# 代数学 I 第 3 回本レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

**問題 1**

$7^{30} \times 9^{15} \times 10^2$ を 8 で割った余りは，$\boxed{\text{ア}}$である．$\boxed{\text{ア}}$に入る数字を半角数字で入力せよ．

**問題 1 解答例.** $\mathbb{Z}/8\mathbb{Z}$ において，$[7^{30} \times 9^{15} \times 10^2]_8 = [r]_8$ を満たす $r$ $(0 \leq r < 8)$ が求める余りである．

$$\begin{aligned}[7^{30} \times 9^{15} \times 10^2]_8 &= [7]_8^{30} \times [9]_8^{15} \times [10]_8^2 \\ &= [-1]_8^{30} \times [1]_8^{15} \times [2]_8^2 \\ &= [(-1)^{30} \times 1^{15} \times 2^2]_8 \\ &= [4]_8\end{aligned}$$

より，求める余りは 4 である． □

**問題 1 補足解説.** この種の計算は mod を使う合同式の計算として既に行ったことがある方も多いと思うが，ここでは今回勉強した $\mathbb{Z}/8\mathbb{Z}$ における演算を用いる形で解答を書いてみた．見た目が違うだけでやっていることは mod と同じである．このような計算ができることは，$\mathbb{Z}/8\mathbb{Z}$ において積 $[a]_8 \times [b]_8 = [ab]_8$ が well-defined であるということが保証していたということに注意しよう．ちなみに，

$$7^{30} \times 9^{15} \times 10^2 = 464065028911716410052005133356603665460100$$

である． □

**問題 2**

$459x + 629y = 34$ を満たす整数の組 $(x, y)$ を全て求めよ．

**問題 2 解答例.** まず，$\gcd(459, 629)$ をユークリッド互除法で求める：

$$\begin{aligned}629 &= 1 \times 459 + 170 & 459 &= 2 \times 170 + 119 & 170 &= 1 \times 119 + 51 \\ 119 &= 2 \times 51 + 17 & 51 &= 3 \times 17 + 0\end{aligned}$$

であるので，$\gcd(459, 629) = 17$. よって，$459x'_0 + 629y'_0 = 17$ を満たす整数の組 $(x'_0, y'_0)$ が存在し，その 1 つは以下のように求められる．

$$\begin{aligned}17 &= 119 - 2 \times 51 \\ &= 119 + (-2) \times (170 - 1 \times 119) \\ &= 3 \times 119 + (-2) \times 170 \\ &= 3 \times (459 - 2 \times 170) + (-2) \times 170 \\ &= 3 \times 459 + (-8) \times 170 \\ &= 3 \times 459 + (-8) \times (629 - 1 \times 459) \\ &= 11 \times 459 + (-8) \times 629.\end{aligned}$$

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

つまり，$(x_0', y_0') = (11, -8)$ が $459x_0' + 629y_0' = 17$ を満たす整数の組の 1 つである．これより，両辺を $2(= 34/17)$ 倍して，$(x_0, y_0) = (22, -16)$ が $459x_0 + 629y_0 = 34$ を満たす整数の組の 1 つである．これより，

$$\begin{aligned} 459x + 629y = 34 &\Leftrightarrow 459(x-22) + 629(y-(-16)) = 0 \\ &\Leftrightarrow 27(x-22) + 37(y+16) = 0 \text{ (両辺を } \gcd(459, 629) = 17 \text{ で割った)} \\ &\Leftrightarrow \text{ある } m \in \mathbb{Z} \text{ を用いて，} (x-22, y+16) = (37m, -27m) \end{aligned}$$

となるので，求める整数の組は，$(x, y) = (22 + 37m, -16 - 27m), m \in \mathbb{Z}$. □

**問題 2 補足解説.** 第 3 回講義資料の P.7 にある方法をそのまま行えばよい．この種の問題では求めた答えが，確かに条件を満たすか ($459x + 629y = 34$ を満たすか) 確認して検算すること．

なお，以下は誤答となるので注意すること．

**誤答例：**(「つまり，$(x_0', y_0') = (11, -8)$ が $459x_0' + 629y_0' = 17$ を満たす整数の組の 1 つである．」までは同じ．) これより，

$$\begin{aligned} 459x + 629y = 17 &\Leftrightarrow 459(x-11) + 629(y-(-8)) = 0 \\ &\Leftrightarrow 27(x-11) + 37(y+8) = 0 \text{ (両辺を } \gcd(459, 629) = 17 \text{ で割った)} \\ &\Leftrightarrow \text{ある } m \in \mathbb{Z} \text{ を用いて，} (x-11, y+8) = (37m, -27m) \end{aligned}$$

となるので，$459x + 629y = 17$ を満たす整数の組は，$(x, y) = (11 + 37m, -8 - 27m), m \in \mathbb{Z}$.

