自然数 m と互いに素な m 以下の自然数の個数を $\phi(m)$ と表す．

(1) p を素数，n を自然数とするとき，$\phi(p^n) = p^n - p^{n-1}$ を示せ．

以下の設問では，$m_1,\ m_2,\ \cdots,\ m_6,\ h$ を，次の (i)，(ii) を満たす自然数とする．

(i) $m_1 < m_2 < \cdots < m_6 < h$
(ii) h と互いに素な h 未満の自然数は集合 $\{m_1,\ m_2,\ \cdots,\ m_6\}$ に属する．

このとき，次の問いに答えよ．ただし，m と n が互いに素な自然数であるとき，$\phi(mn) = \phi(m)\phi(n)$ が成立することは使ってよい．

(2) h は 11 以上の素数で割り切れないことを示せ．
(3) $m_2 = 4$ のとき h を求めよ．

(19 大阪市大 後 理 (数) 6)

【答】
(1) 略
(2) 略
(3) $h = 12$

【解答】

(1) p^n 以下の自然数は p^n 個ある．このうち p と互いに素でないものは，p が素数であることから p の倍数に限られ，$p\cdot 1,\ p\cdot 2,\ \cdots,\ p\cdot p^{n-1}$ の p^{n-1} 個ある．したがって

$$\phi(p^n) = p^n - p^{n-1}$$

である． …… (証明終わり)

(2) 背理法を用いる．h が 11 以上の素数 p で割り切れると仮定すると

$$h = p^a h' \ (a \text{ は自然数},\ h' \text{ は } p \text{ と互いに素な整数})$$

と表すことができる．p^a と h' は互いに素だから

$$\begin{aligned}\phi(h) &= \phi(p^a)\phi(h') = (p^a - p^{a-1})\phi(h') \ (\because\ (1))\\ &= p^{a-1}(p-1)\phi(h')\\ &\geqq 11^0\cdot(11-1)\cdot 1\\ &= 10\end{aligned}$$

これは 条件 (ii) の $\phi(h) \leqq 6$ であることに反する．
よって，h は 11 以上の素数で割り切れない． …… (証明終わり)

(3) 1 と h は互いに素だから，1 は $\{m_1,\cdots,\ m_6\}$ に含まれ，$m_1 < m_2 = 4$ より $m_1 = 1$ である．したがって，2, $3 \notin \{m_1,\cdots,\ m_6\}$ であり，条件 (i)，(ii) より，h と 2, 3 は互いに素ではない．すなわち

$$h = 2^a\cdot 3^b\cdot h'' \ (a,\ b \text{ はともに自然数},\ h'' \text{ は } 2,\ 3 \text{ と互いに素な整数})$$

と表すことができる．このとき

$$\begin{aligned}\phi(h) &= (2^a - 2^{a-1})(3^b - 3^{b-1})\phi(h'')\\ &= (2-1)2^{a-1}\cdot(3-1)3^{b-1}\phi(h'')\\ &= 2^a 3^{b-1}\phi(h'')\end{aligned}$$

条件 (ii) より $\phi(h) \leqq 6$ であり

$$2^a 3^{b-1}\phi(h'') \leqq 6 \qquad \therefore \quad \phi(h'') \leqq 3$$

ここで，$h'' \neq 1$ とすると，h'' と 2, 3 が互いに素であることから h'' は 5 以上の素因数 q をもつ．このとき

$$h'' = q^c h''' \ (c \text{ は自然数, } h''' \text{ は } q \text{ と互いに素な整数})$$

と表すことができて，q^c と h''' は互いに素であるから

$$\begin{aligned}\phi(h'') &= \phi(q^c)\phi(h''') = (q^c - q^{c-1})\phi(h''') \\ &= q^{c-1}(q-1)\phi(h''') \\ &\geqq 5^0 \cdot (5-1) \cdot 1 = 4\end{aligned}$$

$\phi(h'') \leqq 3$ に反するから $h'' = 1$ である．よって

$$\phi(h) = 2^a \cdot 3^{b-1}$$

である．h は素因数 2 をもつから h と $4 = m_2$ は互いに素ではなく，m_2 を互いに素な集合から除くと $\phi(h) \leqq 5$ である．これと $2^a \geqq 2$ より $b = 1$ である．このとき

$$h = 2^a \cdot 3, \quad \phi(h) = 2^a$$

である．

$4 = m_2 < m_3 < \cdots < m_6 < h$ より $h \geqq 9$ でもあるから

$$\begin{cases} 2^a \cdot 3 \geqq 9 \\ 2^a \leqq 5 \end{cases} \qquad \therefore \quad 3 \leqq 2^a \leqq 5 \qquad \therefore \quad a = 2$$

以上より，条件 (i)，(ii) をみたす h が存在するならば

$$h = 2^2 \cdot 3 = \mathbf{12} \qquad \cdots\cdots(\text{答})$$

である．

- $h = 12$ のとき，例えば

  $$m_1 = 1,\ m_2 = 4,\ m_3 = 5,\ m_4 = 7,\ m_5 = 9,\ m_6 = 11$$

  とすれば条件を満たす．