[東京大学 2002 年前期 理科 $\boxed{6}$]

☆―――☆

N を正の整数とする。$2N$ 個からなる数列

$$\{a_1,\ a_2,\ \cdots,\ a_N,\ b_1,\ b_2,\ \cdots,\ b_N\}$$

を

$$\{b_1,\ a_1,\ b_2,\ a_2,\ \cdots,\ b_N,\ a_N\}$$

という数列に並べ替える操作を「シャッフル」と呼ぶことにする。並べ替えた数列は b_1 を初項とし，b_i の次に a_i， a_i の次に b_{i+1} が来るようなものになる。また，数列 $\{1,\ 2,\ \cdots,\ 2N\}$ をシャッフルしたときに得られる数列において，数 k が現れる位置を $f(k)$ で表す。

たとえば， $N=3$ のとき，$\{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$ をシャッフルすると $\{4,\ 1,\ 5,\ 2,\ 6,\ 3\}$ となるので，

$f(1)=2,\ f(2)=4,\ f(3)=6,\ f(4)=1,\ f(5)=3,\ f(6)=5$ である。

（1）数列 $\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\}$ を 3 回シャッフルしたときに得られる数列を求めよ。

（2）$1 \leqq k \leqq 2N$ を満たす任意の整数 k に対し， $f(k)-2k$ は $2N+1$ で割り切れることを示せ。

（3） n を正の整数とし， $N=2^{n-1}$ のときを考える。数列 $\{1,\ 2,\ 3,\ \cdots,\ 2N\}$ を $2n$ 回シャッフルすると， $\{1,\ 2,\ 3,\ \cdots,\ 2N\}$ にもどることを証明せよ。

☆―――☆

（1）1 回シャッフルすると $\{5,\ 1,\ 6,\ 2,\ 7,\ 3,\ 8,\ 4\}$

さらにもう 1 回シャッフルすると $\{7,\ 5,\ 3,\ 1,\ 8,\ 6,\ 4,\ 2\}$

さらにもう 1 回シャッフルすると $\{8,\ 7,\ 6,\ 5,\ 4,\ 3,\ 2,\ 1\}$ これが求める数列である。

（2）数列 $\{1,\ 2,\ 3,\ \cdots,N,\ N+1,\ N+2,\ \cdots,\ 2N\}$ …（＊）を 1 回シャッフルすると

$$\{N+1,\ 1,\ N+2,\ 2,\ N+3,\ 3,\ \cdots,2N,\ N\}$$

となる。

$1 \leqq k \leqq N$ に対し，（＊）の数列の前半部分 $\{1,\ 2,\ 3,\ \cdots,\ N\}$ の k 番目の数は，

シャッフルしたときに $2k$ 番目に移動するので， $f(k)=2k$ である。

よって， $f(k)-2k=0$ より $2N+1$ で割り切れる。

また，$N+1 \leqq k \leqq 2N$ に対し,（∗）の数列の後半部分 $\{N+1,\ N+2,\ \cdots,\ 2N\}$ の $k-N$ 番目の数は,

シャッフルしたときに $2(k-N)-1$ 番目に移動するので， $f(k)=2(k-N)-1$ である。

よって， $f(k)-2K=-2N-1$ より $2N+1$ で割り切れる。よって題意は示された。

(3)（2)より $f(k)$ と $2k$ は $2N+1$ で割ったときの余りが等しい。

したがって， $f(k)\equiv 2k$ （$\mathrm{mod}\ \ 2N+1$） である。

次に， $N=2^{n-1}$ のとき，数列 $\{1,\ 2,\ 3,\ \cdots,\ 2^n\}$ を 1 回シャッフルすると

$1 \leqq k \leqq 2^n$ を満たす任意の k に対して

$$f(k)\equiv 2k \quad (\mathrm{mod}\ \ 2^n+1)$$

さらにもう 1 回（2 回目の）シャッフルすると

$$f\left(f\left(k\right)\right)\equiv 2f\left(k\right)\equiv 2\left(2k\right)=2^2k \quad (\mathrm{mod}\ \ 2^n+1)$$

さらにもう 1 回（3 回目の）シャッフルすると

$$f\left(f\left(f\left(k\right)\right)\right)\equiv 2^2 f\left(k\right)\equiv 2^2\left(2k\right)\equiv 2^3k \quad (\mathrm{mod}\ \ 2^n+1)$$

となる。同様にして， $2n$ 回続けてシャッフルしたとき， $f^{2n}\left(k\right)$ と表すとすると

$$f^{2n}\left(k\right)\equiv 2^{2n}k \quad (\mathrm{mod}\ \ 2^n+1)$$

となる。ここで,

$$2^{2n}k-k=\left(2^{2n}-1\right)k=\left(2^n+1\right)\left(2^n-1\right)k$$

となるので,

$$2^{2n}k-k\equiv 0 \quad (\mathrm{mod}\ \ 2^n+1)$$

である。したがって,

$$f^{2n}\left(k\right)\equiv k \quad (\mathrm{mod}\ \ 2^n+1)$$

となり，$1 \leqq k \leqq 2^n$ から $f^{2n}\left(k\right)=k$ である。

よって，数列 $\{1,\ 2,\ 3,\ \cdots,\ 2N\}$ を $2n$ 回シャッフルすると，元に戻る。