

1 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ において次の元を計算せよ. 解答)

$$(1) (8, 2) + (7, 5) = (2, 2) + (1, 0) = (0, 2)$$

$$(2) (4, -1) + (5, 8) = (1, -1) + (2, 3) = (0, 2)$$

$$(3) (16, 21) + (-37, -33) = (1, 1) + (-1, -3) = (0, -2) = (0, 3)$$

2 次の連立合同方程式を解け.

$$(1) \begin{cases} x \equiv 3 \pmod{7} \\ x \equiv -2 \pmod{11} \end{cases}$$

解答) 合同方程式

$$\begin{cases} 11t_1 \equiv 1 \pmod{7} \\ 7t_2 \equiv 1 \pmod{11} \end{cases}$$

の解を求めると $t_1 \equiv 2 \pmod{7}$, $t_2 \equiv 8 \pmod{11}$. よって求める解は

$$x = 3 \cdot 11 \cdot 2 + (-2) \cdot 7 \cdot 8 = 66 - 112 = -46 \equiv 31 \pmod{77}$$

$$(2) \begin{cases} 3x \equiv -5 \pmod{4} \\ 4x \equiv 6 \pmod{13} \end{cases}$$

解答) $3^{-1} = 3 \pmod{4}$. $4^{-1} = 10 \pmod{13}$. よって合同方程式

$$\begin{cases} x \equiv -5 \cdot 3 \equiv 1 \pmod{4} \\ x \equiv 6 \cdot 10 \equiv 8 \pmod{13} \end{cases}$$

を解けば良い. (1) と同様に解けば, $x \equiv 21 \pmod{52}$.

$$(3) \begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

解答) 合同方程式

$$\begin{cases} 8 \cdot 9t_1 \equiv 1 \pmod{5} \\ 5 \cdot 9t_2 \equiv 1 \pmod{8} \\ 5 \cdot 8t_3 \equiv 1 \pmod{9} \end{cases}$$

を解く. $8 \cdot 9 \equiv 3 \cdot 4 \equiv 2 \pmod{5}$. したがって 1 式より $2t_1 \equiv 1 \pmod{5}$. よって $t_1 \equiv 3 \pmod{5}$.
同様に $t_2 \equiv 5 \pmod{8}$, $t_3 \equiv 7 \pmod{9}$ を得る. よって,

$$x = 2 \cdot 72 \cdot 3 + 3 \cdot 45 \cdot 5 + 4 \cdot 40 \cdot 7 \equiv 67 \pmod{360}.$$

■

$$(4) \begin{cases} x \equiv 13 \pmod{20} \\ x \equiv -12 \pmod{21} \\ x \equiv -7 \pmod{23} \end{cases}$$

解答) 合同方程式

$$\begin{cases} 21 \cdot 23t_1 \equiv 1 \pmod{20} \\ 20 \cdot 23t_2 \equiv 1 \pmod{21} \\ 20 \cdot 21t_3 \equiv 1 \pmod{23} \end{cases}$$

を解く. $t_1 \equiv 7 \pmod{20}$, $t_2 \equiv 10 \pmod{21}$, $t_3 \equiv 4 \pmod{23}$ となる. よって,

$$x = 13 \cdot 21 \cdot 23 \cdot 7 + (-12) \cdot 20 \cdot 23 \cdot 10 + (-7) \cdot 20 \cdot 21 \cdot 4 \equiv 5973 \pmod{9660}.$$

■

- [3] 群 $\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が同型でないことを示せ. (ヒント: 前者には位数 4 の元が存在するが, 後者の元の位数は 2 または 1 であることを用いると良い. 両者の間に同型写像があったとして矛盾を導け.)

解答) 同型写像 $\varphi: \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が存在すると仮定する. このとき, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ の任意の元は 2 倍すると零に等しいので,

$$\varphi(2 \pmod{4}) = \varphi(1 + 1 \pmod{4}) = 2\varphi(1 \pmod{4}) = (0 \pmod{2}, 0 \pmod{2}).$$

一方, $2 \pmod{4} \neq 0$ より φ が単射であることに反する.

■