3分シャフリングの研究

学習院大学理学部数学科
羽田早織

平成 20 年 2 月 4 日

目 次

1　目的

N 枚 (ただし、N は 3 の倍数で正とする）のカードを 3 等分することによるシャフリングした結果を調べ、その周期などを考察する。

2　方法

2.1　シャフリングの方法

$[\underbrace{1, 2, 3, 4, \cdots, n}_{A}, \underbrace{n+1, n+2, \cdots, 2n}_{B}, \underbrace{2n+1, \cdots, 3n}_{C}]$

N 枚のカードを均等に 3 等分し下の表の様に分ける。

表 1:

C	B	A
$2n+1$	$n+1$	1
$2n+2$	$n+2$	2
$2n+3$	$n+3$	3
$\cdots$	$\cdots$	$\cdots$
$3n$	$2n$	n

表の 1 段目,2 段目,$\cdots$と並べていく。

$[2n+1, n+1, 1, 2n+2, n+2, 2, \cdots, 3n, 2n, n]$

これを繰り返す。

****

<補足>

◎ 2 分シャフリングの方法

N 枚のカードを並べ、

$[1, 2, 3, 4, \cdots, n, n+1, \cdots, 2n]$

均等に半分に分け、下のように表にする。

表 2:

$n+1$	1
$n+2$	2
$\cdots$	$\cdots$
$2n$	n

表の 1 段目,2 段目,…と並べていく。
[n + 1, 1, n + 2, 2, ⋯, 2n, n]
と、並べ替えることを繰り返す。

◎ 4 分シャフリングの方法
N 枚のカードを並べ、
[1, 2, 3, 4, ⋯, n, n + 1, ⋯, 2n, 2n + 1, ⋯, 3n, 3n + 1, ⋯, 4n]

下のように表にする。

表 3:

3n + 1	2n + 1	n + 1	1
3n + 2	2n + 2	n + 2	2
3n + 3	2n + 3	n + 3	3
⋯	⋯	⋯	⋯
4n	3n	2n	n

表の 1 段目,2 段目,…と並べていく。
[3n + 1, 2n + 1, n + 1, 1, ⋯, 4n, 3n, 2n, n]
と並べ替えることを繰り返す。

****

2.2 Prolog

このシャフリングを Prolog を用いてコンピューター上に実現し考える。

```
/*3 つに分ける*/
third(L=A+B+C) :- length(L,N),
    N1 is N/3,
    N2 is N/3,
    mid(L=A+C+B,N1,N2),!.

mid(L=A+C+B,N,M) :- left(L=A+D,N),left(D=B+C,M).

/*シャフリング*/
shf3([]+[]+[]=[]).
shf3([X|C]+[Y|B]+[Z|A]=[X,Y,Z|M]) :- shf3(C+B+A=M).
```

```
sh3(L=M) :- third(L=A+B+C),shf3(C+B+A=M),!.


shuffle3(L,0,L) :- write(L).
shuffle3(L,N,A) :- sh3(L=M),
    N1 is N-1,
    N0 is 301-N,
    (M==A -> (write(m=N0),tab(1));shuffle3(M,N1,A)).


shuffle12(L,0) :- write(L),nl.
  shuffle12(L,N) :- sh3(L=M),N1 is N-1,
  write(L),nl,shuffle12(M,N1).


/*元に戻るまでの回数 (周期) と枚数+1 の素因数分解*/
bigshf3(N) :- N1 is 3*N,N2 is N1+1,
    genlist(1,N1,L),
    write(n=N),tab(1),
    write(k=N1),tab(1),
    write(k+1=N2),tab(1),
    factorize(N2,List),
    write(p=List),tab(2),
    shuffle3(L,300,L).



/*bigshf3 を連続して実行する*/
b3(K) :-for(1=<K,N),tab(2),
    bigshf3(N),nl,fail.
b3(K).

*******************************************************************************************
<補足>

/*2 分シャフリング*/
shf([]+[]=[]).
shf([X|B]+[Y|A] = [X,Y|M]) :- shf(B+A=M).

shuffle(L=M) :- half(L=A+B),shf(B+A=M).
```

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

bigshf(N) :- genlist(1,N,L),
shuffle(L,30).


