

自然数 n に対し,

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$$

を n を法とする \mathbb{Z} の剰余類環とする.

1 次の自然数 n に対し, n を法とする \mathbb{Z} の既約剰余類をすべて列挙せよ. なお答えは $\mathbb{Z}/n\mathbb{Z}$ の部分集合 (すなわち既約剰余類群 $(\mathbb{Z}/n\mathbb{Z})^\times$) として答えること:

- (1) $n = 2$ (2) $n = 4$ (3) $n = 18$ (4) $n = 30$

2 剰余類環 $\mathbb{Z}/n\mathbb{Z}$ の元 a に対し, a の乗法逆元を $a^{-1} \pmod n$ で表す. 次の元を求めよ.

- (1) $3^{-1} \pmod 7$
 (2) $8^{-1} \pmod{11}$
 (3) $12^{-1} \pmod{19}$
 (4) $15^{-1} \pmod{34}$
 (5) $26^{-1} \pmod{39}$
 (6) $25^{-1} \pmod{101}$
 (7) $23^{-1} \pmod{130}$
 (8) $123^{-1} \pmod{199}$

3 (1) 14 を法とする \mathbb{Z} の既約剰余類のなす群 $(\mathbb{Z}/14\mathbb{Z})^\times$ の乗法演算表を完成させよ.

| | | | | | | |
|----------|---|---|---|---|----|----|
| \times | 1 | 3 | 5 | 9 | 11 | 13 |
| 1 | | | | | | |
| 3 | | | | | | |
| 5 | | | | | | |
| 9 | | | | | | |
| 11 | | | | | | |
| 13 | | | | | | |

- (2) $11^{-1} \pmod{14}$ を答えよ.

¹解答:

1 (1) $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ (2) $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ (3) $(\mathbb{Z}/18\mathbb{Z})^\times = \{1, 5, 7, 11, 13, 17\}$ (4) $(\mathbb{Z}/30\mathbb{Z})^\times = \{1, 7, 11, 13, 17, 19, 23, 29\}$

2 (1) 5 (2) 7 (3) 8 (4) 25 (5) $\gcd(26, 39) = 13 \neq 1$ より, 逆元 $26^{-1} \pmod{39}$ は存在しない. (6) 97 (7) 17 (8) 144

3 (1)
$$\begin{bmatrix} 1 & 3 & 5 & 9 & 11 & 13 \\ 3 & 9 & 1 & 13 & 5 & 11 \\ 5 & 1 & 11 & 3 & 13 & 9 \\ 9 & 13 & 3 & 11 & 1 & 5 \\ 11 & 5 & 13 & 1 & 9 & 3 \\ 13 & 11 & 9 & 5 & 3 & 1 \end{bmatrix}$$
 (2) 9

¹※この講義に関する情報はホームページを参照. <http://fuji.ss.u-tokai.ac.jp/nasu/2020/alg0.html>