# 数学展望 I レポート問題 [2] (6 月 16 日)

**問 1.** 次の条件をすべてみたす正の整数 $N$ のうち, 最小のものを求めよ:

(a) $N$ は 17 で割ると余りが 2 である.
(b) $N$ は 61 で割ると余りが 58 である.
(c) $N$ は 103 で割ると余りが 1 である.

**(解答例).** まず, $n_1 \equiv 1 \pmod{17}$, $n_1 \equiv 0 \pmod{6,283 = 61 \cdot 103}$ を満たす整数 $n_1$ を**ユークリッドの互除法**により求める.

$$\begin{aligned} \underline{6,283} &= \underline{17} \cdot 369 + \underline{10} \\ \underline{17} &= 1 \cdot \underline{10} + \underline{7} \\ \underline{10} &= 1 \cdot \underline{7} + \underline{3} \\ \underline{7} &= 2 \cdot \underline{3} + 1 \end{aligned}$$

ゆえに,

$$\begin{aligned} 1 &= \underline{7} - 2 \cdot \underline{3} & &= \underline{7} - 2 \cdot (\underline{10} - 1 \cdot \underline{7}) \\ &= (-2) \cdot \underline{10} + 3 \cdot \underline{7} & &= (-2) \cdot \underline{10} + 3 \cdot (\underline{17} - 1 \cdot \underline{10}) \\ &= 3 \cdot \underline{17} + (-5) \cdot \underline{10} & &= 3 \cdot \underline{17} + (-5) \cdot (\underline{6,283} - 369 \cdot \underline{17}) \\ &= (-5) \cdot \underline{6,283} + 1,848 \cdot \underline{17} \end{aligned}$$

そこで,

$$n_1 = (-5) \cdot \underline{6,283} = -31,415$$

とおけば, $n_1$ は求める条件を満たす.

次に, $n_2 \equiv 1 \pmod{61}$, $n_2 \equiv 0 \pmod{1751 = 17 \cdot 103}$ をみたす整数 $n_2$ を求める.

$$\begin{aligned} \underline{1,751} &= 28 \cdot \underline{61} + \underline{43} \\ \underline{61} &= 1 \cdot \underline{43} + \underline{18} \\ \underline{43} &= 2 \cdot \underline{18} + \underline{7} \\ \underline{7} &= 1 \cdot \underline{4} + 3 \\ \underline{4} &= 1 \cdot \underline{3} + 1 \end{aligned}$$

上と同様にして,

$$1 = \underline{4} - 1 \cdot \underline{3} = \underline{4} - 1 \cdot (\underline{7} - 1 \cdot \underline{4}) = \cdots = (-17) \cdot \underline{1,751} + 488 \cdot \underline{61}$$

を得る. そこで,

$$n_2 = (-17) \cdot \underline{1,751} = -29,767$$

とおけばよい.

引き続き, $n_3 \equiv \pmod{103}$, $n_3 \equiv \pmod{1,037 = 17 \cdot 61}$ を求める.

$$\begin{aligned} \underline{1,037} &= 10 \cdot \underline{103} + \underline{7} \\ \underline{103} &= 14 \cdot \underline{7} + \underline{5} \\ \underline{7} &= 1 \cdot \underline{5} + \underline{2} \\ \underline{5} &= 2 \cdot \underline{2} + \underline{1} \end{aligned}$$

から,

$$1 = \underline{5} - 2 \cdot (\underline{7} - 1 \cdot \underline{5}) = \cdots = (-44) \cdot \underline{1,037} + 443 \cdot \underline{103}$$

を得る. そこで, $n_3 = (-44) \cdot \underline{1,037} = -45,628$ とおけばよい.

**中国式剰余定理**により, 条件 (a),(b),(c) すべてをみたすような整数 $N$ は, $K$ を整数として,

$$\begin{aligned} N &= 2n_1 + 58n_2 + n_3 + 17 \cdot 61 \cdot 103 \cdot K \\ &= 2 \cdot (-31,415) + 58 \cdot (-29,767) + (-45628) + 106,811 \cdot K \\ &= -1,834,944 + 106,811 \cdot K \end{aligned}$$

の形にかける. $1,834,944/106,811 = 17.1\ldots$ に注意して,

$$N = 87,654 + 106,811 \cdot (K - 18)$$

と書き直せば, 条件を満たす正の整数のうち最小のもの は,

$$\underline{87,654}$$

であることが分かる. □

**注意 1.** $58 \equiv -3 \pmod{61}$ だから, $N = 2n_1 - 3n_2 + 17 \cdot 61 \cdot 103 \cdot K$ を考えても同じ結論を得る. こちらの方が計算は多少楽になる.

レポートの採点にあたっては, 次のポイントを見る:

(1) ユークリッドの互除法が正しく利用されているか.