/*因数分解*/
factor(P/2):- Q is P//2,P  =:= 2*Q,!.
factor(P/I):- P1 is floor(sqrt(P)),
    for(1 =< P1,J),
    J1 is 2*J+1,
       Q is P//J1,
        P =:= J1*Q,I= J1,!.
     factor(P/P) :-!.


factorize(P,[P]):-factor(P/X),X==P,!.
factorize(P,List):- factor(P/I),
    P1 is P//I,
    List=[I|List1],
    factorize(P1,List1),!.


/*繰り返し*/
for(I =<J,I) :- I =<J.
for(I =<J,K) :- I =<J,
    I1 is I+1,for(I1 =<J,K).

/*リストの定義*/
genlist(A,Z,[]) :- A>Z,!.
genlist(A,Z,[A|List]) :- A1 is A+1,
    genlist(A1,Z,List).
```

****

3　結果

3.1　結果 1

・N = 9 の時
[1, 2, 3, 4, 5, 6, 7, 8, 9]

表 4:

7	4	1
8	5	2
9	6	3

表の 1 段目,2 段目,…と並べていく。
[7, 4, 1, 8, 6, 2, 9, 6, 3]

これを繰り返していく。
[9, 8, 7, 6, 5, 4, 3, 2, 1] ← このときを逆転と言う
[3, 6, 9, 2, 5, 8, 1, 4, 7]
[1, 2, 3, 4, 5, 6, 7, 8, 9] ← 元に戻った

逆転が起きた場合同じ回数繰り返すと元に戻る。
逆転せずにもとに戻る場合もある。
例
・N = 12 の時
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
[9, 5, 1, 10, 6, 2, 11, 7, 3, 12, 8, 4]
[3, 6, 9, 12, 2, 5, 8, 11, 1, 4, 7, 10]
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

3.2　結果 2(Prolog による結果)

N = 9 の時 10 回シャフリングした時の結果

```
?-shuffle12([1,2,3,4,5,6,7,8,9],10).
[1, 2, 3, 4, 5, 6, 7, 8, 9]
[7, 4, 1, 8, 5, 2, 9, 6, 3]
[9, 8, 7, 6, 5, 4, 3, 2, 1]
[3, 6, 9, 2, 5, 8, 1, 4, 7]
[1, 2, 3, 4, 5, 6, 7, 8, 9] ← 4 回で元に戻った
[7, 4, 1, 8, 5, 2, 9, 6, 3] ←後は繰り返し
```

```
[9, 8, 7, 6, 5, 4, 3, 2, 1]
[3, 6, 9, 2, 5, 8, 1, 4, 7]
[1, 2, 3, 4, 5, 6, 7, 8, 9]
[7, 4, 1, 8, 5, 2, 9, 6, 3]
[9, 8, 7, 6, 5, 4, 3, 2, 1]

Yes
```

****

＜補足＞

◎2分シャフリング

・16枚のカードを8回シャフリングした結果

```
?- shuffle([1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16],8).
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]
[9, 1, 10, 2, 11, 3, 12, 4, 13, 5, 14, 6, 15, 7, 16, 8]
[13, 9, 5, 1, 14, 10, 6, 2, 15, 11, 7, 3, 16, 12, 8, 4]
[15, 13, 11, 9, 7, 5, 3, 1, 16, 14, 12, 10, 8, 6, 4, 2]
[16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1]
[8, 16, 7, 15, 6, 14, 5, 13, 4, 12, 3, 11, 2, 10, 1, 9]
[4, 8, 12, 16, 3, 7, 11, 15, 2, 6, 10, 14, 1, 5, 9, 13]
[2, 4, 6, 8, 10, 12, 14, 16, 1, 3, 5, 7, 9, 11, 13, 15]
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]

Yes
```

・10枚のカードを30回シャフリングした時の結果

```
?- bigshf(10).
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]
[6, 1, 7, 2, 8, 3, 9, 4, 10, 5]
[3, 6, 9, 1, 4, 7, 10, 2, 5, 8]
[7, 3, 10, 6, 2, 9, 5, 1, 8, 4]
[9, 7, 5, 3, 1, 10, 8, 6, 4, 2]
[10, 9, 8, 7, 6, 5, 4, 3, 2, 1]
[5, 10, 4, 9, 3, 8, 2, 7, 1, 6]
[8, 5, 2, 10, 7, 4, 1, 9, 6, 3]
[4, 8, 1, 5, 9, 2, 6, 10, 3, 7]
[2, 4, 6, 8, 10, 1, 3, 5, 7, 9]
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]
[6, 1, 7, 2, 8, 3, 9, 4, 10, 5]
```

