離散数理工学　第 5 回

離散代数：整数と有限体

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2023 年 11 月 14 日

最終更新：2023 年 11 月 14 日　09:23

今日の目標

整数の剰余について，次をできるようになる

- 整数の剰余に関する演算を行えるようになる

特に，素数が果たす役割を理解する $\rightsquigarrow$ 有限体

目次

整数全体の集合

記法：整数全体の集合

$\mathbb{Z}$ で整数全体の集合を表す

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

性質：$\mathbb{Z}$ は加法，減法，乗法で閉じている

任意の整数 $a, b \in \mathbb{Z}$ に対して

- $a + b \in \mathbb{Z}$
- $a - b \in \mathbb{Z}$
- $ab \in \mathbb{Z}$

ただし，$a/b \in \mathbb{Z}$ とは限らない (a/b が定義されないこともある)

除法の定理

整数 $a, b \in \mathbb{Z},\ b > 0$

性質：除法の定理

ある整数 $q, r \in \mathbb{Z}$ が **一意に** 存在して，次を満たす

- $a = bq + r$
- $0 \leq r < b$

例：

- $a = 7, b = 3$ のとき $\rightsquigarrow 7 = 3 \cdot 2 + 1$
- $a = 4, b = 9$ のとき $\rightsquigarrow 4 = 9 \cdot 0 + 4$
- $a = -17, b = 4$ のとき $\rightsquigarrow -17 = 4 \cdot (-5) + 3$

証明：演習問題 (ヒントあり)

商と剰余

整数 $a, b \in \mathbb{Z}$, $b > 0$

性質：除法の定理

ある整数 $q, r \in \mathbb{Z}$ が **一意に** 存在して，次を満たす

- $a = bq + r$
- $0 \leq r < b$

定義：商と剰余

a と b に対して，除法の定理で与えられる q と r を次のように呼ぶ

- q は a を b で割ったときの **商**
- r は a を b で割ったときの **剰余** (余り)

この r を $a \bmod b$ で表す (注：mod は二項演算)

つまり

ある整数 q が一意に存在して，$a = bq + (a \bmod b)$

剰余の剰余は剰余

整数 $a, b \in \mathbb{Z},\ b > 0$

性質：剰余の剰余は剰余

$$a \bmod b = (a \bmod b) \bmod b$$

証明：

- 整数 q' を用いて $(a \bmod b) = bq' + ((a \bmod b) \bmod b)$ と書く
- $0 \leq (a \bmod b) < b,\ 0 \leq ((a \bmod b) \bmod b) < b$ であるので，$-b < bq' < b$
- b, q' は整数なので，$q' = 0$ □

法として合同

整数 $a, a' \in \mathbb{Z}$，正整数 $n > 0$

定義：法として合同

a と a' が n **を法として合同** であるとは，次を満たすこと

$$a \bmod n = a' \bmod n$$

a と a' が n を法として合同であることを

$$a \equiv a' \pmod{n}$$

と書くことがある

法として合同：性質

整数 $a, a' \in \mathbb{Z}$，正整数 $n > 0$

性質：法において合同

a と a' が n を法として合同 $\Leftrightarrow$

ある整数 q が存在して，$a - a' = nq$ である

証明 $(\Rightarrow)$：$a \bmod n = a' \bmod n$ と仮定

- ある整数 s, s' が存在して，$a = ns + (a \bmod n), a' = ns' + (a' \bmod n)$
- $a \bmod n = a' \bmod n$ なので，$a - a' = ns - ns' = n(s - s')$
- $q = s - s'$ とすると，q は整数で，$a - a' = nq$

法として合同：性質 (続)

整数 $a, a' \in \mathbb{Z}$，正整数 $n > 0$

性質：法において合同

a と a' が n を法として合同 $\Leftrightarrow$

ある整数 q が存在して，$a - a' = nq$ である

証明 ($\Leftarrow$)：ある整数 q に対して $a - a' = nq$ であると仮定

- ある整数 s, s' が存在して，$a = ns + (a \bmod n), a' = ns' + (a' \bmod n)$
- したがって，

$$\begin{aligned}(a \bmod n) - (a' \bmod n) &= (a - ns) - (a' - ns') = (a - a') - ns + ns' \\ &= nq - ns + ns' = n(s' - s + q)\end{aligned}$$

