p を 2 より大きい素数，n を正の整数とする．$1 \leqq k \leqq p^n$ を満たす整数 k で，p と互いに素であるもの全体の集合を A とする．次の問いに答えよ．

(1) $p=3,\ n=2$ のとき，集合 A を求めよ．

(2) A に属する整数の個数，および A に属するすべての整数の和を求めよ．

(3) A に属する整数 k に対して，$kl-1$ が p^n の倍数となるような A に属する整数 l が存在し，それはただ一つであることを示せ．ただし，整数 a と b が互いに素であるとき，1 次不定方程式 $ax+by=1$ は，整数解をもつことが知られている．必要ならばこの事実を利用してよい．

(4) A に属するすべての整数 k についての $\dfrac{1}{k}$ の和を既約分数で表したとき，分子は p^n の倍数となることを示せ．

(19 金沢大 理工・医薬保健 4)

【答】

(1) $A=\{1,\ 2,\ 4,\ 5,\ 7,\ 8\}$

(2) 個数は $(p-1)p^{n-1}$，和は $\dfrac{1}{2}(p-1)p^{2n-1}$

(3) 略

(4) 略

【解答】

(1) $p=3,\ n=2$ のとき，A は $1 \leqq k \leqq 3^2$ を満たす整数 k で，3 と互いに素であるもの全体の集合であるから

$$\boldsymbol{A=\{1,\ 2,\ 4,\ 5,\ 7,\ 8\}} \qquad \cdots\cdots(\text{答})$$

(2) $1 \leqq k \leqq p^n$ を満たす p^n 個の整数 k のうち，p と互いに素でない整数は

$$p,\ 2p,\ 3p,\ \cdots,\ p^{n-1}p$$

の p^{n-1} 個がある．したがって A に属する整数の個数は

$$p^n-p^{n-1}=\boldsymbol{(p-1)p^{n-1}} \quad (\text{個}) \qquad \cdots\cdots(\text{答})$$

また $1 \leqq k \leqq p^n$ を満たす p^n 個の整数 k の和は

$$\sum_{k=1}^{p^n} k=\frac{1}{2}p^n(p^n+1)$$

p^n 個の整数のうち p と互いに素でない整数 p^{n-1} 個の和は

$$\sum_{j=1}^{p^{n-1}} jp=p\cdot\frac{1}{2}p^{n-1}(1+p^{n-1})=\frac{1}{2}p^n(p^{n-1}+1)$$

よって，A に属するすべての整数の和は

$$\begin{aligned}&\frac{1}{2}p^n(p^n+1)-\frac{1}{2}p^n(p^{n-1}+1)\\=&\frac{1}{2}p^n(p^n-p^{n-1})\\=&\boldsymbol{\frac{1}{2}(p-1)p^{2n-1}}\end{aligned} \qquad \cdots\cdots(\text{答})$$

(3) k は A に属する整数であるから，k と p は互いに素であり，k と p^n も互いに素である．したがって，1 次不定方程式

$$kx + p^n y = 1 \qquad \cdots\cdots ①$$

を満たす整数の組 $(x,\ y)$ が存在する．この整数の組の 1 つをを $(x_0,\ y_0)$ とすると

$$kx_0 + p^n y_0 = 1 \qquad \cdots\cdots ②$$

であり，①，②の辺々を引くと

$$k(x - x_0) + p^n(y - y_0) = 0$$
$$\therefore \quad k(x - x_0) = -p^n(y - y_0)$$

k と p^n は互いに素であるから，任意の整数 m を用いて

$$\begin{cases} x = x_0 + mp^n \\ y = y_0 - mk \end{cases} \qquad \cdots\cdots ③$$

と表すことができる．この x は ① の解であるから

$$kx - 1 = -p^n y$$

であり，$kx - 1$ は p^n の倍数である．

次に，この x を p の倍数とすると，① において，左辺は p の倍数，右辺は 1 である．p は素数なので，これは不合理である．したがって，x は p の倍数でなく，x は p^k の倍数でない．③ において，m を変化させると，x は p^n ずつ変化するから

$$0 < x < p^n$$

を満たす整数 x はただ一つ存在する．これを l とおくと，$kl - 1$ は p^k の倍数であり，l は $1 \leqq k \leqq p^n$ を満たす p と互いに素な整数，すなわち A に属する整数である．

…… (証明終わり)

(4) p は 2 より大きい素数であるから，A に属する整数の個数 $(p-1)p^{n-1}$ は偶数である．正の整数 N を $N = \dfrac{1}{2}(p-1)p^{n-1}$ とする．A に属する整数を小さい方から順に並べたとして，小さい方から i 番目の整数を a_i とすると大きい方から i 番目の整数は $p^n - a_i$ である．

A に属するすべての整数の逆数の和は

$$\sum_{i=1}^{N}\left(\frac{1}{a_i} + \frac{1}{p^n - a_i}\right) = p^n \sum_{i=1}^{N} \frac{1}{a_i(p^n - a_i)}$$

a_i，$p^n - a_i$ は p の倍数ではないので $\displaystyle\sum_{i=1}^{N} \frac{1}{a_i(p^n - a_i)}$ を既約分数で表したとき分母には p は含まれない．

よって，$\displaystyle p^n \sum_{i=1}^{N} \frac{1}{a_i(p^n - a_i)}$ が p で約分されることはなく，分子は p^n の倍数である．

…… (証明終わり)