```
[3, 6, 9, 1, 4, 7, 10, 2, 5, 8]
[7, 3, 10, 6, 2, 9, 5, 1, 8, 4]
[9, 7, 5, 3, 1, 10, 8, 6, 4, 2]
[10, 9, 8, 7, 6, 5, 4, 3, 2, 1]
[5, 10, 4, 9, 3, 8, 2, 7, 1, 6]
[8, 5, 2, 10, 7, 4, 1, 9, 6, 3]
[4, 8, 1, 5, 9, 2, 6, 10, 3, 7]
[2, 4, 6, 8, 10, 1, 3, 5, 7, 9]
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]
[6, 1, 7, 2, 8, 3, 9, 4, 10, 5]
[3, 6, 9, 1, 4, 7, 10, 2, 5, 8]
[7, 3, 10, 6, 2, 9, 5, 1, 8, 4]
[9, 7, 5, 3, 1, 10, 8, 6, 4, 2]
[10, 9, 8, 7, 6, 5, 4, 3, 2, 1]
[5, 10, 4, 9, 3, 8, 2, 7, 1, 6]
[8, 5, 2, 10, 7, 4, 1, 9, 6, 3]
[4, 8, 1, 5, 9, 2, 6, 10, 3, 7]
[2, 4, 6, 8, 10, 1, 3, 5, 7, 9]
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

Yes
**********************************************************************************************
```

また、シャフリングをして元の順番に戻るまでの回数を周期 m と呼ぶ。

bigshf3 より周期が次のように求められる。(N = 3n,k = N,p = k + 1 の素因数分解,m = 周期)

N = 30 の時

```
?- bigshf3(10).
  n=10 k=30 k+1=31 p=[31]  m=30
Yes
```

N + 1 が 31 でそのオイラー関数の値は 30。周期は一般にオイラー関数の約数であり、この場合ちょうど 30 になった。

次に 3 枚から 150 枚までの周期を求めた。
その結果は次の通りである。
ただし、枚数を k とし、k + 1 を素因数分解してできた素因数を p = リストの形で表記し
周期を m = の次に書く。

N = 50 の時

```
?- b3(50).
  n=1 k=3 k+1=4 p=[2, 2]  m=2
  n=2 k=6 k+1=7 p=[7]  m=6
  n=3 k=9 k+1=10 p=[2, 5]  m=4
  n=4 k=12 k+1=13 p=[13]  m=3
  n=5 k=15 k+1=16 p=[2, 2, 2, 2]  m=4
  n=6 k=18 k+1=19 p=[19]  m=18
  n=7 k=21 k+1=22 p=[2, 11]  m=5
  n=8 k=24 k+1=25 p=[5, 5]  m=20
  n=9 k=27 k+1=28 p=[2, 2, 7]  m=6
  n=10 k=30 k+1=31 p=[31]  m=30
  n=11 k=33 k+1=34 p=[2, 17]  m=16
  n=12 k=36 k+1=37 p=[37]  m=18
  n=13 k=39 k+1=40 p=[2, 2, 2, 5]  m=4
  n=14 k=42 k+1=43 p=[43]  m=42
  n=15 k=45 k+1=46 p=[2, 23]  m=11
  n=16 k=48 k+1=49 p=[7, 7]  m=42
  n=17 k=51 k+1=52 p=[2, 2, 13]  m=6
  n=18 k=54 k+1=55 p=[5, 11]  m=20
  n=19 k=57 k+1=58 p=[2, 29]  m=28
  n=20 k=60 k+1=61 p=[61]  m=10
  n=21 k=63 k+1=64 p=[2, 2, 2, 2, 2, 2]  m=16
  n=22 k=66 k+1=67 p=[67]  m=22
  n=23 k=69 k+1=70 p=[2, 5, 7]  m=12
  n=24 k=72 k+1=73 p=[73]  m=12
  n=25 k=75 k+1=76 p=[2, 2, 19]  m=18
  n=26 k=78 k+1=79 p=[79]  m=78
  n=27 k=81 k+1=82 p=[2, 41]  m=8
  n=28 k=84 k+1=85 p=[5, 17]  m=16
  n=29 k=87 k+1=88 p=[2, 2, 2, 11]  m=10
  n=30 k=90 k+1=91 p=[7, 13]  m=6
  n=31 k=93 k+1=94 p=[2, 47]  m=23
  n=32 k=96 k+1=97 p=[97]  m=48
  n=33 k=99 k+1=100 p=[2, 2, 5, 5]  m=20
  n=34 k=102 k+1=103 p=[103]  m=34
  n=35 k=105 k+1=106 p=[2, 53]  m=52
  n=36 k=108 k+1=109 p=[109]  m=27
  n=37 k=111 k+1=112 p=[2, 2, 2, 2, 7]  m=12
  n=38 k=114 k+1=115 p=[5, 23]  m=44
  n=39 k=117 k+1=118 p=[2, 59]  m=29
```

