Sobre el problema de Flavio Josefo

Víctor Arnaiz, Pedro Ángel Castillejo, Álvaro González

9 de abril de 2010

Introducción

El origen del problema se remonta a las llamadas guerras judeo-romanas, durante el siglo I. Según cuenta el historiador judío Flavio Josefo, él y cuarenta soldados camaradas fueron capturados por los romanos después de la caída de Jotapata. Antes que rendirse, decidieron acabar ellos mismos con sus vidas. Para hacerlo, se dispusieron en un círculo y acordaron que irían contando de tres en tres, de forma que cada tercer soldado sería ejecutado por la persona de su izquierda. El último hombre que quedara con vida tendría que suicidarse. Según cuenta la leyenda, Josefo calculó rápidamente cuál sería la posición del último hombre en morir para colocarse allí, y una vez hubieron muerto sus compatriotas, se entregó a los romanos. Josefo, sin embargo, en su obra *Las Guerras de los Judíos*, Libro III, Capítulo 8, dice que el orden de ejecución fue determinado por sorteo, y que él y su mejor amigo se salvaron tal vez por azar, o quizás por la divina intervención en el sorteo.

El problema que nos ocupará reaparece en la Edad Media, en la obra de Abraham ben Meir ibn Ezra (1092-1167), más conocido como Rabbi Ben Ezra, uno de tantos escolares judíos que vivieron y estudiaron en el Califato de Córdoba.

Otras versiones del problema aparecen en la matemática oriental. Un ejemplo es el libro datado en 1627, del matemático japonés Yoshida Koyu llamado *Tratado sobre los grandes y pequeños números*, en que se explica la versión japonesa del problema de Josefo. En ésta se ve involucrada una familia con 30 hijos, la mitad de ellos del primer matrimonio del padre, y la segunda de su segunda mujer. Para elegir al heredero de las propiedades de sus padres, se disponen los treinta en un círculo y se empieza a contar de diez en diez, de forma que el décimo de cada tanda es eliminado. La madre del primer matrimonio dispone a sus hijos de forma que los quince primeros eliminados sean los de la otra mujer, pero cuando ya han sido eliminados 14, el padre decide cambiar el sentido de giro. Así, todavía hay una oportunidad para el hijo del segundo matrimonio que no ha sido eliminado. El problema es hallar la posición que debe ocupar.

El problema clásico

Problema 1. *Se tienen n personas numeradas entorno a un círculo esperando ser ejecutadas. Empezando por la persona número 1, se saltan $m-1$ personas y se*

mata a la m-ésima. A continuación se saltan otras $m-1$ personas y se ejecuta a la siguiente, y así hasta que sólo quede una.

El objetivo es encontrar el lugar inicial en el círculo para sobrevivir $J(n,m)$, dados n y m.

El caso $m = 2$

Si la eliminación se hace de dos en dos, en la primera vuelta son eliminados los números pares. Si en principio había $2n$ personas, tras matar las n primeras se obtiene otro círculo de n personas, de forma que la persona i-ésima de este nuevo círculo se corresponde con la $2i-1$ del primero. En otro caso, si al principio teníamos $2n+1$, tras la muerte de $n+1$ personas obtenemos otro círculo de n personas, y ahora la persona i-ésima de éste se corresponde con la $2i+1$ del círculo de partida. Se establece así la recurrencia siguiente:

$$\begin{aligned} J(1) &= 1 \\ J(2n) &= 2J(n)-1 \\ J(2n+1) &= 2J(n)+1 \end{aligned}$$

Ahora ya podemos construir rápidamente una tabla de valores para $J(n,2)$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1

Se demuestra por inducción la fórmula explícita

$$J(2^m + l, 2) = 2l + 1$$

con $m \geq 0$ y $0 \leq l < 2^m$. Esto lo podemos expresar únicamente en función de n como $J(n) = 1 + 2(n - 2^{\lfloor \log_2 n \rfloor})$.

