

13. 剰余体

代数 II

法5の剰余類(剰余環, 整域, 体)

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

+	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

加法群

加法単位元 0

加法において逆元が存在

乗法に関して結合律を満たす

乗法単位元 1

加法と乗法に関して分配律を満たす

$$x(y + z) = xy + xz$$

$$\text{例) } 1(2 + 3) = 2 + 3 = 0$$

逆元について

1については1

2については3

3については2

4については4

合同式に関する定理

定理m1

n を1より大きい整数とする. このとき, 任意の整数 a, b, c, d について, 次のことが成り立つ

(1) 反射律: $a \equiv a \pmod{n}$

(2) 対称律: $a \equiv b \pmod{n}$ ならば, $b \equiv a \pmod{n}$

(3) 推移律: $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ ならば $a \equiv c \pmod{n}$

(4) $a \equiv b \pmod{n}$ かつ $c \equiv d \pmod{n}$ ならば,

$$a \pm c \equiv b \pm d \pmod{n}, a \cdot c \equiv b \cdot d \pmod{n}$$

定理m2

n を1より大きい整数とする. このとき, 任意の整数 m, a, b について,

$d = (m, n), n = n'd, m = m'd$ とおくとき, 次のことが成り立つ

$$ma \equiv mb \pmod{n} \Leftrightarrow a \equiv b \pmod{n'}$$

とくに, $(m, n) = 1$ のとき, $ma \equiv mb \pmod{n} \Leftrightarrow a \equiv b \pmod{n}$

定理m3

a, b を整数, m, n を1より大きい整数とする. $(m, n) = 1$ であれば, 次のことが成り立つ

$$a \equiv b \pmod{m}, a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{mn}$$

合同式に関する定理

定理m4

$(a, n) = 1$ ならば, $ax \equiv b \pmod{n}$ を満足する整数解 x が存在し,
 n を法としてただ一つである.

定理m5

$ax \equiv b \pmod{n}$ が解をもつための必要十分条件は $(a, n) | b$ となることである.

定理m6

合同方程式 $ax \equiv b \pmod{n}$ が解をもち $(a, n) = d > 1$ であるなれば,
解の個数は n を法として d 個である.

定理m7 (中国剰余の定理)

n_1, \dots, n_s を1より大きい整数とし, $(n_i, n_j) = 1 (i \neq j)$ とする.
このとき, 任意の整数の組 a_1, \dots, a_s に対して連立合同式
 $x \equiv a_1 \pmod{n_1}, \dots, x \equiv a_s \pmod{n_s}$
は, $n = n_1 \dots n_s$ を法として唯1つの解をもつ.

練習問題(4回目)

(1) $9x + 15y = 6$

$$9x \equiv 6 \pmod{15}$$

$$(9,15) = 3$$

3個の解をもつ

定理m2から

$$3x \equiv 2 \pmod{5}$$

両辺を2倍して

$$x \equiv 4 \pmod{5}$$

法15では

$$x \equiv 4, 9, 14 \pmod{15}$$

(2) $8x + 12y = 5$

$$(8,12) = 4$$

4は5の約数ではない

ので、解は無し

(3) $31x + 56y = 3$

$$(31,56) = 1$$

解はある

(4) $3x^2 - x \equiv 2 \pmod{7}$

$$(3x+2)(x-1) \equiv 0 \pmod{7}$$

$$3x+2 \equiv 0 \pmod{7} \text{ または } x-1 \equiv 0 \pmod{7}$$

$$3x+2 \equiv 0 \pmod{7}$$

$$3x \equiv -2 \pmod{7}$$

両辺5倍

$$x \equiv -10 \equiv 4 \pmod{7}$$

答え

$$x \equiv 4 \pmod{7} \text{ または } x \equiv 1 \pmod{7}$$

$$(5) 41x + 310y = 10$$

$(41, 310) = 1$ 唯一つの解をもつ

$$310 = 41 \times 7 + 23 \text{より}$$

$$287x \equiv 70 \pmod{310}$$

$$-23x \equiv 70 \pmod{310}$$

元の式と足して

$$18x \equiv 80 \pmod{310}$$

$$-5x \equiv 150 \pmod{310}$$

両辺4倍

$$-20x \equiv 600 \pmod{310}$$

$$-2x \equiv 680 \equiv 60 \pmod{310}$$

$$-4x \equiv 120 \pmod{310}$$

$$5x \equiv -150 \pmod{310}$$

$$x \equiv -30 \equiv 280 \pmod{310}$$

連立合同式

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

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

$$(2) \begin{cases} 2x \equiv 3(\text{mod } 7) \\ 5x \equiv 1(\text{mod } 11) \end{cases}$$

$$(4) \begin{cases} x \equiv 1(\text{mod } 3) \\ x \equiv 2(\text{mod } 5) \\ x \equiv 6(\text{mod } 11) \end{cases}$$

剰余体

- 法 p (素数)の剰余類の集合

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$$

– 完全剰余系(普通剰余)

$$a \in \mathbb{Z}_p, (a, p) = 1$$

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