O małym twierdzeniu Fermata, twierdzeniu Eulera i tasowaniu kart

Jarosław WRÓBLEWSKI, Wrocław

O tasowaniu kart

Jak tasujemy karty? Można tak: bierzemy talię kart w prawą rękę i przerzucamy do lewej ręki po kilka kart, raz na wierzch, raz na spód. Jeśli karty są stare, mogą się sklejać. Dobrze jest więc wykazać przy tasowaniu nieco staranności. Można tasować z pełną pedanterią, przerzucając do lewej ręki po jednej karcie. Jak wygląda wtedy tasowanie (dla ustalenia uwagi powiedzmy, że mamy 10 kart)?

Gaspard Monge, 1746–1818

Przerzucamy do lewej ręki pierwszą kartę z wierzchu, drugą kartę wrzucamy na wierzch pierwszej, trzecią pod spód, czwartą na wierzch, piątą pod spód, ..., dziesiątą na wierzch (jest to *tasowanie Monge'a*). Jeśli przejrzymy teraz potasowane karty, zobaczymy, że ułożyły się one w następującej kolejności (patrząc od wierzchu):

$$10, 8, 6, 4, 2, 1, 3, 5, 7, 9,$$

numery odnoszą się do pozycji kart przed tasowaniem. Nie jesteśmy zadowoleni, więc tasujemy dalej dokładnie w ten sam sposób. Po kolejnych tasowaniach karty układają się następująco:

2	9	5	1	4	8	10	6	2	3	7
3	7	2	10	4	5	9	1	8	6	3
4	3	8	9	4	2	7	10	5	1	6
5	6	5	7	4	8	3	9	2	10	1
6	1	2	3	4	5	6	7	8	9	10

Po sześciu tasowaniach wszystkie karty wróciły na swoje miejsca.

Bierzemy dla odmiany 14 kart. Teraz karty wracają na swoje miejsca po 14 tasowaniach.

Dorzucamy jeszcze dwie karty. Tasujemy 16 kart. Pierwotny układ pojawia się już po 5 tasowaniach.

Tasowanie wielu kart wiele razy jest dosyć pracochłonne. Czy nie można by przewidzieć bez żmudnego przekładania kart, po ilu tasowaniach wszystkie karty wrócą na swoje miejsca? Można, ale trzeba się najpierw nauczyć dwóch rzeczy. Po pierwsze, inaczej tasować karty. Po drugie, twierdzenia Eulera.

Wprawni gracze tasują karty w następujący sposób. Rozdzielają talię na 2 części, przytrzymują zagięte rogi kart w obu częściach i zbliżają je do siebie, następnie stopniowo puszczają rogi kart tak, aby prostujące się karty z obu części się wymieszały. Perfekcyjny tasowacz podzieli karty na dwie równe części i będzie puszczał po rogu jednej karty z każdej części (takie tasowanie nazywa się niekiedy przeplataniem do wewnątrz). Przy 10 kartach części wyglądają następująco:

$$1, 2, 3, 4, 5 \text{ i } 6, 7, 8, 9, 10.$$

Aby karta 10 nie znalazła się znowu na spodzie, nasz tasowacz puszcza na spód kartę 5, potem 10, potem 4, 9 itd. Po jednokrotnym przetasowaniu otrzyma karty w następującej kolejności:

$$6, 1, 7, 2, 8, 3, 9, 4, 10, 5,$$

co odpowiada permutacji będącej cyklem długości 10:

$$(1, 2, 4, 8, 5, 10, 9, 7, 3, 6).$$

Karty wrócą więc na miejsca po 10 tasowaniach.

Tasowanie 14 kart daje permutację będącą złożeniem trzech cykli długości 4 i cyklu długości 2:

$$(1, 2, 4, 8)\ (3, 6, 12, 9)\ (7, 14, 13, 11)\ (5, 10),$$

zatem karty wrócą na miejsca po 4 tasowaniach.

Przy tasowaniu $2n$ kart uzyskujemy permutację

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n & n+1 & n+2 & \ldots & 2n-1 & 2n \\ 2 & 4 & 6 & \ldots & 2n & 1 & 3 & \ldots & 2n-3 & 2n-1 \end{pmatrix}.$$

Widzimy, że karta z pozycji k przechodzi na pozycję $2k$ dla $k \leq n$ oraz na pozycję $2k - (2n+1)$ dla $k > n$. Możemy więc jednolicie powiedzieć, że karta z pozycji k przechodzi na pozycję $2k \pmod{2n+1}$.