```
  n=40 k=120 k+1=121 p=[11, 11]  m=5
  n=41 k=123 k+1=124 p=[2, 2, 31]  m=30
  n=42 k=126 k+1=127 p=[127]  m=126
  n=43 k=129 k+1=130 p=[2, 5, 13]  m=12
  n=44 k=132 k+1=133 p=[7, 19]  m=18
  n=45 k=135 k+1=136 p=[2, 2, 2, 17]  m=16
  n=46 k=138 k+1=139 p=[139]  m=138
  n=47 k=141 k+1=142 p=[2, 71]  m=35
  n=48 k=144 k+1=145 p=[5, 29]  m=28
  n=49 k=147 k+1=148 p=[2, 2, 37]  m=18
  n=50 k=150 k+1=151 p=[151]  m=50

Yes
```

この結果を表に表わす。

表 5: 枚数と周期の関係

n	枚数 N	枚数+1	因数分解	周期	枚数-周期	周期/枚数	枚数+1 の差	周期の差	逆転
2	6	7	[7]	6	0	1	12	12	○
6	18	19	[19]	18	0	1	12	12	○
10	30	31	[31]	30	0	1	12	12	○
14	42	43	[43]	42	0	1	36	36	○
26	78	79	[79]	78	0	1	48	48	○
42	126	127	[127]	126	0	1	12	12	○
46	138	139	[139]	138	0	1	-	-	○
16	48	49	[7, 7]	42	6	0.88	-	-	○
8	24	25	[5, 5]	20	4	0.83	-	-	○
1	3	4	[2, 2]	2	1	0.67	-	-	○
12	36	37	[37]	18	18	0.5	-	-	○
32	96	97	[97]	48	48	0.5	-	-	○
35	105	106	[2, 53]	52	53	0.5	-	-	○
19	57	58	[2, 29]	28	29	0.49	-	-	○
11	33	34	[2, 17]	16	17	0.48	-	-	○
3	9	10	[2, 5]	4	5	0.44	-	-	○
38	114	115	[5, 23]	44	70	0.39	-	-	×
18	54	55	[5, 11]	20	34	0.37	-	-	×
22	66	67	[67]	22	44	0.33	-	-	○
34	102	103	[103]	34	68	0.33	-	-	○
50	150	151	[151]	50	100	0.33	-	-	○
5	15	16	[2, 2, 2, 2]	4	11	0.27	-	-	×
4	12	13	[13]	3	9	0.25	-	-	×
21	63	64	[2,2,2,2,2,2]	16	47	0.25	-	-	×
31	93	94	[2, 47]	23	70	0.25	-	-	×
36	108	109	[109]	27	81	0.25	-	-	×
39	117	118	[2, 59]	29	88	0.25	-	-	×
47	141	142	[2, 71]	35	106	0.25	-	-	×
7	21	22	[2, 11]	5	16	0.24	-	-	×
15	45	46	[2, 23]	11	34	0.24	-	-	×
41	123	124	[2, 2, 31]	30	93	0.24	-	-	○
25	75	76	[2, 2, 19]	18	57	0.24	-	-	×
9	27	28	[2, 2, 7]	6	21	0.22	-	-	○

n	枚数 N	枚数+1	因数分解	周期	枚数-周期	周期/枚数	枚数+1 の差	周期の差	逆転
33	99	100	[2, 2, 5, 5]	20	79	0.2	-	-	×
28	84	85	[5, 17]	16	68	0.19	-	-	×
48	144	145	[5, 29]	28	116	0.19	-	-	○
20	60	61	[61]	10	50	0.17	-	-	○
23	69	70	[2, 5, 7]	12	57	0.17	-	-	×
24	72	73	[73]	12	60	0.17	-	-	○
44	132	133	[7, 19]	18	114	0.14	-	-	○
17	51	52	[2, 2, 13]	6	45	0.12	-	-	×
45	135	136	[2,2,2,17]	16	119	0.12	-	-	×
49	147	148	[2, 2, 37]	18	129	0.12	-	-	○
29	87	88	[2, 2, 2, 11]	10	77	0.11	-	-	×