Otra forma de ver $J(n,2)$ es poniendo n en base 2. Así,

$$\begin{aligned} n &= (1\, b_{m-1}\, b_{m-2} ... b_1\, b_0)_2 \\ l &= (0\, b_{m-1}\, b_{m-2} ... b_1\, b_0)_2 \\ 2l &= (b_{m-1}\, b_{m-2} ... b_1\, b_0\, 0)_2 \\ 2l+1 &= (b_{m-1}\, b_{m-2} ... b_1\, b_0\, 1)_2 \\ J(n) &= (b_{m-1}\, b_{m-2} ... b_1\, b_0\, b_m)_2 \end{aligned}$$

La última igualdad se sigue de que $b_k = 1$. Por tanto, hemos probado que,

$$J((b_m\, b_{m-1} ... b_1\, b_0)_2) = (b_{m-1}\, b_{m-2} ... b_1\, b_0\, b_m)_2$$

El caso $m = 3$

En general, para todos n y m se cumple que

$$J(n,m) \equiv J(n-1,m) + m \pmod{n} \tag{1}$$

porque después de matar a la primera persona se obtiene un nuevo círculo de $n-1$ personas, donde la primera se corresponde con la $1+m$ del anterior.

A partir de esta recurrencia obtenemos la tabla para los primeros valores de $J(n,3)$:

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

Vemos que la sucesión $J(n)$ aumenta de tres en tres hasta que sobrepasa a n y entonces empieza de nuevo en 1 o en 2. Nos fijaremos ahora en la sucesión $\mathcal{N}_k$ definida como

$$\{\mathcal{N}_k\}_{k=1}^{\infty} = \{n : \ J(n,3) \in \{1,2\}\}$$

Consideremos $\mathcal{N}_{k-1} \leq n < \mathcal{N}_k$. Entonces, utilizando (1) vemos que

$$J(n) = J(\mathcal{N}_{k-1}) + 3(n - \mathcal{N}_{k-1}), \tag{2}$$

y para $n = \mathcal{N}_k$ se cumplirá

$$\mathcal{N}_k + J(\mathcal{N}_k) = J(\mathcal{N}_{k-1}) + 3(\mathcal{N}_k - \mathcal{N}_{k-1}),$$

que reordenando queda como

$$3\mathcal{N}_{k-1} - J(\mathcal{N}_{k-1}) = 2\mathcal{N}_k - J(\mathcal{N}_k)$$

Realizando una distinción de casos, desarrollamos la recurrencia así:

$$\begin{cases} J(\mathcal{N}_1) = J(1) = 1 \\ \text{Si } \mathcal{N}_k \text{ es impar} \begin{cases} J(\mathcal{N}_k) = 1 \Rightarrow J(\mathcal{N}_{k+1}) = J\left(\dfrac{3\mathcal{N}_k + 1}{2}\right) = 2 \\ J(\mathcal{N}_k) = 2 \Rightarrow J(\mathcal{N}_{k+1}) = J\left(\dfrac{3\mathcal{N}_k - 1}{2}\right) = 1 \end{cases} \\ \text{Si } \mathcal{N}_k \text{ es par} \begin{cases} J(\mathcal{N}_k) = 1 \Rightarrow J(\mathcal{N}_{k+1}) = J\left(\dfrac{3\mathcal{N}_k}{2}\right) = 1 \\ J(\mathcal{N}_k) = 2 \Rightarrow J(\mathcal{N}_{k+1}) = J\left(\dfrac{3\mathcal{N}_k}{2}\right) = 2. \end{cases} \end{cases}$$

Además, si escribimos los $\mathcal{N}_k$ en base 3, podemos ver la siguiente

Observación 1.

$$\left.\begin{array}{ll} \mathcal{N}_k \equiv 0 & (\text{mód } 3^l) \\ \mathcal{N}_k \equiv j \cdot 3^l & (\text{mód } 3^{l+1}) \end{array}\right\} \Rightarrow J(\mathcal{N}_k) = \begin{cases} j & \textit{si } l \textit{ es par;} \\ 3 - j & \textit{si } l \textit{ es impar,} \end{cases}$$

para todo k *con* $l \geq 0$ *y* $1 \leq j \leq 2$.