Jeśli numery pozycji poszczególnych kart będziemy traktować jako reszty $\pmod{2n+1}$, to zauważamy, że każda karta po kolejnych tasowaniach „mnoży" numer swojej pozycji przez $2 \pmod{2n+1}$. Co stanie się z pierwszą kartą po t tasowaniach? Znajdzie się ona na pozycji $2^t \pmod{2n+1}$. Kiedy wróci ona na swoje pierwotne położenie? Wtedy, kiedy

$$2^t \equiv 1 \pmod{2n+1}.$$

Wtedy też wrócą na swoje pierwotne położenia wszystkie pozostałe karty.

O małym twierdzeniu Fermata i twierdzeniu Eulera

Pierre de Fermat, 1601–1665

Małe twierdzenie Fermata (wersja 1): Dla dowolnej liczby pierwszej p i liczby całkowitej a zachodzi podzielność

$$p \mid a^p - a.$$

Małe twierdzenie Fermata (wersja 2): Dla dowolnej liczby pierwszej p i liczby całkowitej a względnie pierwszej z p zachodzi podzielność

$$p \mid a^{p-1} - 1.$$

Idea dowodu.

Ponieważ dla $1 \leq i \leq p-1$ liczba $\binom{p}{i}$ dzieli się przez p, więc dla dowolnych liczb całkowitych b, c mamy

$$(b+c)^p = b^p + c^p + \sum_{i=1}^{p-1} \binom{p}{i} b^i c^{p-i} \equiv b^p + c^p \pmod{p}.$$

Przez indukcję otrzymujemy

$$a^p = \underbrace{(1+1+1+\ldots+1+1)^p}_{a} \equiv \underbrace{1^p + 1^p + 1^p + \ldots + 1^p + 1^p}_{a} = a \pmod{p}$$

dla a dodatnich oraz

$$(-a)^p \equiv -a^p \equiv -a \pmod{p}$$

dla a ujemnych.

Uwaga.

Nie każda liczba spełniająca tezę małego twierdzenia Fermata jest pierwsza. Liczby złożone spełniające małe twierdzenie Fermata są zwane liczbami Carmichaela (czyt. karmajkla) i jest ich nieskończenie wiele. Najmniejszą jest $561 = 3 \cdot 11 \cdot 17$.

Leonhard Euler, 1707–1783

Twierdzenie Eulera (wersja powszechnie używana): Dla dowolnej liczby naturalnej n i liczby całkowitej a względnie pierwszej z n zachodzi podzielność

$$n \mid a^{\varphi(n)} - 1,$$

gdzie

$$\varphi(p^k) = (p-1)p^{k-1}$$

dla liczby pierwszej p oraz

$$\varphi(st) = \varphi(s)\varphi(t)$$

dla liczb względnie pierwszych s i t.

Twierdzenie Eulera (wersja wzmocniona): Dla dowolnej liczby naturalnej n i liczby całkowitej a względnie pierwszej z n zachodzi podzielność

$$n | a^{\psi(n)} - 1 \,,$$

gdzie

$$\psi(p^k) = (p-1)p^{k-1}$$

dla liczby pierwszej nieparzystej p,

$$\psi(2) = 1, \quad \psi(4) = \psi(8) = 2, \quad \psi(2^k) = 2^{k-2} \qquad \text{dla } \; k \geq 4$$

oraz

$$\psi(st) = \mathrm{NWW}(\psi(s), \psi(t))$$

dla liczb względnie pierwszych s i t.

Twierdzenie Eulera dla potęg liczb pierwszych dowodzimy indukcyjnie. Krok indukcyjny przebiega następująco. Jeśli liczba a jest względnie pierwsza z p oraz

$$a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k} \,,$$

to $a^{(p-1)p^{k-1}}$ jest postaci $cp^k + 1$, skąd

$$a^{(p-1)p^k} = (cp^k+1)^p \equiv 1 + cp^k \binom{p}{1} + c^2 p^{2k} \binom{p}{2} +$$
$$+ \text{inne wyrazy podzielne przez } p^{k+1} \equiv 1 \pmod{p^{k+1}}.$$

Z powrotem do tasowania

Ze wzmocnionej wersji twierdzenia Eulera wiemy, że

$$2^{\psi(2n+1)} \equiv 1 (\mathrm{mod}\, 2n+1),$$

zatem wszystkie karty na pewno wrócą na swoje miejsca po $\psi(2n+1)$ tasowaniach, ale być może nastąpi to wcześniej. Najmniejsza liczba tasowań potrzebna do powrotu kart na swoje miejsca jest dzielnikiem liczby $\psi(2n+1)$.