- $0 \leq (a \bmod n) < n$ かつ $0 \leq (a' \bmod n) < n$ なので，$s' - s + q = 0$
- $\therefore a \bmod n = a' \bmod n$ □

目次

剰余の集合

正の整数 n を固定

記法：剰余の集合

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ とする

例：

- $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$
- $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$
- $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$
- $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$

剰余の集合上の加法と乗法

正の整数 $n > 0$ を固定，$x, y \in \mathbb{Z}/n\mathbb{Z}$

定義：剰余の集合上の加法と乗法

次のように $\mathbb{Z}/n\mathbb{Z}$ 上の加法 $+$ と乗法 $\cdot$ を定義する

- $x + y = (x + y) \bmod n$
- $x \cdot y = (x \cdot y) \bmod n$

この定義が本当に意味のあるものであるか，確認する必要がある

確認するために必要な性質

整数 $a, b \in \mathbb{Z}$ に対して，$x = a \bmod n, y = b \bmod n$ であるとする

- $x + y = (a + b) \bmod n$
- $x \cdot y = (a \cdot b) \bmod n$

この性質を今から確認する

剰余と加法

正の整数 n，整数 a, a'

性質：剰余と加法

$$(a + a') \bmod n = ((a \bmod n) + (a' \bmod n)) \bmod n$$

注：$(a + a') \bmod n = (a \bmod n) + (a' \bmod n)$ では **ない**

例

$$\begin{aligned}
&(123456789 + 343434343) \bmod 21 \\
&= ((123456789 \bmod 21) + (343434343 \bmod 21)) \bmod 21 \\
&= (15 + 3) \bmod 21 \\
&= 18
\end{aligned}$$

剰余と加法：証明

正の整数 n，整数 a, a'

性質：剰余と加法

$$(a + a') \bmod n = ((a \bmod n) + (a' \bmod n)) \bmod n$$

証明：$a + a'$ と $(a \bmod n) + (a' \bmod n)$ が n を法として合同であることを示せばよい．

- つまり，ある整数 q が存在して，
  $(a + a') - ((a \bmod n) + (a' \bmod n)) = nq$ となることを示せばよい
- ある整数 s, s' を使って，
  $a = ns + (a \bmod n)$，$a' = ns' + (a' \bmod n)$ と書く

剰余と加法：証明

正の整数 n，整数 a, a'

性質：剰余と加法

$$(a + a') \bmod n = ((a \bmod n) + (a' \bmod n)) \bmod n$$

証明：$a + a'$ と $(a \bmod n) + (a' \bmod n)$ が n を法として合同であることを示せばよい．

- つまり，ある整数 q が存在して，
  $(a + a') - ((a \bmod n) + (a' \bmod n)) = nq$ となることを示せばよい
- ある整数 s, s' を使って，
  $a = ns + (a \bmod n)$，$a' = ns' + (a' \bmod n)$ と書く
- このとき，

$$\begin{aligned}
&(a + a') - ((a \bmod n) + (a' \bmod n)) \\
&= (ns + (a \bmod n) + ns' + (a' \bmod n)) - ((a \bmod n) + (a' \bmod n)) \\
&= ns + ns' = n(s + s')
\end{aligned}$$

剰余と加法：証明

正の整数 n，整数 a, a'

性質：剰余と加法

$$(a + a') \bmod n = ((a \bmod n) + (a' \bmod n)) \bmod n$$

証明：$a + a'$ と $(a \bmod n) + (a' \bmod n)$ が n を法として合同であることを示せばよい．

- つまり，ある整数 q が存在して，
  $(a + a') - ((a \bmod n) + (a' \bmod n)) = nq$ となることを示せばよい
- ある整数 s, s' を使って，
  $a = ns + (a \bmod n)$，$a' = ns' + (a' \bmod n)$ と書く
- このとき，
  $$\begin{aligned}&(a + a') - ((a \bmod n) + (a' \bmod n))\\ &= (ns + (a \bmod n) + ns' + (a' \bmod n)) - ((a \bmod n) + (a' \bmod n))\\ &= ns + ns' = n(s + s')\end{aligned}$$
- $q = s + s'$ とすれば，s, s' が整数なので，q も整数
- このとき，$(a + a') - ((a \bmod n) + (a' \bmod n)) = nq$ □