ここから，両辺の $2(= 34/17)$ 倍を考えて，$459x + 629y = 34$ を満たす整数の組は，$(x, y) = (22 + 74m, -16 - 54m), m \in \mathbb{Z}$. □

これは，先に $459x + 629y = 17$ を満たす整数の組を全て求めてから最後にその 2 倍を答えとしている．こうして得られる整数の組 $(x, y)$ は確かに $459x + 629y = 34$ を満たすものとなるが，後から 2 倍すると上を見ればわかるように全ての整数解は求まらない．必ず，

与えられた方程式 ($459x + 629y = 34$) の特殊解を先に求めて，その後一般解を求めないといけない

のである． □

**問題 3**

$(\mathbb{Z}/12\mathbb{Z}, +)$ における部分群 $\{[8m]_{12} \mid m \in \mathbb{Z}\}$ の位数は ア である． 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 3 解答例.** $[k]_{12} \in \{[8m]_{12} \mid m \in \mathbb{Z}\}$ を満たす $1 \leq k \leq 12$ で最小のものを $k_0$ とすると，

$$\{[8m]_{12} \mid m \in \mathbb{Z}\} = \{[k_0 m]_{12} \mid m \in \mathbb{Z}\} =: H_{k_0}$$

であり，このとき $k_0$ は 12 の約数となって，$H_{k_0}$ の位数は $12/k_0$ である (第 3 回講義資料定理 2.2 およびその証明参照)．よって，このような $k_0$ を求める．

$$\begin{aligned} [k]_{12} \in \{[8m]_{12} \mid m \in \mathbb{Z}\} \quad &\Leftrightarrow \quad \text{ある } m_1, m_2 \in \mathbb{Z} \text{ が存在して，} 8m_1 + 12m_2 = k \\ &\Leftrightarrow \quad k \text{ は } \gcd(8, 12) = 4 \text{ の倍数} \end{aligned}$$

となる (最後の同値性は第 3 回講義資料定理 2.4 より)．よって，$k_0 = 4$ となり，求める位数は $12/4 = 3$ である． □

**問題 3 補足解説.** 解答例では一般性のある解き方をしたが，これくらいであれば以下のように具体的に解いても良い．

**別解：**

$$\{[8m]_{12} \mid m \in \mathbb{Z}\} = \{[-8m]_{12} \mid m \in \mathbb{Z}\} = \{[-8m+12m]_{12} \mid m \in \mathbb{Z}\} = \{[4m]_{12} \mid m \in \mathbb{Z}\} = \{[0]_{12}, [4]_{12}, [8]_{12}\}$$

よって，求める位数は 3. □

解答例を見るとこの問題は次のように一般化されることがわかる．

**定理**

$n, a$ を正の整数とする．このとき，$(\mathbb{Z}/n\mathbb{Z}, +)$ における部分群 $\{[am]_n \mid m \in \mathbb{Z}\}$ の位数は $n/\gcd(a,n)$ である．さらに，

$$\{[am]_n \mid m \in \mathbb{Z}\} = \{[\gcd(a,n)m]_n \mid m \in \mathbb{Z}\}$$

である．

証明は問題 3 解答例を順に一般的な言葉に直していけば良い．

**証明.** $[k]_n \in \{[am]_n \mid m \in \mathbb{Z}\}$ を満たす $1 \leq k \leq n$ で最小のものを $k_0$ とすると，

$$\{[am]_n \mid m \in \mathbb{Z}\} = \{[k_0 m]_n \mid m \in \mathbb{Z}\} =: H_{k_0}$$

であり，このとき $k_0$ は $n$ の約数となって，$H_{k_0}$ の位数は $n/k_0$ である (第 3 回講義資料定理 2.2 およびその証明参照)．よって，このような $k_0$ を求める．

$$\begin{aligned} [k]_n \in \{[am]_n \mid m \in \mathbb{Z}\} \quad &\Leftrightarrow \quad \text{ある } m_1, m_2 \in \mathbb{Z} \text{ が存在して，} am_1 + nm_2 = k \\ &\Leftrightarrow \quad k \text{ は } \gcd(a,n) \text{ の倍数} \end{aligned}$$

となる (最後の同値性は第 3 回講義資料定理 2.4 より)．よって，$k_0 = \gcd(a,n)$ となり，$H_{k_0}$ の位数は $n/\gcd(a,n) = n$ である． □

以下の問題 4 はこの定理を適用して解いてみよう． □

**問題 4**

$(\mathbb{Z}/3906\mathbb{Z}, +)$ における部分群 $\{[3410m]_{3906} \mid m \in \mathbb{Z}\}$ の位数は$\boxed{\text{ア}}$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 4 解答例.** 問題 3 補足解説の定理より，求める位数は

$$3906/\gcd(3410, 3906)$$

である．$\gcd(3410, 3906)$ をユークリッド互除法で求める．

$$\begin{aligned} 3906 &= 1 \times 3410 + 496 & \qquad 3410 &= 6 \times 496 + 434 \\ 496 &= 1 \times 434 + 62 & \qquad 434 &= 7 \times 62 + 0 \end{aligned}$$

より，$\gcd(3410, 3906) = 62$．これより，求める位数は，

$$3906/62 = 63.$$

□