N 進シャフリングの数学

学習院大学理学部数学科
渡辺彩香

平成 20 年 2 月 2 日

目 次

1　目的

この研究において、N 進シャフリングを数学的に研究する。特にカードの枚数 n とカードの並びが元に戻るまでの周期 m の関係について調べる。

まず n 枚のカードを N 人に配る。このとき余りが N 未満であっても最後まで配りきる。次に配ったカードを１人目の持っている束が一番下にくるように、順々に重ねて回収する。この操作を N **進シャフリング**という。

＜例＞１０枚のカードを３進シャフリングする時は、

$$\boxed{1}\,\boxed{2}\,\boxed{3}\,\boxed{4}\,\boxed{5}\,\boxed{6}\,\boxed{7}\,\boxed{8}\,\boxed{9}\,\boxed{10}$$

$\Downarrow$　これを３人に配る

①	②	③
1	2	3
4	5	6
7	8	9
10		

余りも最後まで配りきる

$\Downarrow$　③＋②＋①の順に重ねる

$$\boxed{9}\,\boxed{6}\,\boxed{3}\,\boxed{8}\,\boxed{5}\,\boxed{2}\,\boxed{10}\,\boxed{7}\,\boxed{4}\,\boxed{1}$$

となる。これを１回のシャフリングとする。これを繰り返すと、

$$\boxed{4}\,\boxed{2}\,\boxed{3}\,\boxed{7}\,\boxed{5}\,\boxed{6}\,\boxed{1}\,\boxed{10}\,\boxed{8}\,\boxed{9}$$

$$\boxed{8}\,\boxed{6}\,\boxed{3}\,\boxed{10}\,\boxed{5}\,\boxed{2}\,\boxed{9}\,\boxed{1}\,\boxed{7}\,\boxed{4}$$

$$\boxed{7}\,\boxed{2}\,\boxed{3}\,\boxed{1}\,\boxed{5}\,\boxed{6}\,\boxed{4}\,\boxed{9}\,\boxed{10}\,\boxed{8}$$

$$\boxed{10}\,\boxed{6}\,\boxed{3}\,\boxed{9}\,\boxed{5}\,\boxed{2}\,\boxed{8}\,\boxed{4}\,\boxed{1}\,\boxed{7}$$

$$\boxed{1}\,\boxed{2}\,\boxed{3}\,\boxed{4}\,\boxed{5}\,\boxed{6}\,\boxed{7}\,\boxed{8}\,\boxed{9}\,\boxed{10}$$

というように、いつかはカードの並びが元に戻る。この場合は６回で元に戻っているので、周期は６となる。

４進、５進、７進の場合も同様である。

2　方法

Prolog によって、カードの枚数 n に対する３進、４進、５進、７進シャフリングの周期 m をそれぞれ求め、その関係を探る。次に、シャフリングによって定められる置換を、互いに素なサイクルの積によって表す。

2.1　３進シャフリング

/*まず，n 枚のカードを１回だけシャッフルして，それを出力する．*/

```
append0(Z=[]+Z).
append0([A|Z]=[A|X]+Y):-append0(Z=X+Y).

left(A=[]+A,0):-!.
left(A=B+C,N):-N>0,N1 is N-1,!,
            left(A=B1+[X|C],N1),
            append0(B=B1+[X]),!.

half(L=A+B):-length(L,N),
            N1 is floor((N)/2),
            left(L=A+B,N1).

genlist(A,Z,[]):- A>Z,!.
genlist(A,Z,[A|List]):- A1 is A+1,
            genlist(A1,Z,List).

sansin([],[],[],[]).
sansin([X,Y,Z|List],[X|A],[Y|B],[Z|C]):-sansin(List,A,B,C).
sansin([X,Y|List],[X|A],[Y|B],[]):-sansin(List,A,B,C).
sansin([X|List],[X|A],[],[]):-sansin(List,A,B,C).

sansin(List=M):-sansin(List,A,B,C),
   reverse(A,AA),
   reverse(B,BB),
   reverse(C,CC),
   append0(MM=BB+AA),
   append0(M=CC+MM).
```

/*次に，その操作を n 回繰り返す．*/

```
sansin(L,0):-write(L),nl.
sansin(L,N):-sansin(L=M),
              N1 is N-1,
              write(L),nl,
              sansin(M,N1).
```

/*枚数 n を入力し，元に戻ったらシャフリングを終え，その周期を出力する．*/

```
sansin(L,0,A):-write(L),nl.
sansin(L,N,A):-sansin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,sansin(M,N1,A);write(m=N0),true).

sansin(N):-genlist(1,N,L),
            sansin(L,10000,L).

sansin_zoku(L,0,A):-write(L),nl.
```

```
sansin_zoku(L,N,A):-sansin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,sansin_zoku(M,N1,A);write(m=N0),true).

sansin_zoku(List):-max_list(List,Max),
      genlist(1,Max,LL),
      sansin_zoku(List,10000,LL).
```

/*n がＳ～Ｋ枚の時，周期を一気に出力する．*/

```
for(I=<J,I):-I=<J.
for(I=<J,K):-I=<J,
I1 is I+1,for(I1=<J,K).

m_dake_san(L,0,A,NN):-!.
m_dake_san(L,N,A,NN):-sansin(L=M),
                N1 is N-1,
                N0 is 10001-N,
                V is NN/N0,
                gcd(X=(NN,N0)),
                lcm(Y=(NN,N0)),
                (M \==A,m_dake_san(M,N1,A,NN);write(m=N0)).

n_to_m_san(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
           m_dake_san(L,10000,L,N),!.

shf_sansin(S,K):-for(S=<K,N),
           n_to_m_san(N),nl,fail.
shf_sansin(S,K).
```

/*逆転するものを表示する．*/

```
sansin_gyaku(L,0,A):-write(L),nl.
sansin_gyaku(L,N,A):-reverse(A,AA),
                 sansin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==AA,sansin_gyaku(M,N1,A);write(m=N0),tab(4),write(gyaku),true).

bigshf_gyaku(N):-genlist(1,N,L),
            sansin_gyaku(L,10000,L).

m_dake_gyaku(L,0,A,NN):-!.
m_dake_gyaku(L,N,A,NN):-reverse(A,AA),
       sansin(L=M),
       N1 is N-1,
       N0 is 1001-N,
```

```
        P is NN + 1,
        (M\==AA,m_dake_gyaku(M,N1,A,NN);write(gyaku),tab(4),write(m=N0),tab(4),
        write(n+1=P),tab(4),factorize(P,PP),write(PP)).

n_to_m_gyaku(N):-N1 is N,
    genlist(1,N1,L),
    write(n=N1),tab(4),
    m_dake_gyaku(L,1000,L,N),!.

shf_gyaku(S,K):-for(S=<K,N),
    n_to_m_gyaku(N),nl,fail.
shf_gyaku(S,K).



/*シャフリングの結果を用いて, n を入力した時に n のサイクルの積を表示する. */

:-op(700,xfx,is_gr).

member(A,[A|L],1).
member(X,[_|L],P):-member(X,L,P1),
    P is P1+1.

memberd(X,L,R):-member(X,L,P),!.
ifthenelse(P,Q,R):-P -> Q;R.
ifthenelse(P,Q,R):-!.

delete1([A|L]-A=L).
delete1([B|L]-A=[B|M]):-delete1(L-A=M).

cyclic_g(F,A,[W,Z]):-delete1(F-(X:A)=L),
    assertz(c(A)),
    cyclic_g(L,X,[W,Z]),!.
cyclic_g(W,_,[W,D]):-collect1(c,D).

collect1(c,L1):-collect(c,L),
    length(L,N),
    ifthenelse(N==1,L1=[],L1=L),!.

collect(c,[A|L]):-retract1(c(A)),collect(c,L),!.
collect(c,[]):-!.

cyc0(F,F0,W):-member((X:A),F),cyclic_g(F,A,[W,F0]),!.

cyclic([],[]).
cyclic(F,C1):-cyc0(F,W,F0),
    cyclic(F0,C0),cyclic_c(W,C1,C0),!.
cyclic_c([],C,C):-!.
cyclic_c(W,[W|C],C):-!.

num1(X,Y):-length(X,N),num_aux(X,Y,N),!.
num_aux([],[],N).
num_aux([A|L],[(A:NI)|M],N):-length(L,I),
    NI is N-I,
    num_aux(L,M,N).

saikuru(N):-genlist(1,N,L),sansin(L=A),num1(A,D),cyclic(D,LL),write(LL).
```

```
sansin_saikuru(L,0,A,NN):-!.
sansin_saikuru(L,N,A,NN):-sansin(L=M),
               N1 is N-1,
               N0 is 10001-N,
               (M \==A,sansin_saikuru(M,N1,A,NN);write(m=N0),tab(10)).

big_saikuru(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
           sansin_saikuru(L,10000,L,N),saikuru(N),!.



/*n が S～K の時，サイクルの積を一気に表示する．*/

shf_saikuru(S,K):-for(S=<K,N),
           big_saikuru(N),nl,fail.
shf_saikuru(S,K).
```