37	111	112	[2, 2, 2, 2, 7]	12	99	0.11	-	-	×
13	39	40	[2, 2, 2, 5]	4	35	0.1	-	-	×
27	81	82	[2, 41]	8	73	0.1	-	-	○
43	129	130	[2, 5, 13]	12	117	0.09	-	-	×
30	90	91	[7, 13]	6	84	0.07	-	-	×
40	120	121	[11, 11]	5	115	0.04	-	-	×

周期と枚数の関係についてより詳しく表にする。

表 6: 周期と枚数の関係

周期	枚数 N
2	3
3	12
4	9,15,39
5	21,120
6	6,27,51,90
8	81
10	60,87
11	45
12	69,72,111,129
16	33,63,84,135
18	18,36,75,132,147
20	24,54,99
22	66
23	93
27	108
28	57,144
29	117
30	30,123
34	102
35	141
42	42,48
44	114
48	96
50	150
52	105
78	78
126	126
138	138

4　考察

4.1　考察 1(結果 2 から分かること)

●常に周期 ≤ 枚数

●枚数=周期の時
・常に N + 1 は**素数**で、その差は 12 の倍数。
・周期同士の差も 12 の倍数。
・N = 6l と書け、l は奇数。ただし現在のところ証明されていない。
・枚数+1=素数 ≡ 7 (mod12)
・枚数+1=素数 ≡ 3 (mod4)
＜補足＞
素数は 2 を除いて、
4 で割ると余りが 1 になる数 (5,13,17,29,37,41,…)
3 になる数 (3,7,11,19,23,31,…)
の 2 種に分かれる。
ここで出てくる枚数+1 の素数はすべて 4 で割ると余りが 3 になる。

●周期が枚数より小さくなる事と、周期=枚数の時に枚数+1 が素数になる事の証明
$3^m \equiv 1 \bmod 3n + 1$
となる最小の正の数 m が周期。
A = 3n + 1 とおくと、一般に周期 m はオイラー関数 $\varphi(A)$ の約数。$A - 1$ = 3n は枚数となる。
$m \leq \varphi(A) \leq A - 1$
なので周期 ≤ 枚数となる。
$m = A - 1$ なら、$\varphi(A) = A - 1$
となり、A は素数であることが分かる。

4.2　考察 2

シャフリングした時の数の移動に着目する。

N = 6 の時
[1, 2, 3, 4, 5, 6]
↓シャフリング
[5, 3, 1, 6, 4, 2]
↓数をすべて 3 倍する。
[15, 9, 3, 18, 12, 6]
↓数を mod7 でみると
[1, 2, 3, 4, 5, 6]
となってもとの数と一致する。

＜証明＞

X : [1, 2, 3, 4, ⋯, n + 1, ⋯, 2n, 2n + 1, ⋯, 3n]

↓シャフリング

Y : [2n + 1, n + 1, 1, 2n + 2, n + 2, 2, ⋯, 3n, 2n, n]

↓ 3 倍

[6n + 3, 3n + 3, 3, 6n + 6, 3n + 6, 6, ⋯, 9n, 6n, 3n]

ここで

6n + 3 = 1 + 2(3n + 1) ≡ 1 mod 3n + 1

3n + 3 = 3n + 1 + 2 ≡ 2 mod 3n + 1

となるので、

↓それぞれの数を mod 3n + 1 でみると

[1, 2, 3, ⋯, n + 1, ⋯, 2n, 2n + 1, ⋯3n]

これで上記の法則が示された。

****

例

N = 6 の時

[1, 2, 3, 4, 5, 6]

↓ シャフリング

[5, 3, 1, 6, 4, 2] →数を 3 倍 [15, 9, 3, 18, 12, 6]

↓ → mod 7 でみる [1, 2, 3, 4, 5, 6]

[4, 1, 5, 2, 6, 3] →数を 2 倍 [8, 2, 10, 4, 12, 6]

↓ → mod 7 でみる [1, 2, 3, 4, 5, 6]

[6, 5, 4, 3, 2, 1] →数を 6 倍 [36, 30, 24, 18, 12, 6]

↓ → mod 7 でみる [1, 2, 3, 4, 5, 6]

[2, 4, 6, 1, 3, 5] →数を 4 倍 [8, 16, 24, 4, 12, 20]

↓ → mod 7 でみる [1, 2, 3, 4, 5, 6]

[3, 6, 2, 5, 1, 4] →数を 5 倍 [15, 30, 10, 25, 5, 20]

