広がる数学 VI

– 第 15 回 JST 数学キャラバン –

カードのシャフルと合同式

鈴木武史 (岡山大学理学部数学科)

1　数学クイズ：囚人の試練

4人の囚人の1人ひとりの額に0,1,2,3の数字のどれか(例えば, 全員が2でもよい)がペンキで書かれる. あらかじめ決められた時刻に他の3人の数字はいっせいに見えるようになり, その後, 1人ひとり隔離され, 自分の数字を当てるようにいわれる.

少なくとも1人の囚人が正解できれば, 全員に恩赦が与えられ釈放される. 囚人達には事前にこのゲームのルールが知らされ, 作戦を立てる機会が与えられている. 囚人達が100%釈放されるような作戦を考えよ.

(答) 事前に, 囚人達に0,1,2,3の数字を重複のないように割り当てておく. 数字kを担当する囚人は, 4人の額の数字の合計が「4で割るとkあまる数である」と仮定して自分の数字を答える.
(各囚人の答えるべき数字は, それぞれただ一つ定まり, かつ, 4人のうち1人は正しい数字を担当し, 正解する.)

2　合同式 ～割った余りに注目～

自然数nをひとつ固定する.

整数a, bに対して, $a-b$がnの倍数であるとき

$$a \equiv b \mod n$$

と書きaはbとnを法として合同であると言う.

言い換えると,「aをn で割った余り」と「bをn で割った余り」が等しいということ.

例. $1 \equiv 5 \mod 4, \quad 13 \equiv -3 \mod 4$

3　合同式の性質

以下, n を固定し, $a \equiv b \mod n$ を単に $a \equiv b$ とも書く.

性質 1. (1) $a = b \Rightarrow a \equiv b$

(2) $a \equiv b \Leftrightarrow b \equiv a$

(3) $a \equiv b,\ b \equiv c \Rightarrow a \equiv c$

性質 2. どんな整数 a に対しても

$$a \equiv b \mod n \text{ かつ } 0 \leqq b \leqq n-1$$

なる整数 b ($= a$ を n で割った余り) がただ一つ定まる.

性質 3. $a \equiv a'$, $b \equiv b'$ のとき

(1) $a \pm b \equiv a' \pm b'$

(2) $ab \equiv a'b'$

(3) $a^m \equiv (a')^m$ $(m$: 自然数$)$

(証明) $a \equiv a'$, $b \equiv b'$ なので, ある整数 k, l により

$a' = a + kn,\ b' = b + ln$ と書ける.

(1) $a' + b' = (a + kn) + (b + ln) = a + b + (k + l)n$

$\equiv a + b$

(2) $a'b' = (a + kn)(b + ln) = ab + aln + bkn + kln^2$

$\equiv ab$

4　合同式の応用

例題 1. 7^{100} の1の位を求めよ.

(解) 1の位＝10で割った余り. 従って,

$7^{100} \equiv a \mod 10$ なる $0 \leqq a \leqq 9$ を求めればよい.

$7^{100} = (7^2)^{50} = 49^{50} \equiv (-1)^{50} = 1 \mod 10$

により 7^{100} の1の位は1.

∗計算の途中で大きな数が出てきたら, より小さな合同な数で置き換えることで計算が簡単になる.

(別解) $7^1 = 7,\ 7^2 = 49,\ 7^3 = 343,\ 7^4 = 2401,$

$7^5 = 16807$ と周期性に注目しても良い.

例題 2. 17^{15} を 14 で割った余りを求めよ.

(解) 以下により, 余りは13：

$$17^{15} \equiv 3^{15} = (3^3)^5 = 27^5 \equiv (-1)^5 \equiv 13 \mod 14$$

例題 3. aが9の倍数であることと, aの各位の数の総和が9の倍数であることは同値であることを示せ.

(例) 846は$8+4+6=18$なので9の倍数.