Demostración. Procedemos por inducción sobre k. Lo comprobamos para $\mathcal{N}_1 = 1$. Supongamos que es cierto para $\mathcal{N}_k$. Si $\mathcal{N}_k$ es par, entonces $\mathcal{N}_{k+1} = \frac{3}{2}\mathcal{N}_k$ y $J(\mathcal{N}_{k+1}) = J(\mathcal{N}_k)$. Entonces

$$\mathcal{N}_k \equiv j \cdot 3^l \pmod{3^{l+1}} \Rightarrow \mathcal{N}_{k+1} = \frac{3}{2}\mathcal{N}_k \equiv (3-j) \cdot 3^{l+1} \pmod{3^{l+2}}.$$

Si $\mathcal{N}_k$ es impar, entonces

$$J(\mathcal{N}_k) = 1 \Rightarrow \mathcal{N}_{k+1} = \frac{3\mathcal{N}_k + 1}{2} \equiv 2 \pmod{3};$$

$$J(\mathcal{N}_k) = 2 \Rightarrow \mathcal{N}_{k+1} = \frac{3\mathcal{N}_k - 1}{2} \equiv 1 \pmod{3}.$$

□

Busquemos una expresión que nos determine la suma de los m primeros términos de $\{\mathcal{N}_k\}$. Teníamos

$$3\mathcal{N}_k - J(\mathcal{N}_k) = 2\mathcal{N}_{k+1} - J(\mathcal{N}_{k+1})$$

En particular, para $k = 1$:

$$3\mathcal{N}_1 - J(\mathcal{N}_1) = 2\mathcal{N}_2 - J(\mathcal{N}_2)$$

Sumando $\mathcal{N}_2$ a los dos términos de la igualdad obtenemos

$$3\mathcal{N}_1 + \mathcal{N}_2 - J(\mathcal{N}_1) = 3\mathcal{N}_2 - J(\mathcal{N}_2) = 2\mathcal{N}_3 - J(\mathcal{N}_3)$$

$$\mathcal{N}_1 + \mathcal{N}_2 = 2\mathcal{N}_3 - J(\mathcal{N}_3) - 2\mathcal{N}_1 + J(\mathcal{N}_1)$$

siendo $\mathcal{N}_1 = 1$ y $J(\mathcal{N}_1) = 1$. Aplicando inducción sobre k podemos expresar la suma de los k primeros términos de $\{\mathcal{N}_k\}$ como sigue:

$$\mathcal{S}_k = \sum_{i=1}^{k} \mathcal{N}_i = 2\mathcal{N}_{k+1} - J(\mathcal{N}_{k+1}) - 1 \tag{3}$$

No olvidemos que nuestro objetivo es encontrar una expresión que nos determine el término general de $J(n, 3)$. Sigamos.

Proposición 1. *La sucesión* $\mu_k = \dfrac{\mathcal{N}_k}{\left(\frac{3}{2}\right)^{k-1}}$ *es convergente.*

Demostración. Sea t el menor natural tal que $\mathcal{N}_{k+t} \neq \frac{3}{2}\mathcal{N}_{k+t-1}$, entonces se verifica que

$$\mu_{k+t} = \mu_k + \frac{1}{2(\frac{3}{2})^{k+t-1}}, \text{ o bien, } \mu_{k+t} = \mu_k - \frac{1}{2(\frac{3}{2})^{k+t-1}}.$$

Esto quiere decir que podemos expresar $\{\mu_k\}$ como

$$\mu_k = 1 + \frac{1}{2(\frac{3}{2})^{s_1}} - \frac{1}{2(\frac{3}{2})^{s_2}} + \ldots + (-1)^{t+1}\frac{1}{2(\frac{3}{2})^{s_t}}$$

donde $\{s_n\}$ es la subsucesión de números naturales que cumplen que $\mathcal{N}_{s_{i+1}} \neq \frac{3}{2}\mathcal{N}_{s_i}$, es decir:

$$\mathcal{N}_{s_n} = \frac{3\mathcal{N}_{s_n-1} + (-1)^{n+1}}{2}.$$

Cuando m tiende a infinito, tenemos

$$\lim_{k\to\infty} \mu_k = 1 + \frac{1}{2}\sum_{i=1}^{\infty} (-1)^{i+1} \left(\frac{2}{3}\right)^{s_i}$$

y esta serie es convergente, porque $|(-1)^{i+1}\left(\frac{2}{3}\right)^{s_i}| \to 0$. □

