代数学 I 第 4 回本レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

$\mathbb{Z}/1024\mathbb{Z}$ において，

$$[501x]_{1024} = [4]_{1024}$$

を満たす0 以上 1023 以下の自然数 x を半角数字で入力せよ．

問題 1 解答例. $1024 = 2^{10}$ なので, $\gcd(1024, 501) = 1$ である．よって，$[501]_{1024}$ は $\times$ に関する逆元 $[501]_{1024}^{-1}$ を持つ．よって，

$$[501x]_{1024} = [4]_{1024} \quad \Leftrightarrow \quad [501]_{1024}^{-1}[501]_{1024}[x]_{1024} = [501]_{1024}^{-1}[4]_{1024} \quad \Leftrightarrow \quad [x]_{1024} = [501]_{1024}^{-1}[4]_{1024}$$

より，$[501]_{1024}^{-1}$ を求めれば良い．このために，$501x + 1024y = 1$ 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．

$$1024 = 2 \times 501 + 22 \qquad 501 = 22 \times 22 + 17 \qquad 22 = 1 \times 17 + 5$$
$$17 = 3 \times 5 + 2 \qquad 5 = 2 \times 2 + 1 \qquad 2 = 2 \times 1 + 0$$

であるので，

$$\begin{aligned}
1 &= 5 - 2 \times 2 \\
&= 5 + (-2) \times (17 - 3 \times 5) \\
&= 7 \times 5 + (-2) \times 17 \\
&= 7 \times (22 - 1 \times 17) + (-2) \times 17 \\
&= 7 \times 22 + (-9) \times 17 \\
&= 7 \times 22 + (-9) \times (501 - 22 \times 22) \\
&= 205 \times 22 + (-9) \times 501 \\
&= 205 \times (1024 - 2 \times 501) + (-9) \times 501 \\
&= 205 \times 1024 + (-419) \times 501.
\end{aligned}$$

つまり，$(x_0', y_0') = (-419, 205)$ が $501x + 1024y = 1$ を満たす整数の組の 1 つである．これより，

$$[501]_{1024}^{-1} = [-419]_{1024} = [605]_{1024}$$

である．これより，

$$[501x]_{1024} = [4]_{1024} \quad \Leftrightarrow \quad [x]_{1024} = [605]_{1024}[4]_{1024} = [2420]_{1024} = [372]_{1024}$$

よって，求める x は 372. □

問題 1 補足解説. 実数の範囲で一次方程式 $501x = 4$ を解くためには両辺を 501 で割ればよかった．今 $\mathbb{Z}/1024\mathbb{Z}$ の中で考えているので，普通の意味で 501 で割ることはできないが，$[501]_{1024}^{-1}$ が存在するので，両辺にこれを掛ければやはりこの一次方程式の解が求まるのである ($\mathbb{Z}/1024\mathbb{Z}$ の世界においては $[501]_{1024}^{-1}$ を掛けることが “501 で割る” ことに他ならない)．逆元の求め方については，第 4 回講義資料の 3.2 節を参照せよ．

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

なお，今回は逆元を学習したので解答例のような解き方をしたが，

$$[501x]_{1024} = [4]_{1024} \quad \Leftrightarrow \quad \text{ある } y \in \mathbb{Z} \text{ が存在して，} 501x + 1024y = 4$$

なので，$501x + 1024y = 4$ の整数解を拡張ユークリッド互除法で求めて解いても良い．この場合も結局 $501x + 1024y = 1$ の整数解をまず求めることになるので，計算的にはほぼ変わらない． □

問題 2

$\varphi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ をオイラーの φ 関数とする．このとき，