2.2　4進シャフリング

```
/*n 枚の時の周期 m を表示する*/

yonsin([],[],[],[],[]).
yonsin([X,Y,Z,R|List],[X|A],[Y|B],[Z|C],[R|D]):-yonsin(List,A,B,C,D).
yonsin([X,Y,Z|List],[X|A],[Y|B],[Z|C],[]):-yonsin(List,A,B,C,D).
yonsin([X,Y|List],[X|A],[Y|B],[],[]):-yonsin(List,A,B,C,D).
yonsin([X|List],[X|A],[],[],[]):-yonsin(List,A,B,C,D).

yonsin(List=M0):-yonsin(List,A,B,C,D),
   reverse(A,AA),
   reverse(B,BB),
   reverse(C,CC),
   reverse(D,DD),
   append0(MM=BB+AA),
   append0(M=CC+MM),
   append0(M0=DD+M).

yonsin_s(N):-genlist(1,N,List),
   yonsin(List=M),write(M).

yonsin(L,0):-write(L),nl.
yonsin(L,N):-yonsin(L=M),
              N1 is N-1,
              write(L),nl,
              yonsin(M,N1).

yonsin(L,0,A):-write(L),nl.
yonsin(L,N,A):-yonsin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,yonsin(M,N1,A);write(m=N0),true).
```

```
yonsin(N):-genlist(1,N,L),
            yonsin(L,10000,L).

yonsin_zoku(L,0,A):-write(L),nl.
yonsin_zoku(L,N,A):-yonsin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,yonsin_zoku(M,N1,A);write(m=N0),true).

yonsin_zoku(List):-max_list(List,Max),
       genlist(1,Max,LL),
       yonsin_zoku(List,10000,LL).

m_dake_yon(L,0,A,NN):-!.
m_dake_yon(L,N,A,NN):-yonsin(L=M),
               N1 is N-1,
               N0 is 10001-N,
               V is NN/N0,
               gcd(X=(NN,N0)),
               lcm(Y=(NN,N0)),
               (M \==A,m_dake_yon(M,N1,A,NN);write(m=N0)).

n_to_m_yon(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
           m_dake_yon(L,10000,L,N),!.

shf_yonsin(S,K):-for(S=<K,N),
           n_to_m_yon(N),nl,fail.
shf_yonsin(S,K).



/*逆転するものを表示する*/

yonsin_gyaku(L,0,A):-write(L),nl.
yonsin_gyaku(L,N,A):-reverse(A,AA),
                 yonsin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==AA,yonsin_gyaku(M,N1,A);write(m=N0),tab(4),write(gyaku),true).

bigshf_gyaku(N):-genlist(1,N,L),
            yonsin_gyaku(L,10000,L).

m_dake_gyaku(L,0,A,NN):-!.
m_dake_gyaku(L,N,A,NN):-reverse(A,AA),
           yonsin(L=M),
           N1 is N-1,
           N0 is 1001-N,
           P is NN + 1,
           (M\==AA,m_dake_gyaku(M,N1,A,NN);write(gyaku),tab(4),write(m=N0),
           tab(4),write(n+1=P),tab(4),factorize(P,PP),write(PP)).
```

```
n_to_m_gyaku(N):-N1 is N,
       genlist(1,N1,L),
       write(n=N1),tab(4),
       m_dake_gyaku(L,1000,L,N),!.

shf_gyaku(S,K):-for(S=<K,N),
       n_to_m_gyaku(N),nl,fail.
shf_gyaku(S,K).




/*サイクル積を表示する*/

saikuru(N):-genlist(1,N,L),yonsin(L=A),num1(A,D),cyclic(D,LL),write(LL).

yonsin_saikuru(L,0,A,NN):-!.
yonsin_saikuru(L,N,A,NN):-yonsin(L=M),
               N1 is N-1,
               N0 is 10001-N,
               (M \==A,yonsin_saikuru(M,N1,A,NN);write(m=N0),tab(10)).

big_saikuru(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
           yonsin_saikuru(L,10000,L,N),saikuru(N),!.

shf_saikuru(S,K):-for(S=<K,N),
           big_saikuru(N),nl,fail.
shf_saikuru(S,K).
```

2.3　５進シャフリング

```
/*n 枚の時の周期 m を表示する*/

gosin([],[],[],[],[],[]).
gosin([X1,X2,X3,X4,X5|List],[X1|A],[X2|B],[X3|C],[X4|D],[X5|E]):-gosin(List,A,B,C,D,E).
gosin([X1,X2,X3,X4|List],[X1|A],[X2|B],[X3|C],[X4|D],[]):-gosin(List,A,B,C,D,E).
gosin([X1,X2,X3|List],[X1|A],[X2|B],[X3|C],[],[]):-gosin(List,A,B,C,D,E).
gosin([X1,X2|List],[X1|A],[X2|B],[],[],[]):-gosin(List,A,B,C,D,E).
gosin([X1|List],[X1|A],[],[],[],[]):-gosin(List,A,B,C,D,E).

gosin(List=M):-gosin(List,A,B,C,D,E),
   reverse(A,AA),
   reverse(B,BB),
   reverse(C,CC),
   reverse(D,DD),
   reverse(E,EE),
   append0(M1=EE+DD),
   append0(M2=M1+CC),
   append0(M3=M2+BB),
   append0(M=M3+AA).

gosin(L,0):-write(L),nl.
gosin(L,N):-gosin(L=M),
              N1 is N-1,
              write(L),nl,
```

```
              gosin(M,N1).

gosin(L,0,A):-write(L),nl.
gosin(L,N,A):-gosin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,gosin(M,N1,A);write(m=N0),true).

gosin(N):-genlist(1,N,L),
            gosin(L,10000,L).

gonsin_zoku(L,0,A):-write(L),nl.
gosin_zoku(L,N,A):-gosin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,gosin_zoku(M,N1,A);write(m=N0),true).

gosin_zoku(List):-max_list(List,Max),
      genlist(1,Max,LL),
      gosin_zoku(List,10000,LL).

m_dake_go(L,0,A,NN):-!.
m_dake_go(L,N,A,NN):-gosin(L=M),
               N1 is N-1,
               N0 is 10001-N,
               V is NN/N0,
               gcd(X=(NN,N0)),
               lcm(Y=(NN,N0)),
               (M \==A,m_dake_go(M,N1,A,NN);write(m=N0)).

n_to_m_go(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
           m_dake_go(L,10000,L,N),!.

shf_gosin(S,K):-for(S=<K,N),
           n_to_m_go(N),nl,fail.
shf_gosin(S,K).



/*逆転するものを表示する*/

gosin_gyaku(L,0,A):-write(L),nl.
gosin_gyaku(L,N,A):-reverse(A,AA),
                 gosin(L=M),
                 N1 is N-1,
                 N0 is 101-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==AA,gosin_gyaku(M,N1,A);write(m=N0),tab(4),write(gyaku),true).

bigshf_gyaku(N):-genlist(1,N,L),
            gosin_gyaku(L,100,L).
```

```
m_dake_gyaku(L,0,A,NN):-!.
m_dake_gyaku(L,N,A,NN):-reverse(A,AA),
        gosin(L=M),
        N1 is N-1,
        N0 is 301-N,
        P is NN + 1,
        (M\==AA,m_dake_gyaku(M,N1,A,NN);write(gyaku),tab(4),write(m=N0),tab(4),
        write(n+1=P),tab(4),factorize(P,PP),write(PP)).

n_to_m_gyaku(N):-N1 is N,
       genlist(1,N1,L),
       write(n=N1),tab(4),
       m_dake_gyaku(L,300,L,N),!.

shf_gyaku(S,K):-for(S=<K,N),
       n_to_m_gyaku(N),nl,fail.
shf_gyaku(S,K).




/*サイクルの積を表示する*/

saikuru(N):-genlist(1,N,L),gosin(L=A),num1(A,D),cyclic(D,LL),write(LL).

gosin_saikuru(L,0,A,NN):-!.
gosin_saikuru(L,N,A,NN):-gosin(L=M),
               N1 is N-1,
               N0 is 10001-N,
               (M \==A,gosin_saikuru(M,N1,A,NN);write(m=N0),tab(10)).

big_saikuru(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
           gosin_saikuru(L,10000,L,N),saikuru(N),!.

shf_saikuru(S,K):-for(S=<K,N),
           big_saikuru(N),nl,fail.
shf_saikuru(S,K).
```