Aproximamos computacionalmente dicho límite al que llamamos μ:

$$\lim_{k\to\infty} \mu_k = \mu \approx 1,21670287712495\ldots$$

Podemos extender este resultado a las sumas $\mathcal{S}_k$, ya que:

$$\lim_{k\to\infty} \frac{\mathcal{S}_k}{2\left(\frac{3}{2}\right)^k - 2} = \lim_{k\to\infty} \frac{2\mathcal{N}_{k+1} - 1 - J(\mathcal{N}_{k+1})}{2\left(\frac{3}{2}\right)^k - 2} = \lim_{k\to\infty} \frac{\mathcal{N}_{k+1}}{\left(\frac{3}{2}\right)^k} = \mu$$

A continuación, utilizaremos todo esto para obtener el término general de $J(n,3)$. Recordemos (2),

$$J(n) = J(\mathcal{N}_k) + 3\,(n - \mathcal{N}_k)$$

donde $\mathcal{N}_k \leq n < \mathcal{N}_{k+1}$. Ahora, por (3) tenemos

$$\mathcal{S}_{k-1} = 2(\mathcal{N}_k - 1) - J(\mathcal{N}_k) + 1 \Rightarrow J(\mathcal{N}_k) = 2\mathcal{N}_k - 1 - \mathcal{S}_{k-1}$$

y sustituyendo esto en (2) obtenemos

$$J(n) = 3n - 1 - \mathcal{S}_k$$

Entonces, un posible término general para $J(n,3)$ es

$$J(n) = 3n - 1 - \left[2\mu\left(\left(\frac{3}{2}\right)^{\lfloor \log_{3/2}\frac{n}{\mu}\rfloor + 1} - 1\right)\right]$$

Sin embargo, esta fórmula no es válida porque, como ya hemos visto, $\{\mu_k\}$ es una sucesión oscilante. El problema es que cuando $\mu_k < \mu$ se tiene que

$$\log_{3/2}\frac{\mathcal{N}_k}{\mu} < \log_{3/2}\frac{\mathcal{N}_k}{\mu_k} = k - 1$$

y al aproximar hacia abajo obtenemos $k-2$ en vez de $k-1$.

Para arreglar esto, sustituimos $\lfloor \log_{3/2}\frac{n}{\mu}\rfloor + 1$ por $\lfloor \log_{3/2}\frac{3n+1}{2\mu}\rfloor$. Veamos que así el término general sí funciona como queremos.

Es trivial comprobar que

$$\log_{3/2} \frac{3n+1}{2\mu} \geq \log_{3/2} \frac{\mathcal{N}_{k+1}}{\mu_{k+1}} = \log_{3/2} \left(\frac{3}{2}\right)^k = k.$$

Sin embargo, para que el cambio sea lícito ha de cumplirse también la siguiente desigualdad:

$$\log_{3/2} \frac{3n+1}{2\mu} < \log_{3/2} \frac{\mathcal{N}_{k+2}}{\mu_{k+2}} = \log_{3/2} \left(\frac{3}{2}\right)^{k+1} = k+1$$

Para probar esto, es suficiente con probar el peor de los casos, es decir, cuando $n = \mathcal{N}_{k+1} - 1$. La desigualdad queda

$$\frac{3n+1}{2\mu} = \frac{3\mathcal{N}_{k+1} - 2}{2\mu} < \frac{\mathcal{N}_{k+2}}{\mu_{k+2}} = \left(\frac{3}{2}\right)^{k+1}$$

Operando, llegamos a

$$\left(\frac{3}{2}\right)^k (\mu_k - \mu) < 1,$$

que, si $\mu_k < \mu$, es trivial. En caso contrario, hay que demostrar

$$\mu_k - \mu < \frac{1}{\left(\frac{3}{2}\right)^k}$$

Como $\mu_k > \mu$, podemos expresar μ_k como

$$\mu_k = 1 + \frac{1}{2\left(\frac{3}{2}\right)^{s_1}} - \frac{1}{2\left(\frac{3}{2}\right)^{s_2}} + \cdots + \frac{1}{2\left(\frac{3}{2}\right)^{s_t}}$$

