シャッフル

金沢光則

平成 14 年 7 月 7 日

1　出自

2003 年度入試で，東大理科前期に次の問題が出た。

問題

N を正の整数とする。2N 個の項からなる数列

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

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 } に戻ることを証明せよ。

数学の泉 ML で，この問題の一般化についての話題が扱われた。何かに，群論を知っていればこの問題はすぐ分かると書いてあったように思う。そこで，少し考えてみた。

1.1　解答

まず，解答をしよう。

(1) { 1,2,3,4,5,6,7,8 } → { 5,1,6,2,7,3,8,4 } → { 7,5,3,1,8,6,4,2 } → { 8,7,6,5,4,3,2,1 }
最後のものが 3 回シャッフルして得られたものである。
(2) { 1,2,$\cdots$,N,$N+1$,$N+2$,$\cdots$,$2N$} → { $N+1$,1,$N+2$,2,$\cdots$,$2N$,N } だから，
$f(1) = 2$, $f(2) = 4$, $f(3) = 6$, $\cdots$, $f(i) = 2i$, $\cdots$, $f(N) = 2N$, $f(N+1) = 1$, $f(N+2) = 3$, $f(N+3) = 5$, $\cdots$, $f(N+j) = 2j - 1$, $\cdots$, $f(2N) = 2N - 1$
となる。よって，
$1 \leqq k \leqq N$ のとき，$f(k) - 2k = 0$,　$N + 1 \leqq k \leqq 2N$ のとき，$f(k) - 2k = -2N - 1$

となり，いずれの場合でも $2N+1$ で割り切れる。

(3) 数列 $\{1,2,\cdots,2N\}$ を $2n$ 回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 $f^{2n}(k)$ で表すと，$f(k) \equiv 2k (\mathrm{mod} 2N+1)$ ゆえ，

$f^{2n}(k) = \overbrace{f(f(\cdots f}^{2n}(k)\cdots) \equiv 2^{2n}k \ (\mathrm{mod} 2N+1) \equiv \{2^n\}^2 k \equiv \{2N\}^2 k \equiv \{-1\}^2 k \equiv k \ (\mathrm{mod} 2N+1)$

$f^{2n}(k)$ も k も 1,2,$\cdots$, $2N$ のいずれかなので，この合同は実際には等号となり証明が完了する。

2 一般には

N を 2 のベキに制限しない場合に調べて ML に流した方がいた。そのデータは次の通りである。

N	戻るまでの回数
10	6
11	11
12	20
13	18
14	28
15	5
16	10
17	12
18	36
19	12
20	20

さらに，奇数回で戻ることが少ないこと，いずれの場合も $2N$ 回までに戻ることに注意され，後者については一般に成り立つのではないかと予想されていた。

2.1 一般に戻る回数

$f^m(k) \equiv 2^m k \ (\mathrm{mod} 2N+1)$ ゆえ，m 回で戻るのは，$2^m k \equiv k \ (\mathrm{mod} 2N+1) \ \forall k$ が成り立つときである。これは，$2^m \equiv 1 \ (\mathrm{mod} 2N+1)$ と同値である。

ところで，2 で生成される乗法群は $\mathbb{Z}_{2N+1}$ の単数群 (既約剰余類群) の部分群であり，上記の m のうち最小の自然数は，この乗法群の位数である。したがって ${\mathbb{Z}_{2N+1}}^{\times}$ の位数の約数で，$2N+1$ より小さい。

このことから，最大でも $2N$ 回で元に戻ることが分かる。

2.2 奇数回で戻る場合は無限にあるか

${\mathbb{Z}_{2^m-1}}^{\times} \ni 2$ について，$2^m \equiv 1 \ (\mathrm{mod} 2N+1)$ が成り立つが，$2^k \equiv 1$ となる最小の自然数は m の約数となるので，m が奇数なら k も奇数である。

したがって，$2^m - 1 = 2N+1$ となる奇数 m $(N = 2^{m-1}-1)$ をとればよい。

2.3 特に早く戻る場合

$N = 15$ のときは，他の場合と比べて特に早く戻ってくるように見える。このような場合はどういうときに起こるのだろう。

前節と同じに $2^m-1=2N+1$ とすると，m 回で戻るが，$2^k-1<2N+1$ $(k<m)$ なので，m 回以前には戻らない。この状況を表にまとめよう。

m	N	数列	単数群	位数	戻る回数
3	3	$1,2,\cdots,6$	${\mathbb{Z}_7}^\times$	6	3
4	7	$1,2,\cdots,14$	${\mathbb{Z}_{15}}^\times$	8	4
5	15	$1,2,\cdots,30$	${\mathbb{Z}_{31}}^\times$	30	5
6	31	$1,2,\cdots,62$	${\mathbb{Z}_{63}}^\times$	36	6
7	63	$1,2,\cdots,126$	${\mathbb{Z}_{127}}^\times$	126	7
8	127	$1,2,\cdots,254$	${\mathbb{Z}_{255}}^\times$	128	8
9	255	$1,2,\cdots,510$	${\mathbb{Z}_{511}}^\times$	264	9
10	511	$1,2,\cdots,1022$	${\mathbb{Z}_{1023}}^\times$	600	10
11	1023	$1,2,\cdots,2046$	${\mathbb{Z}_{2047}}^\times$	2046	11
12	2047	$1,2,\cdots,4094$	${\mathbb{Z}_{4095}}^\times$	1728	12