剰余と乗法

正の整数 n，整数 a, a'

性質：剰余と乗法

$$(a \cdot a') \bmod n = ((a \bmod n) \cdot (a' \bmod n)) \bmod n$$

注：$(a \cdot a') \bmod n = (a \bmod n) \cdot (a' \bmod n)$ では **ない**

例

$$\begin{aligned}
&(123456789 \cdot 343434343) \bmod 21 \\
&= ((123456789 \bmod 21) \cdot (343434343 \bmod 21)) \bmod 21 \\
&= (15 \cdot 3) \bmod 21 \\
&= 45 \bmod 21 \\
&= 3
\end{aligned}$$

証明：演習問題 (加法のときと同様に証明できる)

加法と乗法の性質：可換性と結合性，分配性，単位元の存在

正の整数 $n \geq 2$ を固定，$x, y, z \in \mathbb{Z}/n\mathbb{Z}$

性質：可換性と結合性，分配性，単位元の存在

1. $x + y = y + x$ (加法の可換性)
2. $(x + y) + z = x + (y + z)$ (加法の結合性)
3. $0 + x = x + 0 = x$ (加法の単位元)
4. $x \cdot y = y \cdot x$ (乗法の可換性)
5. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (乗法の結合性)
6. $1 \cdot x = x \cdot 1 = x$ (乗法の単位元)
7. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (分配性)

証明：整数の加法と乗法の性質からすぐに分かる (省略)

目次

体

直感：体 = 加減乗除ができる集合

定義：体

体 とは，集合 K と，その上の加算 $+$，乗算 $\cdot$ の 3 つ組 $(K, +, \cdot)$ で
次を満たすもののこと

1. 任意の要素 $x, y \in K$ に対して，$x + y = y + x$ (加算の可換性)
2. 任意の要素 $x, y, z \in K$ に対して，$(x + y) + z = x + (y + z)$ (加算の結合性)
3. ある要素 $0 \in K$ が存在して，任意の要素 $x \in K$ に対して
   $0 + x = 0 + x = x$ (加算の単位元)
4. 任意の要素 $x \in K$ に対して，ある要素 $y \in K$ が存在して
   $x + y = y + x = 0$ (加算の逆元)

...

定義は次のページに続く

体 (続き)

直感：体 = 加減乗除ができる集合

定義 (続き)：体

体 とは，集合 K と，その上の加算 $+$，乗算 $\cdot$ の 3 つ組 $(K, +, \cdot)$ で
次を満たすもののこと

5. 任意の要素 $x, y \in K$ に対して，$x \cdot y = y \cdot x$ (乗算の可換性)
6. 任意の要素 $x, y, z \in K$ に対して，$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (乗算の結合性)
7. ある要素 $1 \in K$ が存在して，任意の要素 $x \in K$ に対して
   $1 \cdot x = x \cdot 1 = x$ (乗算の単位元)
8. 任意の要素 $x \in K - \{0\}$ に対して，ある要素 $y \in K$ が存在して
   $x \cdot y = y \cdot x = 1$ (乗算の逆元)
9. 任意の要素 $x, y, z \in K$ に対して，$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ (分配性)

体：例

体であるもの の例

- $(\mathbb{R}, +, \cdot)$ ($\mathbb{R}$：実数全体の集合)
- $(\mathbb{C}, +, \cdot)$ ($\mathbb{C}$：複素数全体の集合)
- $(\mathbb{Q}, +, \cdot)$ ($\mathbb{Q}$：有理数全体の集合)

体でないもの の例

- $(\mathbb{Z}, +, \cdot)$ ($\mathbb{Z}$：整数全体の集合)
- $(\mathbb{R}^{2\times 2}, +, \cdot)$ ($\mathbb{R}^{2\times 2}$：2×2 実行列全体の集合)

疑問

$\mathbb{Z}/n\mathbb{Z}$ は加法 $+$，乗法 $\cdot$ を持つ

- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ は体か？

「加法の逆元」と「乗法の逆元」以外は成り立つことを既に述べた

加法と乗法の逆元

正の整数 $n \geq 2$ を固定

疑問？

$\mathbb{Z}/n\mathbb{Z}$ は次を満たすか？

1. 任意の $x \in \mathbb{Z}/n\mathbb{Z}$ に対して，ある $y \in \mathbb{Z}/n\mathbb{Z}$ が存在して
   $x + y = y + x = 0$ (加法の逆元)
2. 任意の $x \in (\mathbb{Z}/n\mathbb{Z}) - \{0\}$ に対して，ある $y \in \mathbb{Z}/n\mathbb{Z}$ が存在して
   $x \cdot y = y \cdot x = 1$ (乗法の逆元)