↓ → mod 7 でみる [1, 2, 3, 4, 5, 6]

[1, 2, 3, 4, 5, 6]

N = 9 の時

[1, 2, 3, 4, 5, 6, 7, 8, 9]

↓シャフリング

[7, 4, 1, 8, 5, 2, 9, 6, 3] →数を 3 倍する [21, 12, 3, 24, 15, 6, 27, 18, 9]

↓ → mod 10 でみる [1, 2, 3, 4, 5, 6, 7, 8, 9]

[9, 8, 7, 6, 5, 4, 3, 2, 1] →数を 9 倍する [81, 72, 63, 54, 45, 36, 27, 18, 9]

↓ → mod 10 でみる [1, 2, 3, 4, 5, 6, 7, 8, 9]

[3, 6, 9, 2, 5, 8, 1, 4, 7] →数を 7 倍する [21, 42, 63, 14, 35, 56, 7, 28, 49]

↓ → mod 10 でみる [1, 2, 3, 4, 5, 6, 7, 8, 9]

[1, 2, 3, 4, 5, 6, 7, 8, 9]

N = 12 の時

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

↓シャフリング

[9, 5, 1, 10, 6, 2, 11, 7, 3, 12, 8, 4] →数を 3 倍 [27, 15, 3, 30, 18, 6, 33, 21, 9, 36, 24, 12]

↓ → mod 13 でみる [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

[3, 6, 9, 12, 2, 5, 8, 11, 1, 4, 7, 10] →数を 9 倍 [27, 54, 81, 108, 18, 45, 72, 99, 9, 36, 63, 90]

↓ → mod 13 でみる [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

****

◎この事を 2 **分シャフリング**についても考える。

例

N = 6 の時

[1, 2, 3, 4, 5, 6]

↓シャフリング

[4, 1, 5, 2, 6, 3] →数を 2 倍 [8, 2, 10, 4, 12, 6] → mod 7 でみる [1, 2, 3, 4, 5, 6]

↓

[2, 4, 6, 1, 3, 5] →数を 4 倍 [8, 16, 24, 4, 12, 20] → mod 7 でみる [1, 2, 3, 4, 5, 6]

↓

[1, 2, 3, 4, 5, 6]

N = 12 の時

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

↓シャフリング

[7, 1, 8, 2, 9, 3, 10, 4, 11, 5, 12, 6] → 数を 2 倍 [14, 2, 16, 4, 18, 6, 20, 8, 22, 10, 24, 12]

↓ → mod 13 でみる [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

[10, 7, 4, 1, 11, 8, 5, 2, 12, 9, 6, 3] →数を 4 倍
[5, 10, 2, 7, 12, 4, 9, 1, 6, 11, 3, 8] →数を 8 倍
[9, 5, 1, 10, 6, 2, 11, 7, 3, 12, 8, 4] → 3 倍
[11, 9, 7, 5, 3, 1, 12, 10, 8, 6, 4, 2] → 6 倍
[12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1] → 12 倍 → mod 13 でみる [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
[6, 12, 5, 11, 4, 10, 3, 9, 2, 8, 1, 7] → 11 倍
[3, 6, 9, 12, 2, 5, 8, 11, 1, 4, 7, 10] → 9 倍
[8, 3, 11, 6, 1, 9, 4, 12, 7, 2, 10, 5] → 5 倍
[4, 8, 12, 3, 7, 11, 2, 6, 10, 1, 5, 9] → 10 倍
[2, 4, 6, 8, 10, 12, 1, 3, 5, 7, 9, 11] →数を 7 倍
↓シャフリング
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]

＜証明＞
X : [1, 2, 3, 4, ⋯, n + 1, ⋯, 2n]
↓シャフリング