Entonces, existe $l > k$ tal que

$$\mu_l = \mu_k - \frac{1}{2\left(\frac{3}{2}\right)^{s_{t+1}}}$$

donde $s_t \leq k < s_{t+1}$ Por tanto,

$$\mu_k - \mu < \mu_k - \mu_l = \frac{1}{2\left(\frac{3}{2}\right)^{s_{t+1}}} < \frac{1}{\left(\frac{3}{2}\right)^k},$$

como queríamos demostrar.

Por tanto, el término general de $J(n,3)$ es

$$J(n) = 3n - 1 - \mathcal{S}_k = 3n - 1 - \left[2\mu\left(\left(\frac{3}{2}\right)^{\lfloor \log_{3/2} \frac{3n+1}{2\mu} \rfloor} - 1\right)\right]$$

Permutaciones de Josefo

Definición 1. *Se define una permutación de Josefo $P(n,k)$ como una permutación de n elementos resultado de aplicar la eliminación de Josefo con el parámetro m.*

Ejemplos:

$$P(7,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 5 & 3 & 7 \end{pmatrix}$$

$$P(5,60) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

De las $n!$ permutaciones posibles sólo son de Josefo $L(n) = \text{mcm}(1,2,\ldots,n)$, dado que $P(n,k) = P\left(n, k + L(n)\right)$, porque $L(n) \equiv 0 \pmod{1,\ldots,n}$. Hay una correspondencia inmediata entre el sistema de congruencias de k módulos $n, n-1, \ldots, 1$ y la permutación $P(n,k)$.

Con $n = 4$ son:

k	$\text{mod}(4,3,2,1)$	$P(4,k)$
1	1 1 1 1	1 2 3 4
2	2 2 2 1	2 4 3 1
3	3 3 1 1	3 2 4 1
4	4 1 2 1	4 1 3 2
5	1 2 1 1	1 3 4 2
6	2 3 2 1	2 1 4 3
7	3 1 1 1	3 4 1 2
8	4 2 2 1	4 2 1 3
9	1 3 1 1	1 4 2 3
10	2 1 2 1	2 3 1 4
11	3 2 1 1	3 1 2 4
12	4 3 2 1	4 3 2 1

Identificamos el elemento 0 de $\mathbb{Z}_i$ con i para que el número $(n-i)$-ésimo represente el salto en el círculo sin dar más de una vuelta.

Vamos a ver cómo afecta a una permutación de Josefo la transposición de dos de sus elementos.

Proposición 2. *Sea la permutación $P(n,k)$ con $n \geq 4$. Si realizamos una transposición $(i, i+1)$, la permutación resultante no es de Josefo.*

Demostración. Cada permutación tiene asociado un sistema de congruencias con módulos $1, \ldots n$. Para que la permutación sea de Josefo, ha de ser resoluble el sistema de congruencias asociado (el parámetro de eliminación k es la solución del sistema). Vamos a comparar los sistemas antes y después de la transposición.

$$\begin{cases} k \equiv \overline{r_0} & (\text{mód } n) \\ \quad\vdots & \quad\vdots \\ k \equiv \overline{r_{i-2}} & (\text{mód } n-i+2) \\ k \equiv \overline{r_{i-1}} & (\text{mód } n-i+1) \\ k \equiv \overline{r_i} & (\text{mód } n-i) \\ k \equiv \overline{r_{i+1}} & (\text{mód } n-i-1) \\ k \equiv \overline{r_{i+2}} & (\text{mód } n-i-2) \\ \quad\vdots & \quad\vdots \\ k \equiv \overline{r_{n-1}} & (\text{mód } 1) \end{cases} \qquad \begin{cases} q \equiv \overline{r_0} & (\text{mód } n) \\ \quad\vdots & \quad\vdots \\ q \equiv \overline{r_{i-2}} & (\text{mód } n-i+2) \\ q \equiv \overline{\overline{r_{i-1}} + \overline{r_i}} & (\text{mód } n-i+1) \\ q \equiv \overline{1-\overline{r_i}} & (\text{mód } n-i) \\ q \equiv \overline{\overline{r_i} + \overline{r_{i+1}} - 1} & (\text{mód } n-i-1) \\ q \equiv \overline{r_{i+2}} & (\text{mód } n-i-2) \\ \quad\vdots & \quad\vdots \\ q \equiv \overline{r_{n-1}} & (\text{mód } 1) \end{cases}$$