(2) 中国式剰余定理が正しく利用されているか.

(3) 条件をみたすもののうち, 最小のものが求められているか.

(4) 計算間違いがないか.

**問 2.** 平面 $\mathbb{R}^2$ 内の単位円を $n$ 等分して正 $n$ 角形 $P_0P_1\cdots P_{n-1}$ を作る：

$$P_k\left(\cos\frac{2k\pi}{n},\sin\frac{2k\pi}{n}\right)\quad(k=0,1,\ldots,n-1)$$

この正 $n$ 角形の $P_0$ を $P_1$ まで回転させて得られる合同変換を $A$ とし, $A$ の逆回転を $A^{-1}$, $A$ を $k$ 回続けて行なう変換を $A^k$ のように書くとき, **折り返しを含まない合同変換**は,

$$E=A^0, A=A^1,\ldots,A^{n-1}$$

の $n$ 個である. ただし, $E$ は**恒等変換** ($P_0$ を $P_0$ にうつす変換) を表す.

$A^k$ を何回か行なうと, $P_0$ を $P_0$ にうつす恒等変換になる. そのような回数の最小値, すなわち,

$$o(A^k)=\min\{\ell\in\mathbb{Z}\mid \ell \text{ は正の整数}, (A^k)^\ell=E\}$$

を $A^k$ の**位数**と言う. このとき, 次の各問に答えよ.

(1) 正 12 角形に対して, $P_0$ の行き先を追うことにより, 「折り返しを含まない合同変換」 $E, A, A^2,\ldots,A^{11}$ の位数をそれぞれ求めよ.

(2) 一般に, $A^k$ の位数は $\dfrac{n}{(n,k)}$ で与えられることを示せ.

各 $n$ に対して, $\varphi(n)=\#\{k\in\mathbb{Z}\,|\,1\le k\le n, o(A^k)=n\}$ とおく.

(3) $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(12)=4$ を示せ.

(4) $\dfrac{\varphi(n)}{n}=\dfrac{1}{2}$ となるような整数 $n$ を全て決定せよ.

**(解答例).** (1)

$o(E)=1$, $P_0\to P_0$
$o(A)=12$, $P_0\to P_1\to P_2\to P_3\to P_4\to P_5\to P_6\to P_7\to P_8\to P_9\to P_{10}\to P_{11}\to P_0$
$o(A^2)=6$, $P_0\to P_2\to P_4\to P_6\to P_8\to P_{10}\to P_0$
$o(A^3)=4$, $P_0\to P_3\to P_6\to P_9\to P_0$
$o(A^4)=3$, $P_0\to P_4\to P_8\to P_0$
$o(A^7)=12$, $P_0\to P_5\to P_{10}\to P_3\to P_8\to P_1\to P_6\to P_{11}\to P_4\to P_9\to P_2\to P_7\to P_0$
$o(A^8)=3$, $P_0\to P_8\to P_4\to P_0$
$o(A^9)=4$, $P_0\to P_9\to P_6\to P_3\to P_0$
$o(A^{10})=6$, $P_0\to P_{10}\to P_8\to P_6\to P_4\to P_2\to P_0$
$o(A^{11})=12$, $P_0\to P_{11}\to P_{10}\to P_9\to P_8\to P_7\to P_6\to P_5\to P_4\to P_3\to P_2\to P_1\to P_0$

(2) $n$ と $k$ の最大公約数を $d=(n,k)$ とおくと, $n=n'd$, $k=k'd$ (ここで, $n'$ と $k'$ は互いに素な整数) と書くことができる. このとき, $\frac{n}{(n,k)}=n'$ である.

さて, $n'$ が $A^k$ の位数であることを言うには,

$$(A^k)^{n'}=E, \qquad (A^k)^m=E \Longrightarrow n' \,|\, m$$

が言えればよい. (注) $n' \,|\, m$ は $\ell$ が $m$ を割り切ることを意味する. 特に, このとき, $n' \leq m$ となる.

