代数学 I 第 1 回レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

$\mathbb{Z}/25\mathbb{Z}$ において次の値の計算結果を $[n]_{25}(0 \leq n \leq 24)$ の形で答えよ．

(1) $[43]_{25} + [72]_{25}$

(2) $[35]_{25} \times [4]_{25}$

問題 1 解答例.

(1) $[43]_{25} + [72]_{25} = [43 + 72]_{25}[115]_{25} = [15]_{25}$. □

(2) $[35]_{25} \times [4]_{25} = [35 \times 4]_{25} = [140]_{25} = [15]_{25}$. □

問題 2

23^{20} を 3 で割った余りを求めよ．

問題 2 解答例 1. $[23^{20}]_3 = [r]_3$ を満たす $r(0 \leq r < 3)$ が求める余りである．今，

$$[23^{20}]_3 = [23]_3^{20} = [-1]_3^{20} = [(-1)^{20}]_3 = [1]_3$$

より，求める余りは 1 である． □

問題 2 解答例 2(フェルマーの小定理). $[23^{20}]_3 = [r]_3$ を満たす $r(0 \leq r < 3)$ が求める余りである．フェルマーの小定理より，各 $n \in \mathbb{Z}_{>0}$ に対して，

$$[23]_3^{3^n} = [23^3]_3^{3^{n-1}} = [23]_3^{3^{n-1}} = \cdots = [23]_3^3 = [23]_3.$$

であるので，

$$[23^{20}]_3 = ([23]_3^{3^2})^2 \times [23]_3^2 = [23]_3^2 \times [23]_3^2 = [23]_3^4 = [23]_3^3 \times [23]_3 = [23]_3 \times [23]_3 = [23]_3^2 = [529]_3 = [1]_3.$$

よって，求める余りは 1 である． □

問題 2 の解答例 2 の方法を一般化して考えると，以下のことが言える．

p を素数，$n \in \mathbb{Z}_{>0}(:= \{\text{ 正の整数 }\})$ とし，

$$n = n_s p^s + n_{s-1} p^{s-1} + \cdots + n_1 p + n_0 \ (1 \leq n_s, \ldots, n_1, n_0 \leq p - 1)$$

と書く.($n_s n_{s-1} \ldots n_1 n_0$ は n の p 進法表示.) このとき，フェルマーの小定理より，各 $a \in \mathbb{Z}$ に対して，

$$[a]_p^n = [a]_p^{n_s + n_{s-1} + \cdots + n_1 + n_0}$$

となる．これを繰り返し用いれば，$[a]_p^n$ を $[a]_p^{n'}$ $(1 \leq n' \leq p - 1)$ の形にすることができる．

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