Llamaremos $\overline{r_t} = \begin{cases} r_t & \text{si} \quad r_t \neq 0 \\ n-t & \text{si} \quad r_t = 0 \end{cases}$.

En particular, la congruencia $a \equiv b \pmod{2p}$ sólo tendrá solución si $a \equiv b \pmod 2$. Para ver si el sistema tiene solución sólo tendremos en cuenta la paridad.

Se cumple que si $n-t$ es par, entonces $\overline{r_t} \equiv r_t \pmod 2$. Distingamos dos casos:

- Si $n-i$ es par. Entonces $q \equiv 1 - r_i \pmod 2$ y $q \equiv r_{i+2} \pmod 2$, lo cual es imposible, ya que $r_i \equiv r_{i+2} \pmod 2$.
- Si $n-i$ es impar. Entonces $q \equiv r_{i-1} + \overline{r_i} \pmod 2$ y $q \equiv \overline{r_i} + r_{i+1} - 1 \pmod 2$, imposible, porque $r_{i-1} \equiv r_{i+1} \pmod 2$. □

Proposición 3. *Sea la permutación $P(n,k)$ con $n \geq 4$. Si realizamos una transposición de la forma $(i, i+2)$, la permutación resultante no es de Josefo.*

Demostración. El sistema inicial es el mismo, y las $i-1$ primeras congruencias y las $n-i-1$ finales del sistema resultante no varían. Hacemos la transposición $(i,i+2) = (i,1+1) \circ (i,i+2) \circ (i+1,i+2)$ y distinguimos dos casos:

- $n-i$ es par:

S. Inicial	$(i,1+1)$	$(i,i+2)$	$(i+1,i+2)$	
ξ_1	ξ_3		ξ_6	$(\text{mód } n-i+1)$
r_i	r_i+1	$r_i+\xi_4+1$	$r_i+\xi_4$	$(\text{mód } 2)$
ξ_2	ξ_4	ξ_5	ξ_7	$(\text{mód } n-i-1)$
r_{i+2}		$r_{i+2}+\xi_4+1$	$r_{i+2}+\xi_4+1$	$(\text{mód } 2)$

  donde los ξ_t representan los valores con los que es congruente el parámetro de ejecución después de efectuar cada transposición inmediata. No nos interesa su valor porque su módulo es impar.

  Para que el sistema final tenga solución $r_i + \xi_4 \equiv r_{i+2} + \xi_4 + 1$, imposible porque $r_i \equiv r_{i+2}$.

- $n-i$ es impar:

S. Inicial	$(i, 1+1)$	$(i, i+2)$	$(i+1, i+2)$	
r_{i-1}	$r_{i-1}+\xi_1$		$r_{i-1}+\xi_1+\xi_3$	(mód 2)
ξ_1	ξ_2	ξ_3	ξ_5	(mód $n-i$)
r_{i+1}	$r_{i+1}+\xi_1+1$	$r_{i+1}+\xi_1$	$r_{i+1}+\xi_1+\xi_3+1$	(mód 2)
ξ_4		ξ_4	ξ_4	(mód $n-i-2$)

  Para que tenga solución $r_{i-1}+\xi_1+\xi_3 \equiv r_{i+1}+\xi_1+\xi_3+1$, imposible porque $r_{i-1} \equiv r_{i+1}$. □

Observación. Para la transposición $(i, i+3)$, si $n-i$ es par entonces llegamos a que $r_i+\xi_4+\xi_6 \equiv r_{i+2}+\xi_4+\xi_6+1 \Rightarrow r_i \equiv r_{i+2}+1$, contradicción. Sin embargo, para $n-i$ impar no podemos asegurar nada mediante este procedimiento.