まず, $A^n=E$ に注意すると,

$$(A^k)^{n'}=A^{kn'}=A^{(k'd)n'}=A^{nk'}=(A^n)^{k'}=E^{k'}=E$$

を得る. 一方, $(A^k)^m=E$ と仮定する. $km$ を $n$ で割った余りを $r$ とすれば,

$$km=qn+r, \quad 0 \leq r < n$$

と表すことができる. このとき, もし $0<r<n$ ならば,

$$A^r=A^{km-qn}=(A^k)^m(A^n)^{-q}=EE^{-q}=E$$

であるが, これは $A$ の位数が $n$ であることに矛盾する. よって, $r=0$ である. 特に,

$$km=qn \qquad \therefore k'dm=qdn' \qquad \therefore k'm=qn'$$

$k'$ と $n'$ は互いに素だから, $n' \,|\, m$ を得る. ゆえに, $o(A^k)=n'=\frac{n}{(n,k)}$ を証明した.

(3)

- $n=3$ のとき, $o(A)=o(A^2)=3$, $o(E)=1$ ゆえ, $\varphi(3)=2$ である.
- $n=4$ のとき, $o(E)=1$, $o(A)=4$, $o(A^2)=2$, $o(A^3)=4$ ゆえ, $\varphi(4)=2$ である.
- $n=12$ のとき, (1) より, $o(A^k)=12$ となるのは, $k=1,5,7,11$ の 4 つだから, $\varphi(12)=4$ である.

(注) この問題の $n=3$ (resp. $n=4$) の場合の $\varphi(n)$ の値を, (1) における位数が 3 (resp. 4) の $A^k$ の個数と勘違いしている人が結構見られたが, それは勘違いである.

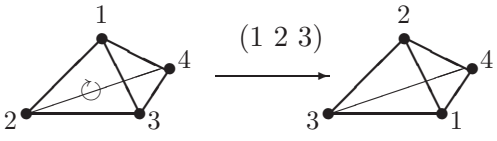
(4) (2) より,

$$\varphi(n)=\#\{k \in \mathbb{Z} \,|\, 1 \leq k \leq n,\ (k,n)=1\}$$

である. $\varphi(2^e)=2^e-2^{e-1}=2^{e-1}$ だから, $n=2^e$ は $\varphi(n)/n=1/2$ を満たす. 逆に, $\varphi(n)=n/2$ と仮定すると, $n/2$ が整数だから, $n$ は偶数である. このとき, $1 \leq k \leq n$ なる整数 $k$ のうち, $k$ が偶数ならば $k$ と $n$ は公約数 2 を持つので, 互いに素でない. ゆえに, $\varphi(n)=n/2$ が成り立つならば, $1 \leq k \leq n$ なるすべての奇数は $n$ と互いに素でなければならない. 特に, $n$ はどんな奇素数も約数にもたない. ゆえに, $n=2^e$ $(e \geq 1)$ の形をしていなければならない.

(注) オイラー関数 $\varphi$ の積の性質：$(m,n)=1 \Longrightarrow \varphi(mn)=\varphi(m)\varphi(n)$ を用いても示すことができる. □

**問 3.** 正４面体の合同変換について考える．正４面体の頂点を $P_1$, $P_2$, $P_3$, $P_4$ とするとき，




は，$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ のように４次の置換として表すことができる．

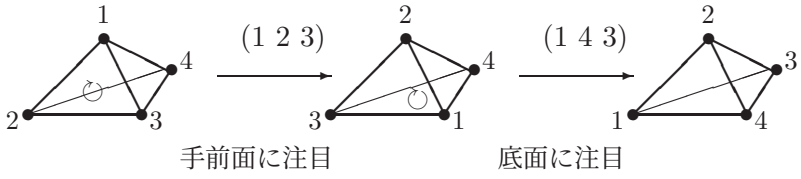
(1) $(12)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ は $(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ のように３つの頂点のみを動かす型の置換の２個の積で表すことができる．具体的に表せ．

(2) 正４面体の合同変換の全体は上に述べた対応により **４次交代群** $A_4$ をなす．４次交代群の元を３つの型に分けてすべて書き出せ．また，それぞれの型の代表元はどのような回転軸を持つかを説明せよ．

(3) ４次交代群の各元は**互換**（２個の文字のみを動かす変換）の偶数個の積で表すことができることを示し，互換（(12) としてよい）に対応する合同変換は存在しないことを導け．

(4) $\mathbb{R}^3$ 内の回転では「{**向き**」（３つの１次独立なベクトルから作られる行列式の符号）が変化しないことに注意して，前問の結論を幾何学的に説明せよ．

**(解答例).** (1) 下の図からもわかるように，$(12)(34) = (143)(123)$ である．




(2) ４次交代群 $A_4$ の元は，

$$\begin{aligned} (1)\text{ 型} &\quad \cdots \quad (1) \\ (12)(34)\text{ 型} &\quad \cdots \quad (12)(34), (13)(24), (14)(23) \\ (123)\text{ 型} &\quad \cdots \quad (123), (132), (124), (142), (134), (143), (234), (243) \end{aligned}$$