2.4　７進シャフリング

```
/*n 枚の時の周期 m を表示する*/

nanasin([],[],[],[],[],[],[],[]).
nanasin([X1,X2,X3,X4,X5,X6,X7|List],[X1|A],[X2|B],[X3|C],[X4|D],[X5|E],[X6|F],[X7|G]):-
                                                            nanasin(List,A,B,C,D,E,F,G).
nanasin([X1,X2,X3,X4,X5,X6|List],[X1|A],[X2|B],[X3|C],[X4|D],[X5|E],[X6|F],[]):-
                                                            nanasin(List,A,B,C,D,E,F,G).
nanasin([X1,X2,X3,X4,X5|List],[X1|A],[X2|B],[X3|C],[X4|D],[X5|E],[],[]):-
                                                            nanasin(List,A,B,C,D,E,F,G).
nanasin([X1,X2,X3,X4|List],[X1|A],[X2|B],[X3|C],[X4|D],[],[],[]):-
                                                            nanasin(List,A,B,C,D,E,F,G).
nanasin([X1,X2,X3|List],[X1|A],[X2|B],[X3|C],[],[],[],[]):-nanasin(List,A,B,C,D,E,F,G).
nanasin([X1,X2|List],[X1|A],[X2|B],[],[],[],[],[]):-nanasin(List,A,B,C,D,E,F,G).
```

```
nanasin([X1|List],[X1|A],[],[],[],[],[],[]):-nanasin(List,A,B,C,D,E,F,G).

nanasin(List=M):-nanasin(List,A,B,C,D,E,F,G),
   reverse(A,AA),
   reverse(B,BB),
   reverse(C,CC),
   reverse(D,DD),
   reverse(E,EE),
   reverse(F,FF),
   reverse(G,GG),
   append0(M1=GG+FF),
   append0(M2=M1+EE),
   append0(M3=M2+DD),
   append0(M4=M3+CC),
   append0(M5=M4+BB),
   append0(M=M5+AA).

nanasin(L,0):-write(L),nl.
nanasin(L,N):-nanasin(L=M),
              N1 is N-1,
              write(L),nl,
              nanasin(M,N1).

nanasin(L,0,A):-write(L),nl.
nanasin(L,N,A):-nanasin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,nanasin(M,N1,A);write(m=N0),true).

nanasin(N):-genlist(1,N,L),
            nanasin(L,10000,L).

nanasin_zoku(L,0,A):-write(L),nl.
nanasin_zoku(L,N,A):-nanasin(L=M),
                 N1 is N-1,
                 N0 is 10001-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==A,nanasin_zoku(M,N1,A);write(m=N0),true).

nanasin_zoku(List):-max_list(List,Max),
      genlist(1,Max,LL),
      nanasin_zoku(List,10000,LL).

m_dake_nana(L,0,A,NN):-!.
m_dake_nana(L,N,A,NN):-nanasin(L=M),
               N1 is N-1,
               N0 is 10001-N,
               V is NN/N0,
               gcd(X=(NN,N0)),
               lcm(Y=(NN,N0)),
               (M \==A,m_dake_nana(M,N1,A,NN);write(m=N0)).

n_to_m_nana(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
```

```
           m_dake_nana(L,10000,L,N),!.

shf_nanasin(S,K):-for(S=<K,N),
           n_to_m_nana(N),nl,fail.
shf_nanasin(S,K).


/*逆転するものを表示する*/

nanasin_gyaku(L,0,A):-write(L),nl.
nanasin_gyaku(L,N,A):-reverse(A,AA),
                 nanasin(L=M),
                 N1 is N-1,
                 N0 is 101-N,
                 write(N0),tab(2),
                 write(L),nl,
                 (M \==AA,nanasin_gyaku(M,N1,A);write(m=N0),tab(4),write(gyaku),true).

bigshf_gyaku(N):-genlist(1,N,L),
            nanasin_gyaku(L,100,L).

m_dake_gyaku(L,0,A,NN):-!.
m_dake_gyaku(L,N,A,NN):-reverse(A,AA),
           nanasin(L=M),
           N1 is N-1,
           N0 is 301-N,
           P is NN + 1,
           (M\==AA,m_dake_gyaku(M,N1,A,NN);write(gyaku),tab(4),write(m=N0),
           tab(4),write(n+1=P),tab(4),factorize(P,PP),write(PP)).

n_to_m_gyaku(N):-N1 is N,
       genlist(1,N1,L),
       write(n=N1),tab(4),
       m_dake_gyaku(L,300,L,N),!.

shf_gyaku(S,K):-for(S=<K,N),
       n_to_m_gyaku(N),nl,fail.
shf_gyaku(S,K).


/*サイクルの積を表示する*/

saikuru(N):-genlist(1,N,L),nanasin(L=A),num1(A,D),cyclic(D,LL),write(LL).

nanasin_saikuru(L,0,A,NN):-!.
nanasin_saikuru(L,N,A,NN):-nanasin(L=M),
               N1 is N-1,
               N0 is 10001-N,
               (M \==A,nanasin_saikuru(M,N1,A,NN);write(m=N0),tab(10)).

big_saikuru(N):-N1 is N,
           genlist(1,N1,L),
           write(n=N1),tab(4),
           nanasin_saikuru(L,10000,L,N),saikuru(N),!.

shf_saikuru(S,K):-for(S=<K,N),
           big_saikuru(N),nl,fail.
shf_saikuru(S,K).
```