Para la transposición (i, j), con $j-i \in \{4, 5, 6\}$ no es cierto que componiéndola con una permutación de Josefo ésta deje de serlo[1] necesariamente. Algunos contraejemplos son:

- Para $i-j=4$: $(1,5) \circ P(6,22) = P(6,25)$ y también $(1,5) \circ P(6,36) = P(6,39)$.
- Para $i-j=5$: $(1,6) \circ P(6,31) = P(6,34)$ y $(2,7) \circ P(7,30) = P(7,387)$.
- Para $i-j=6$: $(1,7) \circ P(7,15) = P(7,390)$ y $(1,7) \circ P(7,286) = P(7,331)$.

Paridad de las permutaciones de Josefo.

Sea $\mathcal{PJ}_n$ el conjunto de las permutaciones de Josefo de n elementos. Definimos la aplicación f como

$$\begin{array}{rccc} f: & \mathcal{PJ}_n & \longrightarrow & \mathcal{PJ}_{n-1} \\ & P(n,k) & \longmapsto & P(n-1,k) \end{array}$$

Consideremos la permutación de Josefo $P(n,k) = (a_1\ a_2\ \ldots\ a_n)$. Entonces, $f(P(n,k)) = P(n-1,k) = (b_2\ b_3\ \ldots\ b_n)$, donde $b_i = a_i + (n-a_1)$, y $b_i \in \mathbb{Z}_n$.

Los sistemas de congruencias asociados a las dos permutaciones son

	Permutación	Sistema de congruencias
$P(n,k)$	$(a_1\ a_2\ \ldots\ a_n)$	$r_n\ r_{n-1}\ \ldots\ r_1 \pmod{n, n-1, \ldots, 1}$
$P(n-1,k)$	$(b_2\ b_3\ \ldots\ b_n)$	$r_{n-1}\ \ldots\ r_1 \pmod{n-1, \ldots, 1}$

Claramente, f es suprayectiva y en general no inyectiva, salvo si $\text{m.c.m}(1, \ldots, n) = \text{m.c.m}(1, \ldots, n-1)$, en cuyo caso es biyectiva.

Supongamos que $P(n-1,k)$ es composición de t transposiciones. Veamos que, a partir de $Id_n = (1\ 2\ \ldots\ n)$ podemos obtener la permutación $P'(n,k) = (n\ b_2\ b_3\ \ldots\ b_n)$

[1] Para $i-j \geq 7$ no podemos asegurar nada, aunque seguramente también existan contraejemplos.

mediante $n-1+t$ transposiciones (probablemente también mediante menos). Ahora, partiendo de $P'(n,k)$, podemos obtener $P(n,k)$ mediante $(n-1)(n-r_n)$ transposiciones (recordemos que $b_i = a_i+(n-a_1) = a_i+(n-r_n)$, en $\mathbb{Z}_n$). Por tanto, denotando $\mathfrak{p}(\sigma)$ la paridad de la permutación σ, tenemos

$$\mathfrak{p}(P(n,k)) = n-1+t+(n-1)(n-r_n) = t+(n-1)(1+n-r_n) \pmod 2,$$

es decir,

$$\mathfrak{p}(P(n,k)) = \mathfrak{p}(P(n-1,k)) + (n-1)(1+n-r_n) \pmod 2.$$

Proposición 4. *Las permutaciones de Josefo de $4k$ y $4k+1$ elementos son pares, mientras que exactamente la mitad de las permutaciones de Josefo de $4k+2$ y $4k+3$ elementos son pares.*

Demostración. Por inducción sobre n. Para $n = 1$ la comprobación es trivial. Supongamos ahora que, para cierto k, todas las permutaciones de Josefo de $n-1 = 4k+1$ elementos son pares. Entonces, $(n-1)(1+n-r_n)$ es par si $r_n \equiv 1 \pmod 2$, y es impar si $r_n \equiv 0 \pmod 2$. Pero $r_n \equiv r_2 \pmod 2$, y como exactamente la mitad de las permutaciones de Josefo tienen $r_2 = 1$ y la otra mitad tienen $r_2 = 2$, se sigue que la mitad de las permutaciones de $4k+2$ elementos son pares y la otra mitad impares. Concretamente, son pares aquellas con $r_2 = 1$ e impares aquellas con $r_2 = 2$.