の３種類である．(1) は変化しない．(12)(34) は，頂点 1,2 を結ぶ辺の中点 $M$ と，頂点 3,4 を結ぶ辺の中点 $N$ を結ぶ直線を回転軸に持つ回転．(123) は，三角形 123 の中心と頂点 4 を結ぶ直線を回転軸に持つ回転

(3) $(12)(34)$ も $(123) = (13)(12)$ も 2 個の互換の積で表すことができるので, (2) の分類にも注意すると, 4 次交代群の任意の元は偶数個の互換の積の形に表すことができることがわかる. 一方, 互換は偶数個の互換の積の形に表すことができない.

(注) 例えば, 差積を用いて証明することができる.

(4) 省略. □

**問 4.** 正６面体の合同変換は, 正６面体の４つの対角線 $P_1Q_1$, $P_2Q_2$, $P_3Q_3$, $P_4Q_4$ に関する置換を引き起こす. また, 異なる合同変換は異なる置換を引き起こす.

これより, 正６面体群は自然に４次対称群の部分群とみなすことができる. 正６面体の６つの面を $F_1, \ldots, F_6$ とする.

(1) 次の事実に注意して, 正６面体群の位数は 24, 特に, 正６面体群＝４次対称群 $S_4$ となることを示せ.

  ($a$) 各 $i = 1, \ldots, 6$ に対して, $F_1$ を $F_i$ にうつす合同変換が存在する.

  ($b$) $F_1$ を $F_i$ にうつす合同変換 $\sigma$, $\sigma'$ の違いは $F_i$ をその中心の周りに回転させるだけの違いである.

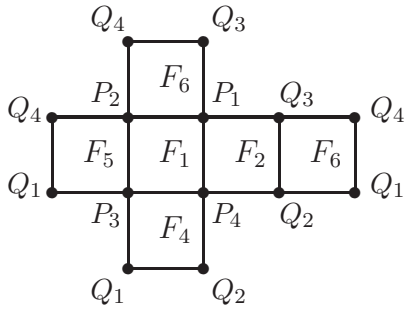
(2) 面 $F_1$ を四角形 $P_1P_2P_3P_4$, 面 $F_2$ を四角形 $P_1P_4Q_2Q_3$ とするとき, $F_1$ を $F_2$ にうつす合同変換[a]を表す置換を具体的に書け. また, (34) に対応する合同変換はどのようにして得られるかを説明せよ.

(3) 互換 (12) を置換 $\sigma = (123)$ と $\tau = (1234)$ のいくつかの積の形に表せ.

(4) ２つの置換 $\sigma = (123)$ と $\tau = (1234)$ を含む $S_4$ の部分群は自分自身に他ならないことを証明せよ. また, この事実を合同変換の視点から説明せよ.

[a](お断り) 正確には, 「$F_1$ を 90° 回転させて $F_2$ にうつす合同変換」とすべきでした。

**(解答例).** 正６面体の各面をさいころのように番号付けする (下図参照)。




「$F_1$ を $F_2$ にうつす」という意味は, 「$F_1$ の面があった場所に $F_2$ が来るように回転させる」の意味とする[1]。

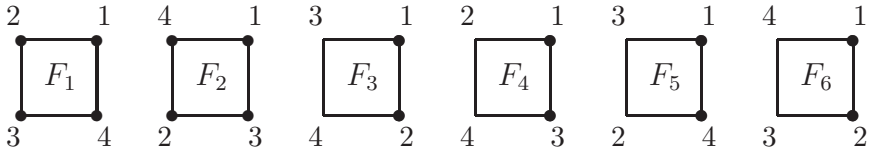
(1) 正６面体群の元の総数は,

$$(F_1 \text{ を } F_i \text{ にうつす合同変換の総数}) \times (\text{面の総数}) = 4 \times 6 = 24 \text{ (個)}$$