3　結果

3.1　枚数 n に対する N 進シャフリングの周期 m

枚数	３進	４進	５進	７進
3	2	—	—	—
4	3	2	—	—
5	4	6	2	—
6	4	5	6	—
7	7	6	5	2
8	8	6	8	6
9	2	9	9	10
10	6	20	6	9
11	10	10	6	30
12	10	10	11	11
13	9	42	15	12
14	6	33	6	12
15	6	10	6	15
16	24	2	9	16
17	16	8	36	18
18	16	20	17	28
19	52	18	18	28
20	4	18	18	4
21	4	20	30	4
22	10	20	22	44
23	22	22	60	80
24	22	22	12	56
25	20	102	2	90
26	6	114	10	120
27	6	18	18	18
28	27	18	238	18
29	28	858	7	110
30	28	70	14	374
31	105	10	420	858
32	32	10	210	30
33	8	220	247	31
34	30	198	16	16
35	12	30	16	16
36	12	6	35	35
37	33	34	124	920
38	18	546	66	120
39	18	6	12	1288
40	39	6	4	39
41	8	96	36	40
42	8	744	572	40
43	288	14	238	360
44	20	14	10	1950
45	10	42	10	126
46	114	45	86	129
47	46	46	84	104
48	46	46	966	16
49	42	1012	21	2
50	20	124	42	14
51	20	4	252	26
52	198	4	510	210
53	52	700	4147	96
54	52	1020	54	660
55	1260	10	18	20
56	24	10	264	20
57	6	340	3472	660
58	120	2886	559	132
59	58	58	58	58
60	58	58	58	280
61	48	264	371	224
62	30	300	2068	30
63	30	6	304	30
64	7337	6	32	63
65	12	114	16	986
66	12	1036	468	4914
67	15961	66	1232	820
68	16	66	364	420
69	16	2040	33	22
70	427	5040	22	22
71	70	70	39270	53592
72	70	70	3588	126
73	285	1050	180	708
74	18	4092	36	300
75	18	50	36	480
76	2544	10	5220	12
77	30	546	2610	6
78	30	4284	864	114
79	3990	78	78	1232
80	16	78	78	700
81	4	82992	3111	4998
82	12	798	2530	5236
83	82	82	150	82
84	82	82	6	82
85	1235	166	6	2790
86	42	85	60	1400
87	42	14	312	850
88	4425	14	86	156
89	88	82992	44	2100
90	88	798	44	12
91	1870	6	1050	12
92	44	6	435	1980
93	22	438	747	172
94	410	2508	46	26520
95	36	90	46	94
96	36	18	95	132990
97	8004	1633	276	96
98	42	7770	18060	96
99	42	30	90	966
100	3237	30	30	276
101	100	4002	1050	2310
102	100	198	1988	6360
103	616	102	468	83076
104	24	102	4	24
105	6	162	4	12
106	31878	70	1044	120
107	106	106	96	25498
108	106	106	1620	100282
109	30932	7810	54	7722
110	20	3696	54	6799

3.2 3進シャフリング

3.2.1 枚数 n、周期 m とその逆転

枚数	周期	逆転	枚数	周期	逆転
3	2	○	57	6	
4	3		58	120	
5	4		59	58	
6	4		60	58	○
7	7		61	48	
8	8		62	30	
9	2		63	30	
10	6		64	7337	
11	10		65	12	
12	10	○	66	12	
13	9		67	15961	
14	6		68	16	
15	6		69	16	
16	24		70	427	
17	16		71	70	
18	16		72	70	○
19	52		73	285	
20	4		74	18	
21	4		75	18	
22	10		76	2544	
23	22		77	30	
24	22	○	78	30	
25	20		79	3990	
26	6		80	16	
27	6	○	81	4	
28	27		82	12	
29	28		83	82	
30	28		84	82	○
31	105		85	1235	
32	32		86	42	
33	8		87	42	
34	30		88	4425	
35	12		89	88	
36	12		90	88	
37	33		91	1870	
38	18		92	44	
39	18		93	22	
40	39		94	410	
41	8		95	36	
42	8		96	36	
43	288		97	8004	
44	20		98	42	
45	10		99	42	
46	114		100	3237	
47	46		101	100	
48	46	○	102	100	
49	42		103	616	
50	20		104	24	
51	20		105	6	
52	198		106	31878	
53	52		107	106	
54	52		108	106	○
55	1260		109	30932	
56	24		110	20	

3.2.2 サイクルの積 (互いに素) とその型

枚数	周期	サイクルの積	型
3	2	(1, 3)	(2,1)
4	3	(1, 3, 4)	(3,1)
5	4	(1, 3, 2, 5) (4)	(4,1)
6	4	(1, 6) (2, 3, 5, 4)	(2,4)
7	7	(1, 6, 4, 2, 3, 5, 7)	(7)
8	8	(1, 6, 7, 4, 5, 2, 3, 8)	(8)
9	2	(1, 9) (2, 6) (4, 8) (3) (5) (7)	(2,2,2,1,1,1)
10	6	(1, 9, 4, 8, 7, 10) (2, 6) (3) (6)	(6,2,1,1)
11	10	(1, 9, 7, 2, 6, 5, 8, 10, 4, 11) (3)	(10,1)
12	10	(1, 12) (2, 9, 10, 7, 5, 11, 4, 3, 6, 8)	(2,10)
13	9	(1, 12, 4, 3, 6, 8, 2, 9, 13) (5, 11, 7) (10)	(9,3,1)
14	6	(1, 12, 7, 8, 5, 14) (2, 9) (3, 6, 11, 10, 13, 4)	(6,2,6)
15	6	(1, 15) (2, 12, 10) (3, 9, 5) (4, 6, 14) (7, 11, 13) (8)	(2,3,3,3,1)
16	24	(1, 15, 4, 6, 14, 7, 11, 16) (2, 12, 13, 10) (3, 9, 5) (8)	(8,4,3,1)
17	16	(1, 15, 7, 14, 10, 5, 3, 9, 8, 11, 2, 12, 16, 4, 6, 17) (13)	(16,1)
18	16	(1, 18) (2, 15, 10, 8, 14, 13, 16, 7, 17, 4, 9, 11, 5, 6, 3, 12)	(2,16)
19	52	(1, 18, 4, 9, 11, 5, 6, 3, 12, 2, 15, 13, 19) (7, 17) (8, 14, 16, 10)	(13,2,4)
20	4	(1, 18, 7, 20) (2, 15, 16, 13) (3, 12, 5, 6) (4, 9, 14, 19) (8, 17, 10, 11)	(4,4,4,4)
21	4	(1, 21) (2, 18, 10, 14) (3, 15, 19, 7) (4, 12, 8, 20) (5, 9, 17, 13) (6) (11) (16)	(2,4,4,4,4,1,1,1)
22	10	(1, 21, 4, 12, 8, 20, 7, 3, 15, 22) (2, 18, 13, 5, 9, 17, 16, 19, 10, 14) (6) (11)	(10,10,1,1)
23	22	(1, 21, 7, 3, 15, 2, 18, 16, 22, 4, 12, 11, 14, 5, 9, 20, 10, 17, 19, 13, 8, 23) (6)	(22,1)
24	22	(1, 24) (2, 21, 10, 20, 13, 11, 17, 22, 7, 6, 9, 23, 4, 15, 5, 12, 14, 8, 3, 18, 19, 16)	(2,22)
25	20	(1, 24, 4, 15, 5, 12, 14, 8, 3, 18, 22, 10, 20, 16, 2, 21, 13, 11, 17, 25) (6, 9, 23, 7) (19)	(20,4,1)

3.3　4進シャフリング

3.3.1　枚数 n、周期 m とその逆転

枚数	周期	逆転
4	2	○
5	6	
6	5	
7	6	
8	6	○
9	9	
10	20	
11	10	
12	10	○
13	42	
14	33	
15	10	
16	2	
17	8	
18	20	
19	18	
20	18	○
21	20	
22	20	
23	22	
24	22	○
25	102	
26	114	
27	18	
28	18	○
29	858	
30	70	
31	10	
32	10	○
33	220	
34	198	
35	30	
36	6	
37	34	
38	546	
39	6	
40	6	
41	96	
42	744	
43	14	
44	14	○
45	42	
46	45	
47	46	
48	46	○
49	1012	
50	124	
51	4	
52	4	
53	700	
54	1020	
55	10	
56	10	
57	340	
58	2886	
59	58	
60	58	○
61	264	
62	300	
63	6	
64	6	○
65	114	
66	1036	
67	66	
68	66	○
69	2040	
70	5040	
71	70	
72	70	○
73	1050	
74	4092	
75	50	
76	10	
77	546	
78	4284	
79	78	
80	78	○
81	82992	
82	798	
83	82	
84	82	○
85	166	
86	85	
87	14	
88	14	
89	82992	
90	798	
91	6	
92	6	
93	438	
94	2508	
95	90	
96	18	
97	1633	
98	7770	
99	30	
100	30	○
101	4002	
102	198	
103	102	
104	102	○
105	162	
106	70	
107	106	
108	106	○
109	7810	
110	3696	

