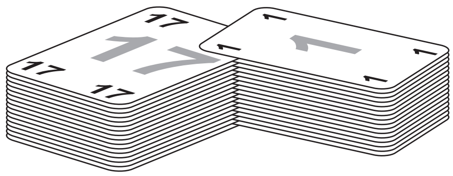
A *Matematika Határok Nélkül* ezévi versenyén szerepelt az alábbi feladat:

Szalonpóker. *Little John és Old Firehand betérnek Black Jacky híres kaszinójába egy kártyapartira. A játékhoz egy 1-től 32-ig megszámozott 32 lapos kártyacsomagot használnak. Mielőtt megbeszélnék a játékszabályokat, Black Jacky összekeveri a kártyákat az alábbi módon. Leteszi az asztalra a kártyapaklit, leveszi a fölső 16 lapot, s megfordítás nélkül a maradék pakli jobb oldalára helyezi. Ekkor úgy keveri össze a két paklit, hogy egymás után hol az egyik, hol a másik pakli egy-egy lapja kerül egymásra a bal oldali pakli alsó lapjával elkezdve a keverést* (a bal oldali pakli alsó lapja marad alul, 1. ábra). *Az így összekevert paklit összefogja, majd ugyanezt többször megismételve folytatja az eljárást. Little John biztos benne, hogy ez nem egy tisztességes keverési mód. Mutassátok meg, hogy többször megismételve az eljárást, meglepő eredmény adódik.*



1. ábra

1	1	1	1	1	1
2	17	9	5	3	2
3	2	17	9	5	3
4	18	25	13	7	4
5	3	2	17	9	5
6	19	10	21	11	6
7	4	18	25	13	7
8	20	26	29	15	8
9	5	3	2	17	9
10	21	11	6	19	10
11	6	19	10	21	11
12	22	27	14	23	12
13	7	4	18	25	13
14	23	12	22	27	14
15	8	20	26	29	15
16	24	28	30	31	16
17	9	5	3	2	17
18	25	13	7	4	18
19	10	21	11	6	19
20	26	29	15	8	20
21	11	6	19	10	21
22	27	14	23	12	22
23	12	22	27	14	23
24	28	30	31	16	24
25	13	7	4	18	25
26	29	15	8	20	26
27	14	23	12	22	27
28	30	31	16	24	28
29	15	8	20	26	29
30	31	16	24	28	30
31	16	24	28	30	31
32	32	32	32	32	32

A meglepő eredmény az, hogy ötszöri keverés után visszakapjuk a kártyalapok eredeti sorrendjét. A mellékelt táblázat hat oszlopában megadtuk, hogy az öt keverési lépés során hogyan alakul a lapok sorrendje.

Jogosan merül fel a kérdés, hogy vajon miért éppen az ötödik keverés után kapjuk vissza az eredeti sorrendet, sőt, már az sem nyilvánvaló, hogy a feladatban leírt keverési lépések ismételgetésével ilyesmire egyáltalán sor kerül. Foglalkozzunk először az utóbbi kérdéssel.

Egy keverés az $1, 2, \ldots, 32$ számok egy permutációjának tekinthető. Mivel a permutációk száma véges, előbb vagy utóbb szükségszerű az ismétlődés. A legelső ismétlődés pedig csak a lapok eredeti sorrendje lehet, mert különböző permutációkból a megadott keverés alkalmazásával különbözőket kapunk. Ezért a legelső ismétlődéskor nem kaphatunk vissza olyan permutációt, amit egy másikból már megkaptunk.

Az első kérdésre adott választ leegyszerűsíti, ha a kongruenciák nyelvén fogalmazunk.

Emlékeztetünk a jól ismert definícióra: ha $m > 1$ egész szám, akkor két egész számról azt mondjuk, hogy kongruensek modulo m, ha különbségük osztható m-mel. Jelölése:

$$a \equiv b \pmod m, \quad \text{ha} \quad m \mid a - b \quad (a,\, b,\, m \text{ egész számok}).$$

Adott m modulusra vonatkozó kongruencia reláció hasonló tulajdonságokkal rendelkezik, mint az egyenlőség, így például

$$\begin{array}{ll} a \equiv a & \text{(reflexív)} \\ a \equiv b \;\to\; b \equiv a & \text{(szimmetrikus)} \\ a \equiv b,\; b \equiv c \;\to\; a \equiv c & \text{(tranzitív)} \\ a \equiv b \;\to\; a + c \equiv b + c,\; ac \equiv bc. & \end{array}$$

Nézzük most az eredeti feladatot. A leírt keverés során a legfelső és a legalsó lap a helyén marad. A többiek nyomonkövetéséhez számozzuk át a lapokat; a felső 16 lap számozása 0-tól 15-ig, az alsó lapok számozása 16-tól 31-ig változik. Vizsgáljuk meg, hogy a k-adik helyen álló lap ($0 \le k \le 31$) egy keverés során melyik helyre kerül. Legyen ez k_1 ($0 \le k_1 \le 31$). Ha $k \le 15$, akkor a fölötte álló lapok száma k-val növekszik (az alsó részből ennyi lap kerül fölé), tehát $k_1 = 2k$. Ha $16 \le k$, akkor a mögötte álló lapok száma $(31 - k)$-val növekszik, ennyivel csökken az előtte álló lapok száma, tehát az új helyének sorszáma $k_1 = k - (31 - k) = 2k - 31$. Így két különböző képlet szerint változik a lapok helyének a sorszáma, attól függően, hogy a pakli alsó vagy felső részében van-e a kártyalap. Ha viszont a kongruenciák nyelvén fogalmazunk, akkor nem kell megkülönböztetni a két lehetőséget: egységesen $k_1 \equiv 2k \pmod{31}$. Most már ugyanígy folytathatjuk: az újabb keverés után k_1-edik helyen álló lap arra a k_2-edik helyre kerül, amelyre $k_2 \equiv 2k_1 \equiv 2^2k \pmod{31}$, és így tovább…

Az ötödik keverés után tehát a k-adik helyről arra a k_5-ödik helyre kerül a kártyalap, amelyre

$$k_5 \equiv 2^5k = 32k \equiv k \pmod{31}, \quad \text{mert} \quad 32 \equiv 1 \pmod{31}.$$

Az $1 \le k_5 \le 31$ feltétel figyelembevételével azt kapjuk, hogy $k_5 = k$, tehát az ötödik keverés után valóban minden lap visszakerül az eredeti helyére.