A co z tasowaniem Monge'a $2n$ kart (przy nieparzystej liczbie kart ostatnia karta zawsze zostaje na spodzie)? Tym razem nie będziemy śledzić losów jednej karty, ale popatrzymy na jedną pozycję i będziemy notować karty, które na nią wchodzą po kolenych tasowaniach. Same karty ponumerujemy w sposób co najmniej dziwaczny. Na kartach napiszemy bowiem po 2 liczby według następującego przepisu:

$2n$	$2n-1$	$2n-2$		$n+1$	n		2	1
$2n+1$	$2n+2$	$2n+3$	$\cdots$	$3n$	$3n+1$	$\cdots$	$4n-1$	$4n$

Na każdej karcie napisane liczby sumują się do $4n+1$.

Po jednokrotnym przetasowaniu otrzymamy:

1	3	5		$2n-1$	$2n$		4	2
$4n$	$4n-2$	$4n-4$	$\cdots$	$2n+2$	$2n+1$	$\cdots$	$4n-3$	$4n-1$

Widzimy, że na każdą pozycję trafiła karta z liczbami pomnożonymi przez $2 (\mathrm{mod}\, 4n+1)$. To samo stanie się przy kolejnych tasowaniach. Jeśli bowiem po pierwszym tasowaniu na pozycję karty $\pm k (\mathrm{mod}\, 4n+1)$ weszła karta $\pm 2k (\mathrm{mod}\, 4n+1)$, to po drugim pojawi się tam karta, która zajęła po pierwszym tasowaniu miejsce karty $\pm 2k (\mathrm{mod}\, 4n+1)$, czyli karta $\pm 4k (\mathrm{mod}\, 4n+1)$.

Pierwsza karta od spodu (a także wszystkie inne karty) trafi na swoje miejsce po t tasowaniach, gdy $2^t \equiv \pm 1 (\mathrm{mod}\, 4n+1)$. Co ciekawego można powiedzieć o liczbie tasowań koniecznej do powrotu kart na swoje miejsca?

Jeszcze jeden rzut oka na twierdzenie Eulera

Z twierdzenia Eulera wypływa następujący

Wniosek: Dla $n \geq 3$ i a względnie pierwszego z n

$$a^{\varphi(n)/2} \equiv \pm 1 \pmod{n} \,.$$

Dowód: .
Jeśli n jest potęgą liczby pierwszej nieparzystej lub podwojoną potęgą liczby pierwszej nieparzystej, wówczas

$$a^{\varphi(n)} - 1 = \left(a^{\varphi(n)/2} + 1\right)\left(a^{\varphi(n)/2} - 1\right) \equiv 0 \pmod{n},$$

skąd wynika, że jeden z czynników iloczynu $\left(a^{\varphi(n)/2} + 1\right)\left(a^{\varphi(n)/2} - 1\right)$ dzieli się przez n.

Dla $n = 4$ teza wniosku jest oczywista.

Gdy n jest potęgą dwójki większą od 4, to

$$a^{\psi(n)} = a^{\varphi(n)/2} \equiv 1 \pmod{n}.$$

Gdy n nie jest potęgą liczby pierwszej, ani podwojoną potęgą liczby pierwszej, tezę wniosku otrzymujemy z podzielności $\psi(n) \mid \frac{\varphi(n)}{2}$; wówczas $a^{\varphi(n)/2} \equiv 1 \pmod{n}$.

Uwaga.

$7^4 \equiv 1 \pmod{15}$, ale to nie znaczy, że $7^2 \equiv \pm 1 \pmod{15}$.

O tasowaniu po raz trzeci

Z wniosku wynika, że w tasowaniu Monge'a wszystkie karty wrócą na swoje miejsca po

$$\frac{\varphi(4n+1)}{2} \leq 2n$$

tasowaniach. Liczba tasowań potrzebnych do powrotu do wyjściowej konfiguracji kart nie przekracza więc liczby kart (ten fakt wynika też z tego, że wszystkie karty wrócą na swoje miejsca, gdy wróci na swoje miejsce pierwsza karta).

Uwagi.

Bezpośrednio z twierdzenia Eulera wynika, że po $\psi(4n+1)$ tasowaniach karty wrócą na swoje miejsca.

Gdy n jest parzyste, a $4n+1$ pierwsze, wystarczy n tasowań. Wynika to ze znanego w teorii liczb faktu, że wówczas 2 jest resztą kwadratową $(\mathrm{mod}\, 4n+1)$, tzn. $2^{2n} \equiv 1 (\mathrm{mod}\, 4n+1)$. Te wartości n podane są w 4-tej kolumnie tabeli poniżej.