3.3.2 サイクルの積 (互いに素) とその型

枚数	周期	サイクルの積	型
4	2	(1, 4) (2, 3)	(2,2)
5	6	(1, 4, 5) (2, 3)	(3,2)
6	5	(1, 4, 2, 3, 6) (5)	(5,1)
7	6	(1, 4, 6, 5, 2, 7) (3)	(6,1)
8	6	(1, 8) (2, 4, 3, 7, 5, 6)	(2,6)
9	9	(1, 8, 5, 6, 2, 4, 3, 7, 9)	(9)
10	20	(1, 8, 9, 5, 10) (2, 4, 3, 7) (6)	(5,4,1)
11	10	(1, 8, 2, 4, 7, 6, 10, 5, 3, 11) (9)	(10,1)
12	10	(1, 12) (2, 8, 6, 3, 4, 11, 5, 7, 10, 9)	(2,10)
13	42	(1, 12, 5, 7, 10, 13) (2, 8, 6, 3, 4, 11, 9)	(6,7)
14	33	(1, 12, 9, 6, 3, 4, 11, 13, 5, 7, 14) (2, 8, 10)	(11,3)
15	10	(1, 12, 13, 9, 10, 6, 7, 3, 4, 15) (2, 8, 14, 5, 11)	(10,5)
16	2	(1, 16) (2, 12) (3, 8) (5, 15) (6, 11) (9, 14) (4) (7) (10) (13)	(2,2,2,2,2,2,1,1,1,1)
17	8	(1, 16, 5, 15, 9, 14, 13, 17) (2, 12) (3, 8) (6, 11) (4) (7) (10)	(8,2,2,2,1,1,1)
18	20	(1, 16, 9, 18) (2, 12, 6, 11, 10, 14, 17, 5, 15, 13) (3, 8) (4) (7)	(4,10,2,1,1)
19	18	(1, 16, 13, 6, 15, 17, 9, 3, 8, 7, 11, 14, 2, 12, 10, 18, 5, 19) (4)	(18,1)
20	18	(1, 20) (2, 16, 17, 13, 10, 3, 12, 14, 6, 19, 5, 4, 8, 11, 18, 9, 7, 15)	(2,18)
21	20	(1, 20, 5, 4, 8, 11, 18, 13, 10, 3, 12, 14, 6, 19, 9, 7, 15, 2, 16, 21) (17)	(20,1)
22	20	(1, 20, 9, 7, 15, 6, 19, 13, 14, 10, 3, 12, 18, 17, 21, 5, 4, 8, 11, 22) (2, 16)	(20,2)
23	22	(1, 20, 13, 18, 21, 9, 11, 3, 12, 22, 5, 4, 8, 15, 10, 7, 19, 17, 2, 16, 6, 23) (14)	(22,1)
24	22	(1, 24) (2, 20, 17, 6, 4, 12, 3, 16, 10, 11, 7, 23, 5, 8, 19, 21, 13, 22, 9, 15, 14, 18)	(2,22)
25	102	(1, 24, 5, 8, 19, 25) (2, 20, 21, 17, 6, 4, 12, 3, 16, 10, 11, 7, 23, 9, 15, 14, 18) (13, 22)	(6,17,2)

3.4　５進シャフリング

3.4.1　枚数 n、周期 m とその逆転

枚数	周期	逆転
5	2	○
6	6	
7	5	
8	8	
9	9	
10	6	
11	6	
12	11	
13	15	
14	6	
15	6	
16	9	
17	36	
18	17	
19	18	
20	18	○
21	30	
22	22	
23	60	
24	12	
25	2	
26	10	
27	18	
28	238	
29	7	
30	14	
31	420	
32	210	
33	247	
34	16	
35	16	
36	35	
37	124	
38	66	
39	12	
40	4	
41	36	
42	572	
43	238	
44	10	
45	10	○
46	86	
47	84	
48	966	
49	21	
50	42	
51	252	
52	510	
53	4147	
54	54	
55	18	
56	264	
57	3472	
58	559	
59	58	
60	58	○
61	371	
62	2068	
63	304	
64	32	
65	16	
66	468	
67	1232	
68	364	
69	33	
70	22	
71	39270	
72	3588	
73	180	
74	36	
75	36	
76	5220	
77	2610	
78	864	
79	78	
80	78	○
81	3111	
82	2530	
83	150	
84	6	
85	6	
86	60	
87	312	
88	86	
89	44	
90	44	
91	1050	
92	435	
93	747	
94	46	
95	46	
96	95	
97	276	
98	18060	
99	90	
100	30	
101	1050	
102	1988	
103	468	
104	4	
105	4	
106	1044	
107	96	
108	1620	
109	54	
110	54	○

3.4.2 サイクルの積 (互いに素) とその型

枚数	周期	サイクルの積	型
5	2	(1, 5) (2, 4) (3)	(2,2,1)
6	6	(1, 5, 6) (2, 4) (3)	(3,2,1)
7	5	(1, 5, 2, 4, 7) (3) (6)	(5,1,1)
8	8	(1, 5, 7, 6, 2, 4, 3, 8)	(8)
9	9	(1, 5, 3, 4, 8, 6, 7, 2, 9)	(9)
10	6	(1, 10) (2, 5, 8) (3, 9, 6) (4) (7)	(2,3,3,1,1)
11	6	(1, 10, 6, 3, 9, 11) (2, 5, 8) (4) (7)	(6,3,3,1,1)
12	11	(1, 10, 11, 6, 3, 9, 2, 5, 8, 7, 12) (4)	(6,6,2)
13	15	(1, 10, 2, 5, 13) (3, 9, 7) (6, 8, 12) (4) (11)	(5,3,3,1,1)
14	6	(1, 10, 7, 8, 3, 14) (2, 5, 4, 9, 12, 11) (6, 13)	(6,6,2)
15	6	(1, 15) (2, 10, 12) (3, 5, 9) (4, 14, 6) (7, 13, 11) (8)	(2,3,3,3,3,1)
16	9	(1, 15, 6, 4, 14, 11, 7, 13, 16) (2, 10, 12) (3, 5, 9) (8)	(9,3,3,1)
17	36	(1, 15, 11, 12, 7, 13, 2, 10, 17) (3, 5, 9) (4, 14, 16, 6) (8)	(9,3,4,1)
18	17	(1, 15, 16, 11, 17, 6, 4, 14, 2, 10, 3, 5, 9, 8, 13, 7, 18) (12)	(17,1)
19	18	(1, 15, 2, 10, 8, 18, 6, 9, 13, 12, 17, 11, 3, 5, 14, 7, 4, 19) (16)	(18,1)
20	18	(1, 20) (2, 15, 7, 9, 18, 11, 8, 4, 5, 19, 6, 14, 12, 3, 10, 13, 17, 16)	(2,18)
21	30	(1, 20, 6, 14, 12, 3, 10, 13, 17, 21) (2, 15, 7, 9, 18, 16) (4, 5, 19, 11, 8)	(10,6,5)
22	22	(1, 20, 11, 8, 4, 5, 19, 16, 7, 9, 18, 21, 6, 14, 17, 2, 15, 12, 3, 10, 13, 22)	(22)
23	60	(1, 20, 16, 12, 8, 4, 5, 19, 21, 11, 13, 3, 10, 18, 2, 15, 17, 7, 9, 23) (6, 14, 22)	(20,3)
24	12	(1, 20, 21, 16, 17, 12, 13, 8, 9, 4, 5, 24) (2, 15, 22, 11, 18, 7, 14, 3, 10, 23, 6, 19)	(12,12)
25	2	(1, 25) (2, 20) (3, 15) (4, 10) (6, 24) (7, 19) (8, 14) (11, 23) (12, 18) (16, 22) (5) (9) (13) (17) (21)	(2,2,2,2,2,2,2,2,2,2, 1,1,1,1,1)