用語

1. この y を $-x$ と書くことが多い
2. この y を x^{-1} と書くことが多い

加法と乗法の逆元：例 1

$n = 5$ のとき

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

加法と乗法の逆元：例 1

$n = 5$ のとき

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- $0 + 0 = 0 + 0 = 0$
- $1 + 4 = 4 + 1 = 0$
- $2 + 3 = 3 + 2 = 0$
- $3 + 2 = 2 + 3 = 0$
- $4 + 1 = 1 + 4 = 0$

加法と乗法の逆元：例 1

$n = 5$ のとき

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- $0 + 0 = 0 + 0 = 0$
- $1 + 4 = 4 + 1 = 0$
- $2 + 3 = 3 + 2 = 0$
- $3 + 2 = 2 + 3 = 0$
- $4 + 1 = 1 + 4 = 0$

- $1 \cdot 1 = 1 \cdot 1 = 1$
- $2 \cdot 3 = 3 \cdot 2 = 1$
- $3 \cdot 2 = 2 \cdot 3 = 1$
- $4 \cdot 4 = 4 \cdot 4 = 1$

加法と乗法の逆元：例 2

$n = 6$ のとき

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

加法と乗法の逆元：例 2

$n = 6$ のとき

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $0 + 0 = 0 + 0 = 0$
- $1 + 5 = 5 + 1 = 0$
- $2 + 4 = 4 + 2 = 0$
- $3 + 3 = 3 + 3 = 0$
- $4 + 2 = 2 + 4 = 0$
- $5 + 1 = 1 + 5 = 0$

加法と乗法の逆元：例 2

$n = 6$ のとき

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $0 + 0 = 0 + 0 = 0$
- $1 + 5 = 5 + 1 = 0$
- $2 + 4 = 4 + 2 = 0$
- $3 + 3 = 3 + 3 = 0$
- $4 + 2 = 2 + 4 = 0$
- $5 + 1 = 1 + 5 = 0$

- $1 \cdot 1 = 1 \cdot 1 = 1$
- $2 \cdot y = y \cdot 2 = 1$ を満たす y はない
- $3 \cdot y = y \cdot 3 = 1$ を満たす y はない
- $4 \cdot y = y \cdot 4 = 1$ を満たす y はない
- $5 \cdot 5 = 5 \cdot 5 = 1$

加法の逆元

正の整数 $n \geq 2$ を固定

性質：加法の逆元

任意の $x \in \mathbb{Z}/n\mathbb{Z}$ に対して，
次を満たす $y \in \mathbb{Z}/n\mathbb{Z}$ がただ 1 つ存在する

$$x + y = y + x = 0$$

存在性と一意性を分けて証明する

加法の逆元：存在性

証明 (存在性) :任意の $x \in \mathbb{Z}/n\mathbb{Z}$ を考える

- $\boxed{y = (-x) \bmod n}$ とする
- このとき，$0 \leq y \leq n-1$ (つまり，$y \in \mathbb{Z}/n\mathbb{Z}$)
- また，

$$\begin{aligned} x + y &= x + ((-x) \bmod n) = (x + ((-x) \bmod n)) \bmod n \\ &= ((x \bmod n) + ((-x) \bmod n)) \bmod n \\ &= (x + (-x)) \bmod n = 0 \end{aligned}$$

- さらに，$y + x = x + y = 0$ □

加法の逆元：一意性

証明 (一意性) :任意の $x \in \mathbb{Z}/n\mathbb{Z}$ を考える

- $y \in \mathbb{Z}/n\mathbb{Z}$ が次を満たすとする
  $x + y = y + x = 0$
- つまり，$(x + y) \bmod n = 0$
- このとき，

$$
\begin{aligned}
y &= y \bmod n \\
&= ((x + y) - x) \bmod n \\
&= ((x + y) \bmod n + (-x \bmod n)) \bmod n \\
&= (0 + (-x \bmod n)) \bmod n \\
&= (-x \bmod n) \bmod n \\
&= -x \bmod n
\end{aligned}
$$