(解) $a = c_n 10^n + \cdots + c_1 10 + c_0 \quad (0 \leqq c_i \leqq 9)$ に対して,

aが9の倍数$\Leftrightarrow \ a \equiv 0 \mod 9$

$\Leftrightarrow \ c_n 10^n + \cdots + c_1 10 + c_0 \equiv 0 \mod 9$

$\Leftrightarrow \ c_n (1)^n + \cdots + c_1 1 + c_0 \equiv 0 \mod 9$

$\Leftrightarrow$ aの各位の数の総和が9の倍数

5　カードのシャフル

シャフル＝カードの並び替え

(N 枚のカードのシャフルは全部で $N!$ 通り)

リフルシャフル（ファローシャフル）：

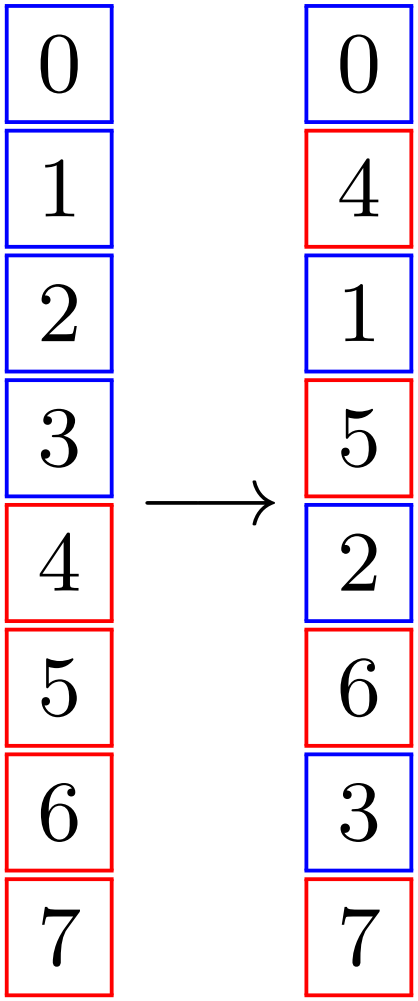
・$N = 2m$ 枚のカードを m 枚ずつ上下2組に分け,

1枚ずつ互い違いに組み合わせる.

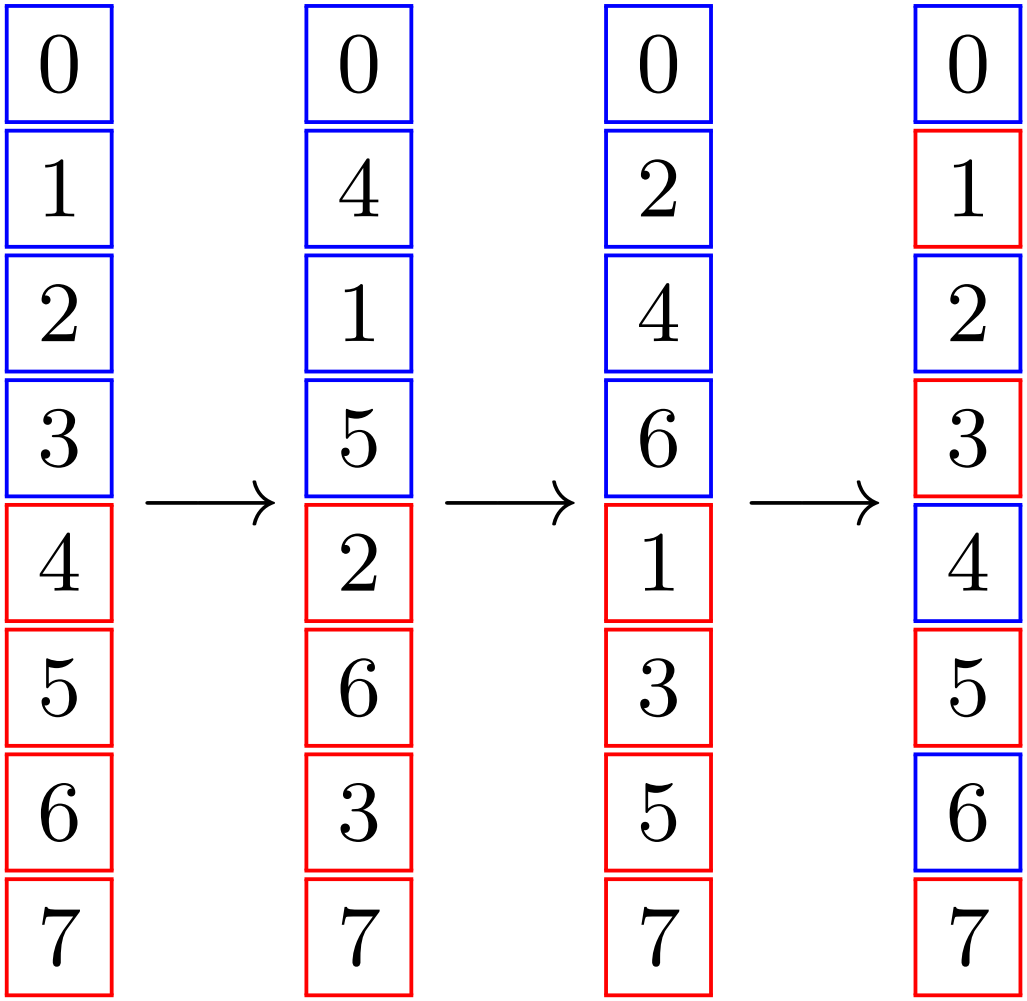
・その際「上の組を上」にして組む.