3.5 7進シャフリング

3.5.1 枚数 n、周期 m とその逆転

枚数	周期	逆転			
7	2	○	59	58	
8	6		60	280	
9	10		61	224	
10	9		62	30	
11	30		63	30	
12	11		64	63	
13	12		65	986	
14	12		66	4914	○
15	15		67	820	
16	16		68	420	
17	18		69	22	
18	28		70	22	
19	28		71	53592	
20	4		72	126	
21	4		73	708	
22	44		74	300	
23	80		75	480	
24	56		76	12	
25	90		77	6	
26	120		78	114	
27	18		79	1232	
28	18	○	80	700	
29	110		81	4998	
30	374		82	5236	
31	858		83	82	
32	30		84	82	
33	31		85	2790	
34	16		86	1400	
35	16		87	850	○
36	35		88	156	
37	920		89	2100	
38	120		90	12	
39	1288		91	12	
40	39		92	1980	
41	40		93	172	
42	40		94	26520	
43	360		95	94	
44	1950		96	132990	
45	126		97	96	
46	129		98	96	
47	104		99	966	
48	16		100	276	
49	2		101	2310	
50	14		102	6360	
51	26		103	83076	
52	210		104	24	
53	96		105	12	
54	660		106	120	
55	20		107	25498	
56	20		108	100282	
57	660		109	7722	
58	132		110	6799	

3.5.2 サイクルの積 (互いに素) とその型

枚数	周期	サイクルの積	型
7	2	(1, 7) (2, 6) (3, 5) (4)	(2,2,2,1)
8	6	(1, 7, 8) (2, 6) (3, 5) (4)	(3,2,2,1)
9	10	(1, 7, 2, 6, 9) (3, 5) (4) (8)	(5,2,1,1)
10	9	(1, 7, 9, 8, 2, 6, 3, 5, 10) (4)	(9,1)
11	30	(1, 7, 3, 5, 4, 11) (2, 6, 10, 8, 9)	(6,5)
12	11	(1, 7, 10, 2, 6, 4, 5, 11, 8, 3, 12) (9)	(11,2)
13	12	(1, 7, 4, 12, 8, 10, 9, 3, 6, 11, 2, 13) (5)	(12,1)
14	12	(1, 14) (2, 7, 11, 9, 10, 3, 13, 8, 4, 6, 5, 12)	(2,12)
15	15	(1, 14, 8, 4, 6, 5, 12, 2, 7, 11, 9, 10, 3, 13, 15)	(15)
16	16	(1, 14, 15, 8, 4, 6, 5, 12, 9, 10, 3, 13, 2, 7, 11, 16)	(16)
17	18	(1, 14, 2, 7, 11, 3, 13, 9, 17) (4, 6, 5, 12, 16, 8) (10) (15)	(9,6,1,1)
18	28	(1, 14, 9, 4, 6, 5, 12, 3, 13, 16, 15, 2, 7, 18) (8, 11, 10, 17)	(14,4)
19	28	(1, 14, 16, 2, 7, 5, 19) (3, 13) (4, 6, 12, 10) (8, 18) (9, 11, 17, 15)	(7,2,4,2,4)
20	4	(1, 14, 3, 20) (2, 7, 12, 17) (4, 13, 10, 11) (5, 6, 19, 8) (9, 18, 15, 16)	(4,4,4,4,4)
21	4	(1, 21) (2, 14, 10, 18) (3, 7, 19, 15) (4, 20, 8, 12) (5, 13, 17, 9) (6) (11) (16)	(2,4,4,4,4,1,1,1)
22	44	(1, 21, 8, 12, 4, 20, 15, 3, 7, 19, 22) (2, 14, 10, 18) (5, 13, 17, 9) (6) (11) (16)	(11,4,4,1,1,1)
23	80	(1, 21, 15, 3, 7, 19, 2, 14, 10, 18, 9, 5, 13, 17, 16, 23) (4, 20, 22, 8, 12) (6) (11)	(16,5,1,1)
24	56	(1, 21, 22, 15, 10, 18, 16, 3, 7, 19, 9, 5, 13, 24) (2, 14, 17, 23, 8, 12, 4, 20) (6) (11)	(14,8,1,1)
25	90	(1, 21, 2, 14, 24, 8, 12, 11, 18, 23, 15, 17, 3, 7, 19, 16, 10, 25) (4, 20, 9, 5, 13) (6) (22)	(18,5,1,1)

4　考察

4.1　サイクルの積との関係

サイクルの積の要素に注目してみると、各々のサイクルの長さの最小公倍数は、周期 m と等しいことがわかった。このことは、次のように置換の理論から証明できる。

定義１：置換 h は共通部分のないサイクルの積でかける。

定義２：$\sigma^m = \varepsilon$ となる最小の自然数 m を σ の位数という。

定義２より、カードが元に戻る回数 m と位数 m は等しい。

定理１ h の位数 m(周期) は、各サイクルの長さの最小公倍数である。

この定理を証明するために、次の補題を示す。

補題① 長さ r のサイクルの位数は r である。 ② 互いに素であるサイクルの積の位数は、各々のサイクルの長さの最小公倍数である。

[証明]

① 長さ r のサイクルを $\sigma = (a_1, a_2, \cdots, a_r)$ とする。

$$\sigma^r(a_1) = \sigma^{r-1}(\sigma(a_1)) = \sigma^{r-1}(a_2) = \cdots = \sigma^1(a_r) = a_1$$
$$\sigma^r(a_2) = \sigma^{r-1}(\sigma(a_2)) = \sigma^{r-1}(a_3) = \cdots = \sigma^1(a_1) = a_2$$
$$\cdots$$

となり、a_r のときも同様である。よって長さ r のサイクルは r 乗すると恒等置換 ε になる。
r が恒等置換になる最小の数であることは明らか。従って長さ r のサイクルの位数は r である。

② $\sigma = \sigma_1\sigma_2\cdots\sigma_l$,　σ_k $(k = 1, \cdots, l)$ の長さを r_k $(k = 1, \cdots, l)$ とする。

互いに素であるサイクルの積は可換であるから、

$$\begin{aligned}\sigma^s &= (\sigma_1\sigma_2\cdots\sigma_l)^s \\ &= \sigma_1^s\sigma_2^s\cdots\sigma_l^s\end{aligned}$$

となる。　①より長さ r のサイクルの位数は r であったから、

$$\sigma_1^{r_1} = \sigma_2^{r_2} = \cdots = \sigma_k^{r_k} = \epsilon$$

となる。すなわち、$\sigma^s = \epsilon$ となる s は、$r_1, r_2, \cdots, r_k$ の最小公倍数であることは明らか。

以上より、定理１が示された。

4.2　n = N^k のとき

3.1 の表より、$N = 3,4,5,7$ について、$n = N, N^2$ のときには、周期はすべて $m = 2$ である。
同様に、$n = N^3$ なら $m = 6$、
$n = N^4$ なら $m = 4$、
$n = N^5$ なら $m = 10$、
$\vdots$
以下、$n = N^k$ のときの周期 m をわかりやすく表でまとめてみた。

n	3 進	4 進	5 進	7 進
N	2	2	2	2
N^2	2	2	2	2
N^3	6	6	6	6
N^4	4	4	4	4
N^5	10	10	10	10
N^6	6	6	6	6
N^7	14	14	14	14

$n = N^k$ のときの周期は、表より一目瞭然である。

予想
N^k 枚の周期は、$k = 2l \quad (l = 1,2,\cdots)$ のとき k
$k = 2l - 1 \quad (l = 1,2,\cdots)$ のとき $2k$
である。特に $k = 2l - 1$ のときは k 回目で逆転する。

[証明]
$n = N$ のとき
N 枚のカードの最初の並びを $[a_1, a_2, \cdots, a_N]$ とする。
N 枚のカードを N 個に分け、1 番目のカードが一番下にくるように重ねるので、
シャフリングの操作は以下のようになる。

$[a_1, a_2, \cdots, a_{N-1}, a_N]$
$\downarrow$ 1 回目のシャフリング
$[a_N, a_{N-1}, \cdots, a_2, a_1]$
$\downarrow$ 2 回目のシャフリング
$[a_1, a_2, \cdots, a_{N-1}, a_N]$