Ahora, si $n-1 = 4k+2$, entonces $(n-1)(1+n-r_n)$ es par para todos los r_n; luego la mitad de las permutaciones de $4k+3$ elementos son pares y la otra mitad impares.

Sigamos, si $n-1 = 4k+3$, entonces $(n-1)(1+n-r_n)$ es par si $r_2 = 1$, y es impar si $r_2 = 2$. Pero las permutaciones de $4k+3$ elementos con $r_2 = 1$ son pares mientras que las que tienen $r_2 = 2$ son impares. Por tanto, todas las permutaciones de Josefo de $4k+4$ elementos son pares.

Por último, si $n-1 = 4k$, entonces $(n-1)(1+n-r_n)$ es par para todos los r_n, luego todas las permutaciones de $4k+1$ elementos son pares.

□

Problemas abiertos

Observación. Para $P(n,1) = Id$, al realizar una transposición cualquiera, la permutación deja de ser de Josefo.

Demostración. Para probar esto veamos que

$$P(n,1): \begin{cases} k \equiv 1 & \pmod n \\ \vdots & \\ k \equiv 1 & \pmod 2 \end{cases}$$

Tras aplicar la transposición, para que la permutación obtenida sea de Josephus ha de existir q tal que

$$\begin{cases} q \equiv j-i+1 & (\text{mód } n-i+1) \\ q \equiv n-j+2 & (\text{mód } n-i) \\ q \equiv n-j+1 & (\text{mód } n-j+1) \\ q \equiv 1 & (\text{mód } k)\ \ \forall k \neq n-i+1, n-i, n-j+1 \end{cases}$$

Distingamos dos casos:

1) $n-i+1$ es par. Si $j-i+1$ es par, entonces n y j tienen la misma paridad y $n-j+1$ es impar, por lo que existe $k \neq n-i+1$ que es par tal que $m \equiv 1(\text{mod}\, k)$ y el sistema no tiene solución. Si $j-i+1$ es impar, entonces n y j tienen distinta paridad, luego $n-j+1$ es par, lo que es imposible.

2) $n-i$ es par. Si $n-j+2$ es par, entonces $n-j+1$ es impar y existe $k \neq n-i$ que es par tal que $m \equiv 1(\text{mod}\, k)$, luego el sistema no tiene solución. Por el contrario, si $n-j+2$ es impar, entonces $n-j+1$ es par, lo que es imposible. □

Problema 1 Para $P(n,1) = Id$, al realizar una transposición cualquiera, la permutación deja de ser de Josefo. Encontrar las permutaciones $P(n,k)$ que comparten esta propiedad.

Problema 2 Diremos que un *subconjunto de Josefo* de $\{1,2,\ldots,n\}$ es un conjunto de p números para los cuales, existe algún k tal que las personas con los otros $n-p$ números son eliminadas primero. Con $n=9$, tres de los 2^9 subconjuntos no son de Josefo, a saber, $\{1,2,5,8,9\}$, $\{2,3,4,5,8\}$, y $\{2,5,6,7,8\}$. Hay 13 subconjuntos que no son de Josefo con $n=12$, ninguno para otros valores de $n \leq 12$. ¿Existen subconjuntos que no son de Josefo para $n > 12$?

Referencias

[1] R. Cooke *The History of Mathemaics: A brief course*

Wiley, 1997, 247-248

[2] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics: A foundation for Computer Science,*

Addison Wesley, 2nd ed., 1994.

[3] A. M. Odlyzko, H. S. Wilf, *Functional iteration and the Josephus problem.*

[4] P. Schumer, *The Josephus Problem: Once More Around, Mathematics Magazine.*

[5] R. Stephan, *On a sequence related to the Josephus problem.*

`www.arxiv.org/abs/math/0305348v1`