

1 次の体  $\mathbb{Z}/p\mathbb{Z}$  とその元  $a \in \mathbb{Z}/p\mathbb{Z}$  に対し,  $a$  の乗法逆元  $a^{-1}$  を求めよ.

(1)  $\mathbb{Z}/5\mathbb{Z}, a = 3$

(2)  $\mathbb{Z}/17\mathbb{Z}, a = 8$

(3)  $\mathbb{Z}/101\mathbb{Z}, a = 33$

(解答) (1)  $a^{-1} = 2$  (2)  $a^{-1} = 15$  (3)  $a^{-1} = 49$

(解説) (3) のみ紹介する. 不定方程式  $ax + py = 1$  を解けば良い (実際は一つの解を与えるだけで良い). したがってこの場合は

$$33x + 101y = 1 \quad (\heartsuit)$$

を解くことになる. 101 と 33 に対しユークリッドの互除法を適用すると

$$101 = 33 \times 3 + 2$$

$$33 = 2 \times 16 + 1$$

となる. したがって

$$\begin{aligned} 1 &= 33 - 2 \times 16 \\ &= 33 - (101 - 33 \times 3) \times 16 \\ &= 33 \times (1 + 3 \times 16) - 101 \times 16 \\ &= 33 \times 49 - 101 \times 16 \end{aligned}$$

となる.  $(\heartsuit)$  のひとつの解は  $(x, y) = (49, -16)$  である. 式

$$33 \cdot 49 + 101 \cdot (-16) = 1$$

において  $\text{mod } 101$  を取ると

$$33 \cdot 49 \equiv 1 \pmod{101}$$

を得る. したがって  $33^{-1} = 49$  となる.

2 (1) 環  $\mathbb{Z}/15\mathbb{Z}$  における零因子を求めよ.

(2) 環  $\mathbb{Z}/12\mathbb{Z}$  におけるべき零元を求めよ.

(3) 素数  $p \in \mathbb{Z}$  に対し, 環  $\mathbb{Z}/p\mathbb{Z}$  が整域になることを示せ.

(解答)

(1) 整数  $n \in \mathbb{Z}, n > 0$  に対し, 環  $\mathbb{Z}/n\mathbb{Z}$  において

$$a \in \mathbb{Z}/n\mathbb{Z} \text{ が零因子} \iff a \text{ と } n \text{ は互いに素でない (すなわち } \gcd(a, n) > 1)$$

が成り立つ. したがって  $\mathbb{Z}/15\mathbb{Z}$  の零因子は  $0, 3, 5, 6, 9, 10, 12$  である.

(2)  $0, 6$

$$(12 = 2 \times 3^2 \text{ より, } a \in \mathbb{Z}/12\mathbb{Z} \text{ がべき零元} \iff \text{ある } n > 0 \text{ が存在し } a^n \equiv 0 \pmod{12} \iff 6 \mid a.)$$

(3)  $p$  は素数であるため, 整数  $a, b \in \mathbb{Z}$  に対し  $p \mid ab$  ならば  $p \mid a$  または  $p \mid b$  が成り立つ. したがって  $p$  を法として  $a \not\equiv 0$  かつ  $b \not\equiv 0$  ならば,  $ab \not\equiv 0$  である.

3  $p$  が素数のとき,

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$$

が剰余類の演算 ( $a, b \in \mathbb{Z}/p\mathbb{Z}$  に対し, 和と積をそれぞれ  $a + b \pmod{p}$  と  $ab \pmod{p}$  により定義する) のもとで体になることを示せ.

(解答)

(1) 和に関して  $\mathbb{Z}/p\mathbb{Z}$  は可換群になる.

(2)  $p$  は素数であるため, 整数  $a, b \in \mathbb{Z}$  に対し  $p \mid ab$  ならば  $p \mid a$  または  $p \mid b$  が成り立つ. したがって  $p$  を法として  $a \not\equiv 0$  かつ  $b \not\equiv 0$  ならば,  $ab \not\equiv 0$  である. このことから

$$(\mathbb{Z}/p\mathbb{Z})^\times := \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$$

は乗法について閉じている. また合同式の性質によって,  $(\mathbb{Z}/p\mathbb{Z})^\times$  は乗法に関する結合法則を満たし, 1 はその単位元となる. 最後に乗法逆元の存在を示す.  $a \not\equiv 0 \pmod{p}$  とすると, 不定方程式

$$ax + py = 1$$

は整数解  $x, y \in \mathbb{Z}$  をもつ. したがって, 合同式

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

は (ただ一つの) 解をもつ. このことは任意の  $a \in (\mathbb{Z}/p\mathbb{Z})^\times$  に乗法逆元  $a^{-1}$  が存在することを意味する. したがって,  $(\mathbb{Z}/p\mathbb{Z})^\times$  は乗法群である.

(3) 任意の整数  $n$  について  $\mathbb{Z}/n\mathbb{Z}$  は環となる. したがって  $n$  が素数  $p$  のときも,  $\mathbb{Z}/p\mathbb{Z}$  は分配法則を満たす.

---

<sup>1</sup>※この講義に関する情報はホームページを参照. <https://hirokazunasu.github.io/2025/alg2.html>