□

乗法の逆元

素数 $p \geq 2$ を固定

性質：乗法の逆元

任意の $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ に対して，
次を満たす $y \in \mathbb{Z}/p\mathbb{Z}$ がただ 1 つ存在する

$$x \cdot y = y \cdot x = 1$$

存在性と一意性を分けて証明する

- 証明には，次に挙げる性質を用いる

ベズーの等式

正整数 x, y，$x \geq y$

性質：ベズーの等式

$ax + by = \gcd(x, y)$ を満たす整数 a, b が存在する

証明：y に関する数学的帰納法で証明する

- $y = 1$ のとき，$\gcd(x, y) = 1$ なので，$a = 0, b = 1$ とすれば

$$\gcd(x, y) = 1 = y = ax + by$$

- $k \geq 2$ を 2 以上の任意の正整数とする
- $y \leq k - 1$ のときにベズーの等式が正しいとする
- 証明したいことは，
  $ax + bk = \gcd(x, k)$ となる整数 a, b が存在すること

ベズーの等式 (続)

正整数 x, y, $x \geq y$

性質：ベズーの等式

$ax + by = \gcd(x, y)$ を満たす整数 a, b が存在する

証明 (続)：

- ユークリッドのアルゴリズム (の原理) より，
  $\gcd(x, k) = \gcd(k, x \bmod k)$ で，$x \bmod k \leq k - 1$ なので，
  帰納法の仮定より，ある整数 a', b' が存在して

$$a'k + b'(x \bmod k) = \gcd(k, x \bmod k) = \gcd(x, k)$$

- ある整数 q に対して，$x = kq + (x \bmod k)$ なので，

$$\gcd(x, k) = a'k + b'(x - kq) = b'x + (a' - b'q)k$$

- $a = b'$, $b = a' - b'q$ とすればよい □

零因子の非存在性

素数 $p \geq 2$，整数 a, b

性質：零因子の非存在性

$ab \bmod p = 0$ ならば，$a \bmod p = 0$ または $b \bmod p = 0$

証明：$ab \bmod p = 0$ と仮定

- $0 = ab \bmod p = ((a \bmod p) \cdot (b \bmod p)) \bmod p$
- $\therefore$ ある整数 q が存在して，$(a \bmod p) \cdot (b \bmod p) = pq$
- $0 \leq a \bmod p < p, 0 \leq b \bmod p < p$ で，p は素数なので，

$$a \bmod p = 0 \text{ または } b \bmod p = 0$$ □

乗法の逆元：存在性

証明 (存在性) :任意の $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ を考える

- x を整数だと思うと，p は素数なので，$\gcd(x, p) = 1$
- ベズーの等式より，$ax + bp = 1$ を満たす整数 a, b が存在する
- したがって，$(ax + bp) \bmod p = 1 \bmod p = 1$ $(\because p \geq 2)$
- $(ax + bp) \bmod p = ax \bmod p = ((a \bmod p) \cdot (x \bmod p)) \bmod p$ なので，

$$((a \bmod p) \cdot (x \bmod p)) \bmod p = 1$$

- $((a \bmod p) \cdot (x \bmod p)) \bmod p = a \cdot x$ なので，

$$a \cdot x = 1$$

□

乗法の逆元：一意性

証明 (一意性) :任意の $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ を考える

- ある $a, a' \in \mathbb{Z}/p\mathbb{Z}$ に対して $a \cdot x = 1$ かつ $a' \cdot x = 1$ であるとする

- $a, a' \in \mathbb{Z}/p\mathbb{Z}$ なので， $a = a'$ □

乗法の逆元：一意性

証明 (一意性) :任意の $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ を考える

- ある $a, a' \in \mathbb{Z}/p\mathbb{Z}$ に対して $a \cdot x = 1$ かつ $a' \cdot x = 1$ であるとする
- このとき,

$$\begin{aligned} 0 &= (a \cdot x) - (a' \cdot x) \\ &= ((a \bmod p) \cdot (x \bmod p)) \bmod p \\ &\quad - ((a' \bmod p) \cdot (x \bmod p)) \bmod p \\ &= (((a - a') \bmod p) \cdot (x \bmod p)) \bmod p \end{aligned}$$