というように、1 回目のシャフリングで逆転し、2 回目のシャフリングで元に戻る。
よって $n = N$ の周期は 2 で、1 回目で逆転する。

$n = N^2$ のとき
便宜上、N^2 枚のカードの最初の並びを N 次正方行列に見立て、

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{N1} & \cdots & \cdots & a_{NN} \end{bmatrix}$$

とする。

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{N1} & \cdots & \cdots & a_{NN} \end{bmatrix} \to \begin{bmatrix} a_{NN} & a_{N-1N} & \cdots & a_{1N} \\ \vdots & & & \vdots \\ \vdots & & & a_{12} \\ a_{N1} & \cdots & \cdots & a_{11} \end{bmatrix} \to \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ \vdots & & & \vdots \\ \vdots & & & a_{N-1N} \\ a_{N1} & \cdots & \cdots & a_{NN} \end{bmatrix}$$

となり、$n = N^2$ は固定点 $a_{1N}, a_{2N-1}, a_{3N-2}, \cdots, a_{N1}$ を対称軸に入れ替わり、
２回のシャフリングで元に戻る。

$n = N^3$のとき

$n = N^3$ のとき $n = N^2$ のときと同様のやり方で表すと、$N \times N^2$ 行列になるので、
N 段の $N \times N$ 行列があると見立て、

$$\left[\begin{array}{cccc} a_{(1,1,1)} & a_{(1,1,2)} & \cdots & a_{(1,1,N)} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{(1,N,1)} & \cdots & \cdots & a_{(1,N,N)} \\ \hline \multicolumn{4}{c}{\vdots} \\ \multicolumn{4}{c}{\vdots} \\ \hline a_{(N,1,1)} & a_{(N,1,2)} & \cdots & a_{(N,1,N)} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{(N,N,1)} & \cdots & \cdots & a_{(N,N,N)} \end{array}\right]$$

となる。このとき、α 段、β 行、γ 列の文字を $a_{(\alpha,\beta,\gamma)}$ と表示することにする。$(1 \leq \alpha, \beta, \gamma \leq N)$

$$\left[\begin{array}{cccc} a_{(1,1,1)} & a_{(1,1,2)} & \cdots & a_{(1,1,N)} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{(1,N,1)} & \cdots & \cdots & a_{(1,N,N)} \\ \hline \multicolumn{4}{c}{\vdots} \\ \multicolumn{4}{c}{\vdots} \\ \hline a_{(N,1,1)} & a_{(N,1,2)} & \cdots & a_{(N,1,N)} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{(N,N,1)} & \cdots & \cdots & a_{(N,N,N)} \end{array}\right] \to \left[\begin{array}{cccc} a_{(N,N,N)} & a_{(N,N-1,N)} & \cdots & a_{(N,1,N)} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{(1,N,N)} & \cdots & \cdots & a_{(1,1,N)} \\ \hline \multicolumn{4}{c}{\vdots} \\ \multicolumn{4}{c}{\vdots} \\ \hline a_{(N,N,1)} & a_{(N,N-1,1)} & \cdots & a_{(N,1,1)} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{(1,N,1)} & \cdots & \cdots & a_{(1,1,1)} \end{array}\right]$$

$$
\to \left[\begin{array}{cccc}
a_{(1,1,1)} & a_{(2,1,1)} & \cdots & a_{(N,1,1)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(1,1,N)} & \cdots & \cdots & a_{(N,1,N)} \\
\hline
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\vdots} \\
\hline
a_{(1,N,1)} & a_{(N,1,2)} & \cdots & a_{(N,N,1)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(1,N,N)} & \cdots & \cdots & a_{(N,N,N)}
\end{array}\right]
\to \left[\begin{array}{cccc}
a_{(N,N,N)} & a_{(N,N,N-1)} & \cdots & a_{(N,N,1)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(N,1,N)} & \cdots & \cdots & a_{(N,1,1)} \\
\hline
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\vdots} \\
\hline
a_{(1,N,N)} & a_{(1,N,N-1)} & \cdots & a_{(1,N,1)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(1,1,N)} & \cdots & \cdots & a_{(1,1,1)}
\end{array}\right]
$$

$$
\to \left[\begin{array}{cccc}
a_{(1,1,1)} & a_{(1,2,1)} & \cdots & a_{(1,N,1)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(N,1,1)} & \cdots & \cdots & a_{(N,N,1)} \\
\hline
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\vdots} \\
\hline
a_{(1,1,N)} & a_{(1,2,N)} & \cdots & a_{(1,N,N)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(N,1,N)} & \cdots & \cdots & a_{(N,N,N)}
\end{array}\right]
\to \left[\begin{array}{cccc}
a_{(N,N,N)} & a_{(N-1,N,N)} & \cdots & a_{(1,N,N)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(N,N,1)} & \cdots & \cdots & a_{(1,N,1)} \\
\hline
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\vdots} \\
\hline
a_{(N,1,N)} & a_{(N-1,1,N)} & \cdots & a_{(1,1,N)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(N,1,1)} & \cdots & \cdots & a_{(1,1,1)}
\end{array}\right]
$$

$$
\to \left[\begin{array}{cccc}
a_{(1,1,1)} & a_{(1,1,2)} & \cdots & a_{(1,1,N)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(1,N,1)} & \cdots & \cdots & a_{(1,N,N)} \\
\hline
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\vdots} \\
\hline
a_{(N,1,1)} & a_{(N,1,2)} & \cdots & a_{(N,1,N)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(N,N,1)} & \cdots & \cdots & a_{(N,N,N)}
\end{array}\right]
$$

となる。一般に $a_{(\alpha,\beta,\gamma)}$ は、

$$
a_{(\alpha,\beta,\gamma)} \to a_{(N-\beta+1,N-\gamma+1,N-\alpha+1)} \to a_{(\gamma,\alpha,\beta)} \to a_{(N-\alpha+1,N-\beta+1,N-\gamma+1)} \to a_{(\beta,\gamma,\alpha)} \to a_{(N-\gamma+1,N-\alpha+1,N-\beta+1)} \to a_{(\alpha,\beta,\gamma)}
$$

と変化していることがわかった。よって、$n = N^3$ の周期は 6 で、3 回目で逆転する。

この証明から、a の添え字の個数を k 個としたとき、

$$\boxed{\begin{aligned}
&a_{(\alpha,\beta,\gamma,\delta,\cdots)} \quad (1 \leq \alpha,\beta,\gamma,\delta,\cdots \leq N) \text{ は、}\\
&\qquad a_{(\alpha,\beta,\gamma,\delta,\cdots)} \to a_{(N-\beta+1,N-\gamma+1,N-\delta,\cdots,N-\alpha+1)}\\
&\qquad\qquad \to a_{(\gamma,\delta,\cdots,\alpha,\beta)}\\
&\qquad\qquad \to a_{(N-\delta+1,\cdots,N-\alpha+1,N-\beta+1,N-\gamma+1)}\\
&\qquad\qquad \to \cdots\\
&\qquad\qquad \to a_{(\alpha,\beta,\gamma,\delta,\cdots)}
\end{aligned}}$$