Najmniejsza liczba tasowań potrzebna do powrotu kart na swoje miejsca jest dzielnikiem liczb podanych powyżej.

Gdy $n = 2^m$, wszystkie karty wrócą jednocześnie na swoje miejsca po raz pierwszy po $m+2$ tasowaniach.

Poniżej podane są liczby tasowań potrzebne do powrotu kart na swoje miejsca zgodnie z powyższymi wzorami oraz najmniejsza liczba tasowań Min.

$2n$	$\frac{\phi(4n+1)}{2}$	$\psi(4n+1)$	n	Min
2	2	4		2
4	3	6		3
6	6	12		6
8	8	16	4	4
10	6	6		6
12	10	20		10
14	14	28		14
16	10	10		5
18	18	36		18
20	20	40	10	10
22	12	12		12
24	21	42		21
26	26	52		26
28	18	18		9

$2n$	$\frac{\phi(4n+1)}{2}$	$\psi(4n+1)$	n	Min
30	30	60		30
32	24	12		6
34	22	22		22
36	36	72	18	9
38	30	30		30
40	27	54		27
42	32	16		8
44	44	88	22	11
46	30	30		10
48	48	96	24	24
50	50	100		50
52	24	12		12
54	54	108		18
56	56	112	28	14

$2n$	$\frac{\phi(4n+1)}{2}$	$\psi(4n+1)$	n	Min
58	36	12		12
60	55	110		55
62	50	100		50
64	42	42		7
66	54	18		18
68	68	136	34	34
70	46	46		46
72	56	28		14
74	74	148		74
76	48	48		24
78	78	156		26
80	66	66		33
82	40	20		20
84	78	156		78
86	86	172		86
88	58	58		29
90	90	180		90
92	72	36		18
94	54	18		18
96	96	192	48	48
98	98	196		98
100	66	66		33
102	80	40		10
104	90	90		45
106	70	70		70
108	90	30		15
110	96	48		24
112	60	60		60
114	114	228		38
116	116	232	58	29
118	78	78		78
120	120	240	60	12
122	84	84		84
124	82	82		41
126	110	110		110
128	128	256	64	8

$2n$	$\frac{\phi(4n+1)}{2}$	$\psi(4n+1)$	n	Min
130	84	84		84
132	104	52		26
134	134	268		134
136	72	12		12
138	138	276		46
140	140	280	70	35
142	72	36		36
144	136	272		68
146	146	292		146
148	90	90		45
150	126	42		42
152	120	60		30
154	102	102		102
156	156	312	78	78
158	158	316		158
160	106	106		53
162	120	60		30
164	138	138		69
166	108	36		36
168	168	336	84	21
170	150	30		10
172	88	44		44
174	174	348		174
176	176	352	88	44
178	96	48		24
180	171	342		171
182	144	72		36
184	120	120		60
186	186	372		186
188	168	84		42
190	126	126		14
192	120	60		60
194	194	388		194
196	130	130		65
198	198	396		22
200	200	400	100	100

Uwagi ogólne

1. Przy nieparzystej liczbie kart (przy obu sposobach tasowania) jedna karta zawsze zostaje na swoim miejscu, dlatego rozważamy tylko tasowanie parzystej liczby kart.

2. Zarówno przy tasowaniu Monge'a, jak i przy przeplataniu do wewnątrz, karty wracają jednocześnie na swoje miejsca po liczbie tasowań nie większej niż liczba kart. Tymczasem permutacja zbioru 15-elementowego będąca złożeniem cykli rozłącznych długości 3, 5 i 7 wymaga 105-krotnego złożenia, aby dać w wyniku permutację identycznościową.

3. Liczba tasowań potrzebnych do powrotu kart na swoje miejsca nie jest najlepszym miernikiem jakości tasowania. Gdyby tak było, to tasowaniem nie gorszym od obydwu opisanych powyżej, byłoby tasowanie n kart odpowiadające permutacji będącej cyklem długości n:

$$(1\ 2\ 3\ \ldots\ n)\ .$$

Tymczasem polega ono na przełożeniu jednej karty ze spodu talii na wierzch. Autor szczerze wątpi, czy znalazłby się gracz, który miałby odwagę zaproponować przy stole karcianym ten sposób tasowania.

Bibliografia

[1] John H. Conway, Richard K. Guy, *Księga liczb*, Warszawa 1999.
[2] Szczepan Jeleński, *Śladami Pitagorasa*, Warszawa 1956.