2.4 戻る回数と N の関係

m 回で戻るとすると，$2^m\equiv 1\ (\mathrm{mod}2N+1)$ だから，$2^m-1\geqq 2N+1$ である。
よって $\log_2(N-1)+1\leqq m\leqq 2N$ となる。

3 特に遅く戻る場合

${}^\#{\mathbb{Z}_{2N+1}}^\times=2N$ となるのは，$2N+1=p$ が素数のときである。このとき $2^k\not\equiv 1$ $(k=1,2,\cdots,N)$ となれば $2N$ 回で初めて戻ることになる。$\mathbb{Z}_p$ は整域ゆえ $2^N\equiv -1\ (\mathrm{mod}p)$ となればよい。

N	$2N+1$	$2^N\equiv$	N	$2N+1$	2^N	N	$2N+1$	2^N	N	$2N+1$	2^N
1	3	-1	17	$35=5\cdot 7$	—	33	67	-1	49	$99=3^2\cdot 11$	—
2	5	-1	18	37	-1	34	$69=3\cdot 23$	—	50	101	-1
3	7	1	19	$39=3\cdot 13$	—	35	71	1	51	103	1
4	$9=3^2$	—	20	41	1	36	73	1	52	$105=3\cdot 5\cdot 7$	—
5	11	-1	21	43	-1	37	$75=3\cdot 5^2$	—	53	107	-1
6	13	-1	22	$45=3^2\cdot 5$	—	38	$77=7\cdot 11$	—	54	109	-1
7	$15=3\cdot 5$	—	23	47	1	39	79	1	55	$111=3\cdot 37$	—
8	17	1	24	$49=7^2$	—	40	$81=3^4$	—	56	113	1
9	19	-1	25	$51=3\cdot 17$	—	41	83	-1	57	$115=5\cdot 23$	—
10	$21=3\cdot 7$	—	26	53	-1	42	$85=5\cdot 17$	—	58	$117=3^2\cdot 13$	—
11	23	1	27	$55=5\cdot 11$	—	43	$87=3\cdot 29$	—	59	$119=7\cdot 17$	—
12	$25=5^2$	—	28	$57=3\cdot 19$	—	44	89	1	60	$121=11^2$	—
13	$27=3^3$	—	29	59	-1	45	$91=7\cdot 13$	—	61	$123=3\cdot 41$	—
14	29	-1	30	61	-1	46	$93=3\cdot 31$	—	62	$125=5^3$	—
15	31	1	31	$63=3^2\cdot 7$	—	47	$95=3^2\cdot 5$	—	63	127	1
16	$33=3\cdot 11$	—	32	$65=5\cdot 13$	—	48	97	1	64	$129=3\cdot 43$	—

この表から，$p=2N+1$ が素数のとき，1 と -1 が 2 つずつ繰り返されるように見える。
2 が ${\mathbb{Z}_{\text{ı}}}^\times$ で平方剰余 $\iff \left(\dfrac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=1 \iff p\equiv\pm 1\ (\mathrm{mod}\ 8)$
表と比べると，「$2^N\equiv -1 \iff$ 2 は平方非剰余」に見える。

3.1 平方非剰余との関係

アーベル群の基本定理から，$\mathbb{Z}_l{}^{\times}$ は巡回群である。
2 が生成元なら $2^N \not\equiv 1$ だから $2N$ 回で初めて元に戻る。
2 が生成元でないとき，存在する生成元を $a(>1)$ とする。
$a^N \equiv -1$ となる。また，$a^l \equiv 2\ (l>1)$ とおく。
ここで 2 が平方非剰余なら l は奇数となる。
$l = 2l'+1$ とおくと，$2^N \equiv (a^l)^N \equiv a^{Nl} \equiv a^{2l'N+N} \equiv (a^N)^{2l'} \cdot a^N \equiv (-1)^{2l'} \cdot (-1) \equiv -1$
2 が平方剰余なら l は偶数としてよい。$l = 2l'$ とおくと，$2^N \equiv (a^l)^N \equiv a^{Nl} \equiv a^{2l'N} \equiv (a^N)^{2l'} \equiv (-1)^{2l'} \equiv 1$
以上から，
$p = 2N+1$ が素数のとき，シャッフルが $2N$ 回で初めて戻る $\iff p \equiv 3,5\ (\mathrm{mod}8)$
となることが分かる。この条件を満たす素数は無数にあるから，戻る回数が最大となる場合も無数にあることが分かる。

参考文献

[1] 足立恒雄, 類体論へ至る道, 日本評論社

[2] 木田祐司・牧野潔夫, Ubasic によるコンピュータ整数論, 日本評論社