秘密鍵を定めよ．また，平文 3 を送るものとし，暗号文と復号化の手順を記せ．