代数学 I 第 3 回レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

$\mathbb{Z}/80\mathbb{Z}$ において，$[9x]_{80} = [35]_{80}$ が成立するとき，$[x]_{80} \in \mathbb{Z}/80\mathbb{Z}$ を具体的に求めよ．

問題 1 解答例. $\gcd(9, 80) = 1$ なので，$[9]_{80}$ は $\mathbb{Z}/80\mathbb{Z}$ において $\times$ に関する逆元 $[9]_{80}^{-1}$ を持つ．よって，

$$[9x]_{80} = [35]_{80} \quad \Leftrightarrow \quad [9]_{80}^{-1}[9]_{80}[x]_{80} = [9]_{80}^{-1}[35]_{80} \quad \Leftrightarrow \quad [x]_{80} = [9]_{80}^{-1}[35]_{80}$$

なので，$[9]_{80}^{-1}$ を求めればよい．まず，$9x + 80y = 1$ を満たす整数の組 (x, y) を拡張ユークリッド互除法で求める：

$$80 = 8 \times 9 + 8 \qquad 9 = 1 \times 8 + 1 \qquad 8 = 8 \times 1 + 0$$

であるので，

$$\begin{aligned} 1 &= 9 - 1 \times 8 \\ &= 9 + (-1) \times (80 - 8 \times 9) \\ &= 9 \times 9 + (-1) \times 80 \end{aligned}$$

より，$(x, y) = (9, -1)$ が $9x + 80y = 1$ を満たす整数の組の例である．よって，$[9]_{80}^{-1} = [9]_{80}$．よって，求める $[x]_{80}$ は $[x]_{80} = [9]_{80}^{-1}[35]_{80} = [9]_{80}[35]_{80} = [315]_{80} = [75]_{80}$． □

問題 1 補足解説. 一次方程式 $9x = 35$ を解くためには両辺を 9 で割る，つまり，両辺に 9^{-1} を掛ければ良いのであった．これと同じことを，$\mathbb{Z}/80\mathbb{Z}$ における $\times$ に関する逆元を用いて行えばよい． □

問題 2

5 以上の任意の素数 p に対し，$2^{p-2} + 3^{p-2} + 6^{p-2}$ を p で割った余りは 1 であることを証明せよ．

問題 2 解答例. $[2^{p-2} + 3^{p-2} + 6^{p-2}]_p = [1]_p$ であることを示せばよい．いま，p は 5 以上の素数なので，$\gcd(p, 6) = 1$ である，よって，$[6]_p$ は $\mathbb{Z}/p\mathbb{Z}$ において $\times$ に関する逆元 $[6]_p^{-1}$ を持つ．よって，

$$[2^{p-2} + 3^{p-2} + 6^{p-2}]_p = [1]_p \;\Leftrightarrow\; [6]_p[2^{p-2} + 3^{p-2} + 6^{p-2}]_p = [6]_p[1]_p \;\Leftrightarrow\; [3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1}]_p = [6]_p$$

となるので，$[3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1}]_p = [6]_p$ を示せばよい．

フェルマーの小定理より，

$$[2^{p-1}]_p = [3^{p-1}]_p = [6^{p-1}]_p = [1]_p$$

なので，$[3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1}]_p = [3]_p[2^{p-1}]_p + [2]_p[3^{p-1}]_p + [6^{p-1}]_p = [3]_p[1]_p + [2]_p[1]_p + [1]_p = [6]_p$．よって，示すべきことは示された． □

問題 2 補足解説. フェルマーの小定理の応用問題である．ちなみに，$p = 2$ とすると，$2^{p-2} + 3^{p-2} + 6^{p-2} = 1 + 1 + 1 = 3$ なので，2 で割った余りは 1 であり，$p = 3$ とすると，$2^{p-2} + 3^{p-2} + 6^{p-2} = 2 + 3 + 6 = 11$ なので，3 で割った余りは 2 である．よって，『$2^{p-2} + 3^{p-2} + 6^{p-2}$ を p で割った余りは 1』が成立しない p は $p = 3$ だけである． □

* *e-mail*：hoya@shibaura-it.ac.jp