$$\varphi(625) = \boxed{\text{ア}}$$

である．$\boxed{\text{ア}}$ に入る自然数を半角数字で入力せよ．なお，自然数なので 2 桁以上の数もあり得ることに注意せよ．

問題 2 解答例. $625 = 5^4$ である．これより，$1 \leq m \leq 625$ に対し，

$$\gcd(m, 625) = 1 \quad \Leftrightarrow \quad m \text{ は } 5 \text{ の倍数ではない}$$

となる．1 以上 625 以下の 5 の倍数は $625 \div 5 = 125$ 個あるので，

$$\varphi(625) = 625 - 125 = 500.$$

□

問題 2 補足解説. 本問の方法は 5 を一般の素数 p に変えても上手く行くことがわかる．つまり以下の定理が同様に証明される．

定理

p を素数とし，$k \in \mathbb{Z}_{>0}$ とする．このとき，

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

証明. p は素数なので，$1 \leq m \leq p^k$ に対し，

$$\gcd(m, p^k) = 1 \quad \Leftrightarrow \quad m \text{ は } p \text{ の倍数ではない}$$

となる．1 以上 p^k 以下の p の倍数は $p^k \div p = p^{k-1}$ 個あるので，

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

□

なお，この定理は実は次のように一般化される．

定理

$n \in \mathbb{Z}_{>0}$ に対し，

$$\varphi(n) = n \prod_{p:\text{素数}, p \mid n} \left(1 - \frac{1}{p}\right).$$

ここで，$p \mid n$ は「p が n を割り切る」という意味で，$\prod_{p:\text{素数}, p \mid n}$ は「n を割り切る素数 p に渡って積を取る」という記号である ($\sum$ の掛け算バージョン)．

ここではこの定理の証明は行わないが，n と互いに素な自然数を数える時に「n の素因数の倍数を除いていく」という方法を念頭におくと証明をすることができる．この定理を用いれば例えば，以下のような定理も容易に証明できる．

定理

$m, n \in \mathbb{Z}_{>0}$ に対し，$\gcd(m,n) = 1$ であれば，

$$\varphi(mn) = \varphi(m)\varphi(n).$$

この定理と初めの定理を合わせて考えれば，例えば

$$\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2)\varphi(3) = (2^2 - 2)(3 - 1) = 4$$

というような計算も可能になる． □

問題 3

乗法群 $(\mathbb{Z}/7\mathbb{Z})^\times$ の以下の部分集合がそれぞれ $(\mathbb{Z}/7\mathbb{Z})^\times$ の部分群であるかどうかを判定せよ．

(1) $\{[1]_7, [2]_7, [4]_7, [6]_7\}$.
(2) $\{[1]_7, [2]_7, [4]_7\}$.

問題 3 解答例.

(1) $H_1 \coloneqq \{[1]_7, [2]_7, [4]_7, [6]_7\}$ とする．H_1 が $(\mathbb{Z}/7\mathbb{Z})^\times$ の部分群であるためには，任意の $[a]_7, [b]_7 \in H_1$ に対して，$[a]_7[b]_7 = [ab]_7 \in H_1$ となる必要がある．しかし，$[2]_7, [6]_7 \in H_1$ に対し，

$$[2]_7[6]_7 = [12]_7 = [5]_7 \notin H_1$$

となるので，H_1 は $(\mathbb{Z}/7\mathbb{Z})^\times$ の部分群とはならない．

(2) $H_2 \coloneqq \{[1]_7, [2]_7, [4]_7\}$ とする．$[2]_7^3 = [8]_7 = [1]_7$ に注意すると，$[2]_7^{-1} = [2]_7^2 = [4]_7$ でもあるので，任意の $k \in \mathbb{Z}$ に対し，$[2]_7^k$ は $[1]_7, [2]_7, [4]_7$ のいずれかに一致する (k が負の値のとき，$[2]_7^k$ は $[2]_7^{-1}$ の $-k$ 乗を意味する)．よって，

$$H_2 = \{[2]_7^k \mid k \in \mathbb{Z}\}$$

である．これより，任意の $k_1, k_2 \in \mathbb{Z}$ に対し，

$$[2]_7^{k_1}[2]_7^{k_2} = [2]_7^{k_1+k_2} \in H_2, \qquad ([2]_7^{k_1})^{-1} = [2]_7^{-k_1} \in H_2$$

となるので，H_2 は $(\mathbb{Z}/7\mathbb{Z})^\times$ の部分群である． □

問題 3 補足解説. 第 1,2 回講義資料命題 1.5 より，群 G の部分集合 H が G の部分群であることの必要十分条件は，

『H が空でなく，任意の $h, k \in H$ に対し，$h \cdot k \in H$ かつ $h^{-1} \in H$ となること』

であった．このため，部分群であることを確かめるときはこの条件を確認すればよい．

(1) の集合は二項演算では閉じていないが実は逆元を取る操作では閉じている．実際，

$$[1]_7^{-1} = [1]_7, \quad [2]_7^{-1} = [4]_7, \quad [4]_7^{-1} = [2]_7, \quad [6]_7^{-1} = [6]_7$$

である．(2) の集合が二項演算で閉じていることのチェックは (積の可換性より) 積を 6 パターン計算すれば良いだけなので容易であるが，解答例では少し抽象的な方法を書いた (これは私がこの問題をどう考えて作ったかということに関連している)．このように 1 つの元 (ここでは $[2]_7$) から二項演算および逆元を取る操作を何度も繰り返して得られる元を集めてできる群を**巡回群**と言う．これは今後の講義内でも登場する． □