・　「完璧な」シャフルを考える.

例. N=8 枚のカードが上から 0,1,2,3,4,5,6,7 と並んでいるとする. リフルシャフルを繰り返すと：



例. N=8 枚のカードが上から 0,1,2,3,4,5,6,7 と並んでいるとする. リフルシャフルを繰り返すと：



3 回で元に戻った!

6　シャフルの周期

8枚のカードにリフルシャフルを3回繰り返すとカードの並びが元に戻った.

実は, どんなシャフルも (正確に) 何回か繰り返すとカードの並びが元に戻る.

はじめて元に戻るときの繰り返しの回数をシャフルの周期と呼ぶ.

[リフルシャフルの周期]

$N = 4$枚 $\Rightarrow$ 2回で戻る：$01|23 \to 02|13 \to 01|23$

$N = 6$枚 $\Rightarrow$ 4回で戻る：$012|345 \to 031|425 \to$

$043|215 \to 024|135 \to 012|345$

$N = 8$枚 $\Rightarrow$ 3回で戻る

$N = 10$枚 $\Rightarrow$ 6回で戻る：$01234|56789 \to$

$05162|73849 \to 07531|86429 \to 08765|43219 \to$

$04837|26159 \to 02468|13579 \to 0123456789$

$\cdots$

$N = 52$枚 (1組のトランプ) $\Rightarrow$ 8回で戻る

$N = 54$枚 $\Rightarrow$ 52回で戻る

問題

・カードの枚数 N と, 並びが元に戻るまでのリフルシャフルの回数(周期) L の関係. (N から L を簡単に計算できるか？)

・他のシャフルの場合？

[式で表す] リフルシャフルによってk番目のカードが$F(k)$番目に移るとする. (1番上を「0番目」と呼ぶ.)

例. $N = 8$:

$$
\begin{array}{ccc}
0 & 0 & F(0) = 0 \\
1 & 4 & F(1) = 2 \\
2 & 1 & F(2) = 4 \\
3 & 5 & F(3) = 6 \\
4 & 2 & F(4) = 1 \\
5 & 6 & F(5) = 3 \\
6 & 3 & F(6) = 5 \\
7 & 7 & F(7) = 7
\end{array}
\qquad
\begin{array}{c}
\longrightarrow \\
\\
\\
\\
\\
\\
\\
\\
\end{array}
\qquad
\Rightarrow
$$

$$
F(k) = \begin{cases} 2k & (k \leqq 3) \\ 2k - 7 & (4 \leqq k) \end{cases}
$$

7　合同式で捉える

一般に, $N = 2m$ 枚のとき

$$F(k) = \begin{cases} 2k & (0 \leqq k \leqq m-1) \\ 2k-(N-1) & (m \leqq k \leqq N-1) \end{cases}$$

と, 場合分けが生じるが, ここで, $N-1$ で割った余りに注目すると, 全ての k に対して

$$F(k) \equiv 2k \mod N-1$$

と, 1つの合同式で書ける.

シャフルをℓ回繰り返したときのk番目のカードの移り先$F^{\ell}(k)$について：

$$F(k) \equiv 2k \mod N-1$$

$$F^2(k) = F(F(k)) \equiv 2F(k) \equiv 2^2 k \mod N-1$$

$$F^3(k) = F(F^2(k)) \equiv 2F^2(k) \equiv 2^3 k \mod N-1$$

$\ldots$

$\ldots$

$$\boxed{F^{\ell}(k) \equiv 2^{\ell} k \mod N-1}$$

定理(リフルシャフルの周期条件)

N 枚のカードにリフルシャフルを L 回繰り返したとき, カードの並びが元に戻るための必要十分条件は：　　$2^L \equiv 1 \bmod N-1$

(証明) L 回で元に戻る

$\Leftrightarrow F^L(k) = k \quad (k = 0, 1, \ldots, N-1)$

$(k = 0, N-1$ での成立は分かっている.)

