代数学 I 第 2 回レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

$756x + 1064y = 56$ を満たす整数の組 (x, y) を全て求めよ.

問題 1 解答例. まず，$\gcd(756, 1064)$ をユークリッド互除法で求める：

$$1064 = 1 \times 756 + 308 \qquad 756 = 2 \times 308 + 140$$
$$308 = 2 \times 140 + 28 \qquad 140 = 5 \times 28 + 0$$

であるので，$\gcd(756, 1064) = 28$. よって，$756x + 1064y = 56 (= 2 \times 28)$ を満たす整数の組 (x, y) は存在し，その 1 つは以下のように求められる.

$$\begin{aligned} 56 = 2 \times 28 &= 2 \times (308 - 2 \times 140) = 2 \times 308 + (-4) \times 140 \\ &= 2 \times 308 + (-4) \times (756 - 2 \times 308) = (-4) \times 756 + 10 \times 308 \\ &= (-4) \times 756 + 10 \times (1064 - 1 \times 756) = (-14) \times 756 + 10 \times 1064 \end{aligned}$$

より，$(x, y) = (-14, 10)$ が $756x + 1064y = 56$ を満たす整数の組 (x, y) の例である. これより，一般に，

$$\begin{aligned} 756x + 1064y = 56 &\Leftrightarrow 756(x + 14) + 1064(y - 10) = 0 \\ &\Leftrightarrow 27(x + 14) + 38(y - 10) = 0 \text{ (両辺を } \gcd(756, 1064) = 28 \text{ で割った)} \\ &\Leftrightarrow \text{ある } t \in \mathbb{Z} \text{ を用いて，} (x + 14, y - 10) = (38t, -27t) \end{aligned}$$

となるので，求める整数の組は，$(x, y) = (-14 + 38t, 10 - 27t), t \in \mathbb{Z}$. □

問題 2

乗法群 $(\mathbb{Z}/15\mathbb{Z})^\times$ の元を具体的に全て求め，各 $[a]_{15} \in (\mathbb{Z}/15\mathbb{Z})^\times$ に対する $([a]_{15})^{-1}$ を全て求めよ.

問題 2 解答例. $(\mathbb{Z}/15\mathbb{Z})^\times = \{[a]_{15} \mid 0 \leq a \leq 14, \gcd(a, 15) = 1\}$ より，

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}.$$

さらに，

$$[1]_{15}^{-1} = [1]_{15} \qquad [2]_{15}^{-1} = [8]_{15} \qquad [4]_{15}^{-1} = [4]_{15} \qquad [7]_{15}^{-1} = [13]_{15}$$
$$[8]_{15}^{-1} = [2]_{15} \qquad [11]_{15}^{-1} = [11]_{15} \qquad [13]_{15}^{-1} = [7]_{15} \qquad [14]_{15}^{-1} = [14]_{15}$$

である. (これらは例えば次のように全て直接確かめられる：$[2]_{15} \times [8]_{15} = [16]_{15} = [1]_{15}$.) □

問題 2 の $([a]_{15})^{-1}$ を求める部分は，候補が限られているので，解答中に書いたように全て直接調べても (これくらいの大きさだと) 苦ではない. しかし，もう少し一般的な方法もここで解説しておく. $(\mathbb{Z}/n\mathbb{Z})^\times$ の元を具体的に求めた部分の議論を思い出すと，

$$[a]_n \times [x]_n = [1]_n \Leftrightarrow [ax]_n = [1]_n \Leftrightarrow \text{ある } y \in \mathbb{Z} \text{ が存在して，} ax + ny = 1.$$

であった (このため，a が n と互いに素であることが逆元を持つことの必要十分条件となるのであった).

* *e-mail* : hoya@shibaura-it.ac.jp

よって，n と互いに素である a に対して，

$$ax + ny = 1 \text{ を満たす整数の組 } (x, y) \text{ を求めれば，} [x]_n \text{ が } ([a]_n)^{-1}$$

となる．そして，このような整数の組は拡張ユークリッド互除法で一般的に求められる．これが一般の場合の逆元の求め方である．

解答例 2 の場合で $ax + 15y = 1$ との対応を確かめてみると，

$$\begin{array}{rrr} 1 \times 1 + 15 \times 0 = 1 & 2 \times 8 + 15 \times (-1) = 1 & 4 \times 4 + 15 \times (-1) = 1 \\ 7 \times 13 + 15 \times (-6) = 1 & 11 \times 11 + 15 \times (-8) = 1 & 14 \times 14 + 15 \times (-13) = 1 \end{array}$$

である．拡張ユークリッド互除法を用いても良いし，もちろん暗算でできればそれでよい．