- $x \bmod p \neq 0$ なので, $(a - a') \bmod p = 0$
- $a, a' \in \mathbb{Z}/p\mathbb{Z}$ なので, $a = a'$ □

乗法の逆元：一意性

証明 (一意性) :任意の $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ を考える

- ある $a, a' \in \mathbb{Z}/p\mathbb{Z}$ に対して $a \cdot x = 1$ かつ $a' \cdot x = 1$ であるとする
- このとき,

$$\begin{aligned} 0 &= (a \cdot x) - (a' \cdot x) \\ &= ((a \bmod p) \cdot (x \bmod p)) \bmod p \\ &\quad - ((a' \bmod p) \cdot (x \bmod p)) \bmod p \\ &= (((a - a') \bmod p) \cdot (x \bmod p)) \bmod p \end{aligned}$$

- $x \bmod p \neq 0$ なので, $(a - a') \bmod p = 0$
- $(a - a') \bmod p = ((a \bmod p) - (a' \bmod p)) \bmod p$ なので

$$a \bmod p = a' \bmod p$$

- $a, a' \in \mathbb{Z}/p\mathbb{Z}$ なので, $a = a'$ □

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ は体か？

疑問 (再掲)

$\mathbb{Z}/n\mathbb{Z}$ は加法 $+$，乗法 $\cdot$ を持つ

- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ は体か？

「加法の逆元」と「乗法の逆元」以外は成り立つことを既に述べた

結論

n が素数 $\Rightarrow$ $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ は体

n が素数でない $\rightsquigarrow$ 次節の内容

加法の逆元：計算法 — 例 1

素数 89 に対して，$\mathbb{Z}/89\mathbb{Z}$ を考える

例 1

$(32 + x) \bmod 89 = 0$ を満たす $x \in \mathbb{Z}/89\mathbb{Z}$ は何か？

解答例：そのような x は $-32 \bmod 89$ であるが，これは

$$\begin{aligned} -32 \bmod 89 &= (-32 \bmod 89) + (89 \bmod 89) \\ &= ((-32 \bmod 89) + (89 \bmod 89)) \bmod 89 \\ &= ((-32 + 89) \bmod 89) \bmod 89 \\ &= (57 \bmod 89) \bmod 89 \\ &= 57 \end{aligned}$$

□

乗法の逆元：計算法 — 例 2

素数 89 に対して，$\mathbb{Z}/89\mathbb{Z}$ を考える

例 2

$32x \bmod 89 = 1$ を満たす $x \in \mathbb{Z}/89\mathbb{Z}$ は何か？

Step 1：ベズーの等式における係数を定める

- ユークリッドのアルゴリズムによって，$\gcd(89, 32) = \gcd(32, 25) = \gcd(25, 7) = \gcd(7, 4) = \gcd(4, 3) = \gcd(3, 1) = 1$
- したがって，

$$
\begin{aligned}
1 &= 3 - 2 \cdot 1 = 3 - 2 \cdot (4 - 3) = -2 \cdot 4 + 3 \cdot 3 \\
&= -2 \cdot 4 + 3 \cdot (7 - 4) = 3 \cdot 7 - 5 \cdot 4 \\
&= 3 \cdot 7 - 5 \cdot (25 - 3 \cdot 7) = -5 \cdot 25 + 18 \cdot 7 \\
&= -5 \cdot 25 + 18 \cdot (32 - 25) = 18 \cdot 32 - 23 \cdot 25 \\
&= 18 \cdot 32 - 23 \cdot (89 - 2 \cdot 32) = -23 \cdot 89 + 64 \cdot 32
\end{aligned}
$$

乗法の逆元：計算法 — 例 2 (続き)

素数 89 に対して，$\mathbb{Z}/89\mathbb{Z}$ を考える

例 2

$32x \bmod 89 = 1$ を満たす $x \in \mathbb{Z}/89\mathbb{Z}$ は何か？

Step 2：剰余に対する演算により，解を導出する

- ゆえに，

$$
\begin{aligned}
1 &= 1 \bmod 89 \\
&= (-23 \cdot 89 + 64 \cdot 32) \bmod 89 \\
&= ((-23 \cdot 89) \bmod 89 + (64 \cdot 32) \bmod 89) \bmod 89 \\
&= 64 \cdot 32 \bmod 89
\end{aligned}
$$

