Josephus Permutations

James Dowdy
and
Michael E. Mays
Department of Mathematics
West Virginia University
Morgantown, WV 26506

Abstract. The Josephus problem is concerned with anticipating which will be the last elements left in the ordered set $\{1,2,\ldots,n\}$ as successive mth elements (counting cyclically) are eliminated. We study the set of permutations of $\{1,2,\ldots,n\}$ which arise from the different orders of elimination as m varies, and give a criterion based on the Chinese Remainder Theorem for deciding if a given permutation can be interpreted as arising as a given order of elimination for some step size m in a Josephus problem.

As the Jewish historian Flavius Josephus relates the story [9], he and forty compatriots were trapped in a cave after the fall of the city Jotapata. He contrived to survive, after the others decided that it would be better to commit suicide rather than surrender to the Romans, by suggesting that the suicide be done serially, by lot, with each lot drawer killing the previous lot holder. Josephus was last, surrendered, and lived to tell the tale. Josephus's details on the mechanism for his feat were vague, so it was for Bachet [2] to suggest a specific mechanism for the order to be established. His suggestion was to arrange the men in a circle and to count around by threes to determine the order of elimination. This idea is said to have motivated S. Ulam's definition of *lucky numbers*, which are given by a sieving procedure where successive step sizes are determined by the most recent uneliminated number. A summary of the history of the problem is provided in [15].

There are three themes which are developed in the extensive literature on the Josephus problem. The first is a "mathematics appreciation" approach, which gives the historical background of the problem or variants of it and then poses particular questions about the order of elimination. This is the approach introduced in [2], followed in [5], [6], and the first set of exercises in [10]. A second, more sophisticated, approach is to generate formulas, algorithms, or general approaches to determining the order of elimination for a particular set size n and step size m. One can find which element is eliminated on the kth iteration of the cyclic counting procedure, or which iteration eliminates the kth element, instead of just looking at the last element, in the special case $k = n$. A related problem in this more general mold is frequently cast as one involving Christians and Turks. Here, half of a mixed group is to be eliminated before anyone in the other half has to be sacrificed. Whether it is to be Christians or Turks to be spared depends on who is telling the story. An algorithm given in [12] is considered in [4], and described in

[1]. This is the substance of [3], [8], and [14], the second set of exercises in [10], and [7], [11], and [13]. The third approach is to back away from the particular m and consider more generally what can be said for a fixed n and varying m. The notation of [8] links m-enumeration of a set with the Josephus problem and permutations, and the terminology of Josephus permutations that [10] introduces is especially appropriate.

This paper is a contribution in this third area: a study of the set of *Josephus permutations* of a set of n elements. Notation will be that of Jakóbczyk [8]: Start with the ordered set $Z_n = \{1, 2, \ldots, n\}$. Choose a_1 to be the mth element, if $m \leq n$, or the kth element, where $k \equiv m \pmod{n}$, if $m > n$, and successive elements $a_2, a_3, \ldots$ by removing cyclically, from left to right, each mth element of Z_n until the set is exhausted. The chosen elements form a new ordered set $\{a_1, a_2, \ldots, a_n\}$, which we denote $Z_n^{(m)}$. This determines the permutations of $\{1, 2, \ldots, n\}$

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix}$$

The identification algorithm we develop is more easily implemented using the inverse of this permutation. We will give the permutation by listing the bottom row alone, interpreted as specifying at which step the kth entry in the ordered set is eliminated, rather than the natural interpretation of the bottom row above, which gives which entry of the initial ordered set is eliminated at the kth step.

The point of exercises 28 and 29 of p. 181 of [10] is that these permutations have an interesting cycle structure. However, the cycle notation obscures the patterns generated as m varies. In the table on the next page, we list the 60 distinct ordered sets $Z_6^{(m)}$, obtained as m takes on values between 1 and 60.

There are patterns to notice in the table which can be established in general. The first concerns the size of the table.

Theorem 1. *There are exactly $l(n) = lcm(1, 2, \ldots, n)$ distinct Josephus permutations of a set with n elements, which may be generated by taking m to be $1, 2, \ldots, l(n)$.*

Proof: First note that the number of Josephus permutations is less than or equal to $l(n)$. This follows from the observation that in counting cyclically through a set of no more than n elements, stepping by m or stepping by $m + l(n)$ yields the same result since $l(n) \equiv 0 \pmod{k}$ for any $k, 1 \leq k \leq n$. Now we show that the number is at least $l(n)$ by induction on n. We verify that there are 2 distinct Josephus permutations for $n = 2$ (and 6 distinct Josephus permutations for $n = 3$), and then suppose we have $l(k-1)$ distinct Josephus permutations for a set of $k-1$ elements. Then the smallest value of $m > 1$ for which $Z_k^{(m)} = Z_k$ must satisfy $m \equiv 1 \pmod{k}$, because 1 is the first element of $Z_k^{(m)}$ only for $m \equiv 1 \pmod{k}$. On the other hand, once 1 is placed we are counting around a set with $k - 1$ elements, and by the induction hypothesis this preserves the order of $\{2, 3, \ldots, n\}$ only for $m \equiv 1 \pmod{l(k-1)}$. By the Chinese Remainder Theorem these two congruences have a unique solution modulo $lcm(k, l(k-1)) = l(k)$. That solution is $m \equiv 1 \pmod{l(k)}$, and so the number of distinct Josephus permutations is at least $l(k)$. This, together with the first remark, establishes the theorem.