[1](注意) $F_1$ を $F_2$ の面があった場所に移動させる, としても (答) は異なるが, 解答としては成立する。

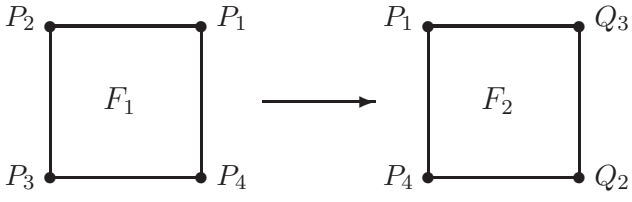
である。

さて, 正６面体群の各元 $\sigma$ に対して, ４本の対角線の置換を考えることにより, ４次対称群 $S_4$ の元が対応する。その元を $\varphi(\sigma)$ と書く。例えば, (2) で見るように, $F_1$ を $90^\circ$ 回転させて $F_2$ に写すような合同変換 $\sigma$ に対して, $\varphi(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ が対応している。この対応が１：１であることを見よう[2]。既に見たように正６面体群は４次対称群 $S_4$ と同じ $4! = 24$ 個の元を含むので, 対応 $\varphi$ が１：１, すなわち, $\sigma \neq \sigma'$ ならば $\varphi(\sigma) \neq \varphi(\sigma')$ であることを見ればよい。$\sigma' \circ \sigma^{-1}\colon F_1 \mapsto F_1$ だから, $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ に対応する合同変換が恒等変換に限ることを見ればよい。




のように $F_1$ 以外の面は, 頂点の並び順が異なるので, $F_1 \to F_i$ $(i \neq 1)$ にうつすような合同変換は $e$ には対応しない。よって, $F_1 \mapsto F_1$ なる合同変換のみを考えればよいが, そのようなものは $F_1$ と $F_6$ を固定して, それらの中心を結ぶ直線の周りの $0^\circ$, $90^\circ$, $180^\circ$, $270^\circ$ の回転のみである。これらのうち, 対角線 $P_1Q_1$ を固定するものは明らかに恒等変換しかない。

(2) $\sigma\colon F_1 \mapsto F_2$ を図示すると,

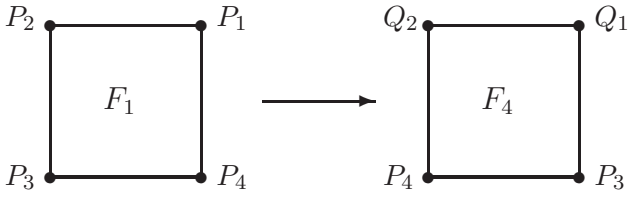



となる。このとき, 対角線に注目すると,

$$\begin{aligned} P_1Q_1 &\longrightarrow Q_3P_3 \\ P_2Q_2 &\longrightarrow P_1Q_1 \\ P_3Q_3 &\longrightarrow P_4Q_4 \\ P_4Q_4 &\longrightarrow Q_2P_2 \end{aligned}$$

だから, $\sigma$ には, $\varphi(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ が対応している。

(34) に対応する合同変換は, 次のものである：




[2]厳密には合成の仕方が対応していることも見る必要があるが, それは省略する。

(3) $(1234) = (14)(13)(12)$, $(123) = (13)(12)$ に注意して,

$$(ik)(ij)(ik) = (kj), \qquad (ij)(ij)(ij) = (ij), \qquad (k\ell)(ij)(k\ell) = (ij),$$

を用いる[3]。

$$\rho := \tau^{-2}\sigma^2\tau^2 = (24)(13)(12)(13)(13)(24) = (24)(13)(12)(24) = (13)(14) = (143).$$

とおくと,

$$\rho\tau = (143)(1234) = (13)(14)(14)(13)(12) = (12).$$

ゆえに, $(12) = \tau^2\sigma^2\tau^3$ が得られる[4]。

(4) (3) の計算に注意すると, 4 次対称群 $S_4$ の勝手な元は互換の積で書けることが分かる。また, 勝手な互換は $(23) = (13)(12)(13)$ のように $(12)$, $(13)$, $(14)$ のいくつかの積で書ける。

$\sigma = (123)$ と $\tau = (1234)$ を含む部分群を $H$ とするとき, $S_4$ の元がすべて $H$ の元であることを見るには, $(12)$, $(13)$, $(14)$ が $H$ の元であることを見ればよい。

(3) の結果より, $H$ は $(12)$ を含む. また,

$$(13) = (13)(12)(12) = \sigma(12), \quad (14) = (14)(13)(12)(12)(13) = \tau\sigma^{-1} = \tau\sigma^2$$

だから, $H$ は $(13)$ および $(14)$ も含むことが分かる. ゆえに, $H = S_4$ である。

$(123)$ は対角線 $P_4Q_4$ を固定軸に持つような回転である。また, $(1234)$ は $F_1$ と $F_6$ のそれぞれの中心を結ぶ直線を軸にもつような回転である。結局, 「正 6 面体の合同変換はこのような回転をいくつか合成して得られる」ことが分かった。 □

[3]直接計算してもよい。

[4](注) 表し方は一通りではない。ここでは試行錯誤の末に見つけるしかない。