- 逆元の一意性より，$x = 64$ である □

乗法の逆元：計算法 — 例 3

素数 61 に対して，$\mathbb{Z}/61\mathbb{Z}$ を考える

例 3

$3x \bmod 61 = 1$ を満たす $x \in \mathbb{Z}/61\mathbb{Z}$ は何か？

解答例：

- ユークリッドのアルゴリズムによって，$\gcd(61, 3) = \gcd(3, 1) = 1$
- したがって，

$$1 = 3 - 2 \cdot 1 = 3 - 2 \cdot (61 - 20 \cdot 3) = -2 \cdot 61 + 41 \cdot 3$$

- ゆえに，

$$1 = 1 \bmod 61 = (-2 \cdot 61 + 41 \cdot 3) \bmod 61 = 41 \cdot 3 \bmod 61$$

- 逆元の一意性より，$x = 41$ である □

目次

有限体

定義：有限体

有限体 とは，K の要素数が有限であるような体 $(K, +, \cdot)$
$(K, +, \cdot)$ が有限体であるとき，要素数 $|K|$ をその体の **位数** という

今までの議論のまとめ：

- n が素数 $\Rightarrow$ $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ は有限体 (位数 $|\mathbb{Z}/n\mathbb{Z}| = n$)

疑問

n が素数ではないとき，位数 n の有限体は存在するか？

例として，$n = 4$ のときと $n = 6$ のときを考える

$\mathbb{Z}/4\mathbb{Z}$ の加算と乗算

$(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ は体ではない

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	4

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}/6\mathbb{Z}$ の加算と乗算

$(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ は体ではない

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

位数 4 の有限体は存在，位数 6 の有限体は非存在

事実

1. 位数 4 の有限体は存在する
2. 位数 6 の有限体は存在しない

- 「位数 6 の有限体が存在しない」ことを証明するのは大変なので，行わない
- 「位数 4 の有限体が存在する」ことを今から紹介する

事実：より一般的に

整数 $n \geq 2$ に対して

- n が素数のべきである $\Rightarrow$ 位数 n の有限体は存在する
- n が素数のべきではない $\Rightarrow$ 位数 n の有限体は存在しない

位数 4 の有限体：構成 (1)

次の行列の集合を考える

$$S = \left\{ O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, A^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\} \subseteq (\mathbb{Z}/2\mathbb{Z})^2$$

確認：例えば,

$$A^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} (0 \cdot 0) + (1 \cdot 1) & (0 \cdot 1) + (1 \cdot 1) \\ (1 \cdot 0) + (1 \cdot 1) & (1 \cdot 1) + (1 \cdot 1) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

$$A + I = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0+1 & 1+0 \\ 1+0 & 1+1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = A^2$$

位数 4 の有限体：構成 (1)

次の行列の集合を考える

$$S = \left\{ O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, A^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\} \subseteq (\mathbb{Z}/2\mathbb{Z})^2$$

$+$	O	I	A	A^2
O	O	I	A	A^2
I	I	O	A^2	A
A	A	A^2	O	I
A^2	A^2	A	I	O

$\cdot$	O	I	A	A^2
O	O	O	O	O
I	O	I	A	A^2
A	O	A	A^2	I
A^2	O	A^2	I	A

有限体の記号

事実：位数 q の有限体が存在するとき，それは本質的に 1 つに定まる

記号：有限体

位数 q の有限体を $\mathbb{F}_q$ または $\mathrm{GF}(q)$ で表す

今までの話より，q は素数のべきでなくてはならない

$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_4$	$\mathbb{F}_5$	$\mathbb{F}_6$	$\mathbb{F}_7$	$\mathbb{F}_8$	$\mathbb{F}_9$	$\mathbb{F}_{10}$	$\mathbb{F}_{11}$	$\mathbb{F}_{12}$	$\mathbb{F}_{13}$	$\mathbb{F}_{14}$
○	○	○	○	×	○	○	○	×	○	×	○	×

目次

今日のまとめ

今日の目標

整数の剰余について，次をできるようになる

- 整数の剰余に関する演算を行えるようになる

特に，素数が果たす役割を理解する $\rightsquigarrow$ 有限体

まとめ

n が素数である $\Leftrightarrow$ $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ は体である

格言

抽象化 は 数学の威力

目次