Y : [n + 1, 1, n + 2, 2, ⋯, 2n, n]
↓ 2 倍
[2n + 2, 2, 2n + 4, 4, ⋯, 4n, 2n]
↓
ここで
2n + 2 = 2n + 1 + 1 ≡ 1 mod 2n + 1
2n + 4 = 2n + 1 + 3 ≡ 3 mod 2n + 1
となるので、
↓それぞれの数を mod 2n + 1 でみると
[1, 2, 3, 4, ⋯, 2n]

これで上記の法則が 2 分シャフリングの場合でも示された。

◎ 4 **分シャフリング**の場合

N = 8 の時
[1, 2, 3, 4, 5, 6, 7, 8]
↓シャフリング
[7, 5, 3, 1, 8, 6, 4, 2] →数を 4 倍 [28, 20, 12, 4, 32, 24, 16, 8] → mod 9 でみる [1, 2, 3, 4, 5, 6, 7, 8]
↓
[4, 8, 3, 5, 2, 6, 1, 7] →数を 7 倍 [28, 56, 21, 35, 14, 42, 7, 49] → mod 9 でみる [1, 2, 3, 4, 5, 6, 7, 8]
↓
[1, 2, 3, 4, 5, 6, 7, 8]

＜証明＞

X : [1, 2, 3, 4, $\cdots n, n+1, \cdots, 2n, 2n+1, \cdots, 3n, 3n+1, \cdots, 4n$]

↓シャフリング

Y : [$3n+1, 2n+1, n+1, 1 \cdots, 4n, 3n, 2n, n$]

↓ 4 倍

[$12n+4, 8n+4, 4n+4, 4, \cdots, 16n, 12n, 8n, 4n$]

↓

ここで

$12n + 4 = (4n + 1)3 + 1 \equiv 1 \mod 4n + 1$

$8n + 4 = (4n + 1)2 + 2 \equiv 2 \mod 4n + 1$

$4n + 4 = (4n + 1) + 3 \equiv 3 \mod 4n + 1$

$8n = (4n + 1)2 - 2 \equiv 4n - 1 \mod 4n + 1$

$4n = (4n + 1) - 1 \equiv 4n \mod 4n + 1$

となるので、

↓それぞれの数を mod $4n + 1$ でみると

[$1, 2, 3, 4, \cdots, 4n - 1, 4n$]

これで上記の法則が 4 分シャフリングの場合でも示された。

****

・以上から分かること

1. N 枚を使って 3 分シャフリングを 1 回した場合、左から X 番目にでた数 Y を 3 倍した $3Y$ を mod $N + 1$ で考えると元の数 X に戻る。

2. X から Y を求める方法は次の通り

   $3Y \equiv X \mod N + 1$

   $Y \equiv 1/3X \mod N + 1$

   $3n + 1 = p \equiv 0 \mod N + 1$

   $3n \equiv -1 \mod N + 1$

   $1/3 \equiv -n \mod N + 1$

   $Y \equiv -nX \mod N + 1$

   X を $-n$ 倍し mod $N + 1$ をとると Y が求まる。

＜2 分シャフリングの場合＞

$2Y \equiv X \mod N+1$
$Y \equiv 1/2X \mod N+1$

$2n+1 = p \equiv 0 \mod N+1$
$2n \equiv -1 \mod N+1$
$1/2 \equiv -n \mod N+1$

$Y \equiv -nX \mod N+1$

よって 2 分シャフリングの場合も 3 分シャフリングの時と同じことが言えた。

＜4 分シャフリングの場合＞

$4Y \equiv X \mod N+1$
$Y \equiv 1/4X \mod N+1$

$4n+1 = p \equiv 0 \mod N+1$
$4n \equiv -1 \mod N+1$
$1/4 \equiv -n \mod N+1$

$Y \equiv -nX \mod N+1$

よって 4 分シャフリングの場合も同じことが言えた。

5 終わりに

5.1 感想

このゼミが始まった頃は、卒論など本当に完成させることが出来るのだろうかと不安で一杯でした。しかし、飯高先生やゼミの皆のお陰でこんな私でも何とかまとめる事ができました。とても感謝しています。ありがとうございました。

参考文献

[1] NUMBER THEORY Gerge E.Andrews

[2] 日本語 LATEX2 ε ブック　　中野 賢　著　アスキー出版局