$\Leftrightarrow F^L(k) \equiv k \bmod N-1 \quad (k = 0, 1, \ldots, N-1)$

$\Leftrightarrow 2^L k \equiv k \bmod N-1 \quad (k = 0, 1, \ldots, N-1)$

$\Leftrightarrow 2^L \equiv 1 \bmod N-1$

[確認]

(1) $N = 8$: $2^1 = 2, 2^2 = 4,$

$2^3 = 8 \equiv 1 \mod 7$

$\therefore L = 3$回ではじめて戻る(周期3).

(2) $N = 52$: $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16,$

$2^5 = 32,$

$2^6 = 64 \equiv 13 \mod 51,$

$2^7 = 128 \equiv 26 \mod 51,$

$2^8 = 256 = 51 \times 5 + 1 \equiv 1 \mod 51$

$\therefore L = 8$回ではじめて戻る(周期8).

8　他のシャフル

[その1] 裏リフルシャフル(下の組が上):

(例) $N = 6$:

$$\begin{array}{cc} 0 & 3 \\ 1 & 0 \\ 2 & 4 \\ 3 & 1 \\ 4 & 5 \\ 5 & 2 \end{array} \longrightarrow \quad \Rightarrow \quad \begin{array}{l} F'(0) = 1 \\ F'(1) = 3 \\ F'(2) = 5 \\ F'(3) = 0 \\ F'(4) = 2 \\ F'(5) = 4 \end{array}$$

$$F'(k) = \begin{cases} 2k+1 \\ 2k+1-7 \end{cases}$$

一般に N 枚の場合,

$F'(k) \equiv 2k+1 \mod N+1$

定理

N 枚のカードに裏リフルシャフルを L 回繰り返すと元に戻る $\Leftrightarrow$ $2^L \equiv 1 \mod N+1$

この定理から, 一般に,

N 枚の裏リフルシャフルの周期

$=N+2$ 枚の(表)リフルシャフルの周期

(例) $N=52$ 枚のときは, 裏シャフルの周期=52.

[その2] r-リフルシャフル

$N = rm$ 枚のカードを m 枚ずつ r 組に分け, 下の例のように組みなおす.

(例) $r = 3, m = 2,\ N = 6.$

$$\begin{array}{ll} 0 & 0 \\ 1 & 2 \\ 2 & 4 \\ 3 & 1 \\ 4 & 3 \\ 5 & 5 \end{array} \quad \begin{array}{l} F_r(0) = 0 \\ F_r(1) = 3 \\ F_r(2) = 1 \\ F_r(3) = 4 \\ F_r(4) = 2 \\ F_r(5) = 5 \end{array}$$

$$\longrightarrow \quad \Rightarrow$$

$$F_r(k) = \begin{cases} 3k \\ 3k - (N-1) \\ 3k - 2(N-1) \end{cases}$$

一般に N 枚の場合,

$F_r(k) \equiv rk \mod N-1$

定理

$N = rm$ 枚のカードに r-リフルシャフルを L 回繰り返すと元に戻る $\Leftrightarrow r^L \equiv 1 \mod N-1$

(例) $r = m$ のとき, $r^2 = N \equiv 1 \mod N-1$. したがって, r^2 枚のカードに r-リフルシャフルを2回繰り返すと元に戻る.

9　関連する話題

・フェルマーの小定理 (整数論・群論)

素数pおよびpの倍数でない整数aに対して

$$a^{p-1} \equiv 1 \mod p$$

・RSA暗号

n, e, cが与えられたとき$m^e \equiv c \mod n$となるmを求める問題.

・ランダムシャフル〜確率論

52枚のカードに対する「完璧でない」リフルシャフルは, 7回くらい繰り返すとよく混ざる.

10　参考文献

[1] 群論, これはおもしろい ートランプで学ぶ群ー (数学のかんどころ 16) , 飯高 茂 (著), 共立出版

[2] 続・とっておきの数学パズル,
ピーター・ウィンクラー (著), 日本評論社