が成立するのではないかと推測した。

[証明]

n = N^k のとき、$N \times N$ 行列が N^{k-2} 段あり、それを N^{k-3} ずつに分け $\cdots$ と、N 等分のかたまりで k 個の段階に区切っていき、各成分 $a_{(\alpha,\beta,\gamma,\delta,\cdots)}$ $(1 \leq \alpha,\beta,\gamma,\delta,\cdots \leq N)$ を考える。

$$\left[\begin{array}{cccc}
a_{(1,1,\cdots,1,1)} & a_{(1,1,\cdots,1,2)} & \cdots & a_{(1,1,\cdots,1,N)}\\
a_{(1,1,\cdots,2,1)} & & & \vdots\\
\vdots & & & \vdots\\
a_{(1,1,\cdots,N,1)} & \cdots & \cdots & a_{(1,1,\cdots,N,N)}\\
\hline
\multicolumn{4}{c}{\vdots}\\
\multicolumn{4}{c}{\vdots}\\
\hline
a_{(N,N,\cdots,1,1)} & a_{(N,N,\cdots,1,2)} & \cdots & a_{(N,N,\cdots,1,N)}\\
\vdots & & & \vdots\\
\vdots & & & a_{(N,N,\cdots,N-1,N)}\\
a_{(N,N,\cdots,N,1)} & \cdots & \cdots & a_{(N,N,\cdots,N,N)}
\end{array}\right]$$

$$\to \left[\begin{array}{cccc}
a_{(N,N,\cdots,N,N)} & a_{(N,N,\cdots,N-1,N)} & \cdots & a_{(N,N,\cdots,1,N)}\\
a_{(N,N,\cdots,N-1,N,N)} & & & \vdots\\
\vdots & & & \vdots\\
a_{(N,N,\cdots,1,N,N)} & \cdots & \cdots & a_{(N,N,\cdots,1,1,N)}\\
\hline
\multicolumn{4}{c}{\vdots}\\
\multicolumn{4}{c}{\vdots}\\
\hline
a_{(1,1,\cdots,N,N,1)} & a_{(1,1,\cdots,N,N-1,1)} & \cdots & a_{(1,1,\cdots,N,1,1)}\\
a_{(1,1,\cdots,N-1,N,1)} & & & \vdots\\
\vdots & & & a_{(1,1,\cdots,2,1,1)}\\
a_{(1,1,\cdots,N,1)} & \cdots & a_{(1,1,\cdots,2,1)} & a_{(1,1,\cdots,1,1)}
\end{array}\right]$$

$$
\to \left[\begin{array}{cccc}
a_{(1,1,\cdots,1,1)} & a_{(1,1,\cdots,2,1,1)} & \cdots & a_{(1,1,\cdots,N,1,1)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(1,1,\cdots,N,1,1,1)} & \cdots & \cdots & a_{(1,1,\cdots,N,N,1,1)} \\
\hline
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\vdots} \\
\hline
a_{(N,N,\cdots,1,1,N,N)} & \cdots & \cdots & a_{(N,N,\cdots,1,N,N,N)} \\
\vdots & & & \vdots \\
\vdots & & & \vdots \\
a_{(N,N,\cdots,1,N,N)} & \cdots & a_{(N,N,\cdots,N-1,N,N)} & a_{(N,N,\cdots,N,N)}
\end{array}\right]
$$

$$\to \cdots$$

$$
\to \left[\begin{array}{cccc}
a_{(1,1,\cdots,1,1)} & a_{(1,1,\cdots,1,2)} & \cdots & a_{(1,1,\cdots,1,N)} \\
a_{(1,1,\cdots,2,1)} & & & \vdots \\
\vdots & & & \vdots \\
a_{(1,1,\cdots,N,1)} & \cdots & \cdots & a_{(1,1,\cdots,N,N)} \\
\hline
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\vdots} \\
\hline
a_{(N,N,\cdots,1,1)} & a_{(N,N,\cdots,1,2)} & \cdots & a_{(N,N,\cdots,1,N)} \\
\vdots & & & \vdots \\
\vdots & & & a_{(N,N,\cdots,N-1,N)} \\
a_{(N,N,\cdots,N,1)} & \cdots & \cdots & a_{(N,N,\cdots,N,N)}
\end{array}\right]
$$

となるので、この公式を証明することができた。

実際に $k=4$ のときをやってみると、$a_{(\alpha,\beta,\gamma,\delta)}$ $(1 \leq \alpha,\beta,\gamma,\delta \leq N)$ において、

$$a_{(\alpha,\beta,\gamma,\delta)} \to a_{(N-\beta+1,N-\gamma+1,N-\delta+1,N-\alpha+1)} \to a_{(\gamma,\delta,\alpha,\beta)} \to a_{(N-\delta+1,N-\alpha+1,N-\beta+1,N-\gamma+1)} \to a_{(\alpha,\beta,\gamma,\delta)}$$

となり、確かに４回で元に戻っている。

この公式から、

$n=N^k$ において、k が偶数なら k 回で元に戻り、 k が奇数なら k 回で逆転し、$2k$ 回で元に戻る。

という予想は、正しいことが証明された。

4.3　逆転するとき

カードの並びが最初の並びと逆転するものがあることがわかった。以下に逆転するものだけを表にまとめ、その特徴は何なのか考えてみる。

N	3 進	4 進	5 進	7 進
n	3	4	5	7
	12	8	20	28
	24	12	45	63
	27	20	60	84
	48	24	80	112
	60	28	110	119
	72	32		
	84	44		
	108	48		
		60		
		64		
		68		
		72		
		80		
		84		
		100		
		104		
		108		

表より、逆転をする必要条件は、n が N 倍の数であると予想できる。周期も $n-2$ となるものが多い。また、この n を N で割ってみると、

N	3 進	4 進	5 進	7 進
n	3=3 × 1 12=3 × 4 24=3 × 6 27=3 × 9 48=3 × 16 60=3 × 20 72=3 × 26 84=3 × 28 108=3 × 36	4=4 × 1 8=4 × 2 12=4 × 3 20=4 × 5 24=4 × 6 28=4 × 7 32=4 × 8 44=4 × 11 48=4 × 12 60=4 × 15 64=4 × 16 68=4 × 17 72=4 × 18 80=4 × 20 84=4 × 21 100=4 × 25 104=4 × 26 108=4 × 27	5=5 × 1 20=5 × 4 45=5 × 9 60=5 × 12 80=5 × 18 110=5 × 22	7=7 × 1 28=7 × 4 63=7 × 9 84=7 × 12 112=7 × 16 119=7 × 17

というように、平方の数がかけられていることが多い。

また、逆転をするもののサイクルの積に着目すると、面白いことに気がついた。各サイクルの要素を半分にして上下に並べ、それぞれ足し算をすると、すべて $n+1$ になっている。24 枚のときの 3 進シャフリングのサイクルの積で説明すると、

$$(1,24) \quad (2,21,10,20,13,11,17,22,7,6,9,23,4,15,5,12,14,8,3,18,19,16)$$

$$\Downarrow$$

$$\begin{array}{rcrrrrrrrrrrr} 1 & & 2 & 21 & 10 & 20 & 13 & 11 & 17 & 22 & 7 & 6 & 9 \\ +\,24 & & 23 & 4 & 15 & 5 & 12 & 14 & 8 & 3 & 18 & 19 & 16 \\ \hline 25 & & 25 & 25 & 25 & 25 & 25 & 25 & 25 & 25 & 25 & 25 & 25 \end{array}$$

これは逆転をするとき以外にもあり得る。このことから何が導かれるのか、解明することはできなかった。

逆転については、今後も研究を進めていきたいと思う。

5　おわりに

5.1　感想

カードのシャフリングというテーマは、日常でも使われるような具体的な内容で、非常に興味を持って研究することができました。自分なりに研究を進めていくうちに、自分で規則性を発見したり、定理を導いたりすることができて、すごくオリジナルな研究になってしまいましたが、本当に良かったと思います。N 進シャフリングについては、まだまだ謎がたくさん残されているので、いつか解明できればと思います。

最初の頃はプロログを理解できず、ただ単にプリントの通りにプログラムを打ち込んでいただけでしたが、自分でプログラムを考え、理解しはじめてからは一気にその面白さに引き込まれ、深夜遅くまでプロログに没頭した日もありました。プログラムを実行して、思い通りの結果が出力されるのは本当に快感でした。

飯高先生には、最初から最後まで本当にお世話になり、心から感謝しています。この研究室はとても楽しかったです。高校のときにオープンキャンパスで飯高先生に心をひかれ、この大学に入学し、先生の研究室に入って、本当に良かったと思っています。１年間ありがとうございました♡

5.2　参考文献

[1] George E.Andrews 著 『Number Theory』
[2] 野崎昭弘 著 『トランプ』