60 Josephus Permutations of 6 Elements

1	2	3	4	5	6 : 1	6	5	4	3	2	1 : 60
5	1	4	2	6	3 : 2	3	6	2	4	5	1 : 59
6	4	1	3	5	2 : 3	2	5	3	1	4	6 : 58
3	2	4	1	6	5 : 4	5	6	1	4	2	3 : 57
6	4	5	2	1	3 : 5	3	1	2	5	4	6 : 56
2	4	3	6	5	1 : 6	1	5	6	3	4	2 : 55
1	4	2	5	6	3 : 7	3	6	5	2	4	1 : 54
4	1	6	3	2	5 : 8	5	2	3	6	1	4 : 53
2	3	1	5	6	4 : 9	4	6	5	1	3	2 : 52
4	6	2	1	5	3 : 10	3	5	1	2	6	4 : 51
4	5	3	6	1	2 : 11	2	1	6	3	5	4 : 50
3	2	6	5	4	1 : 12	1	4	5	6	2	3 : 49
1	5	6	2	3	4 : 13	4	3	2	6	5	1 : 48
6	1	3	5	4	2 : 14	2	4	5	3	1	6 : 47
5	2	1	6	4	3 : 15	3	4	6	1	2	5 : 46
6	5	3	1	2	4 : 16	4	2	1	3	5	6 : 45
2	3	6	4	1	5 : 17	5	1	4	6	3	2 : 44
6	5	2	4	3	1 : 18	1	3	4	2	5	6 : 43
1	6	3	4	2	5 : 19	5	2	4	3	6	1 : 42
2	1	5	4	6	3 : 20	3	6	4	5	1	2 : 41
6	4	1	2	3	5 : 21	5	3	2	1	4	6 : 40
5	3	4	1	6	2 : 22	2	6	1	4	3	5 : 39
6	2	4	5	1	3 : 23	3	1	5	4	2	6 : 38
5	4	3	2	6	1 : 24	1	6	2	3	4	5 : 37
1	3	4	5	6	2 : 25	2	6	5	4	3	1 : 36
4	1	2	6	3	5 : 26	5	3	6	2	1	4 : 35
4	3	1	5	2	6 : 27	6	2	5	1	3	4 : 34
2	4	6	1	5	3 : 28	3	5	1	6	4	2 : 33
4	5	2	3	1	6 : 29	6	1	3	2	5	4 : 32
4	3	6	5	2	1 : 30	1	2	5	6	3	4 : 31

There is a more constructive procedure which can be developed as well. To decide whether or not a number m exists so that an arbitrary permutation is a

Josephus permutation of step size m, we can set up a system of $n-1$ congruences

$$\{m \equiv b_i \pmod{n+1-i} \mid 1 \leq i \leq n-1\}$$

that the step size would have to satisfy. If the system of congruences is solvable, the solution is the unique value of m to assign to the permutation. To build the system of congruences, let b_1 be the position to which 1 is assigned, and b_2 the number of steps (cycling back to the beginning if necessary) from 1 to 2. Take b_3 as the number of steps from 2 to 3, but skip over 1. In general, b_k is the number of steps from $k-1$ to k, skipping over numbers less than k.

For example, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 2 & 5 \end{pmatrix}.$$

would require an m satisfying $m \equiv 1 \pmod 6$, since 1 is in the first position, $m \equiv 4 \pmod 5$, since we step from 1 to 6 to 3 to 4 to get to 2, $m \equiv 3 \pmod 4$, stepping from 2 to 5 to 6 (skipping 1) to reach 3, $m \equiv 1 \pmod 3$, since 3 is adjacent to 4, and $m \equiv 1 \pmod 2$, since we skip 2 between 4 and 5.

This system is satisfied by $m \equiv 19 \pmod{60}$, and indeed 1 6 3 4 2 5 is the 19th entry in the table above.

On the other hand, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix}$$

would have to be associated with an m satisfying $m \equiv 1 \pmod 6$, $m \equiv 5 \pmod 5$, $m \equiv 2 \pmod 4$, $m \equiv 1 \pmod 3$, and $m \equiv 1 \pmod 2$. No such m exists since the congruences (mod 4) and (mod 2) are inconsistent, and the ordered set corresponding to this permutation, 1 6 3 4 5 2, does not appear in the table.

Theorem 2. *If step size m generates the ordered set*

$$Z_n^{(m)} = \{a_1, a_2, \ldots, a_n\},$$

then step size $l(n) + 1 - m$ generates the ordered set

$$Z_n^{(l(n)+1-m)} = \{a_n, a_{n-1}, \ldots, a_2, a_1\}.$$

Proof: We generate the set of congruences satisfied by m

$$\{m \equiv b_i \pmod{n+1-i} \mid 1 \leq i \leq n-1\}.$$

Since m exists, this set of congruences has a solution which is unique (mod $l(n)$). We can interpret a negative step size as counting from right to left in the set of congruences

$$\{m^* \equiv -b_i \pmod{n+1-i} \mid 1 \leq i \leq n-1\}.$$

and this set of congruences is satisfied by $m^* \equiv -m \equiv l(n) - m \pmod{l(n)}$. Shifting from $l(n) - m$ to $l(n) - m + 1 = l(n) - (m-1)$ moves the a_i entry from the left end to the right, and counting backwards then rebuilds the entire ordered set from right to left.

For $n = 2$ and $n = 3$ the set of Josephus permutations is all of the symmetric groups S_2 and S_3. For 4 and 5 the set coincides with the alternating groups A_4 and A_5. In contrast to these nice algebraic structures, for $n = 6$ the set of Josephus permutations is closed under neither products nor inverses. We can define a different binary operation for two Josephus permutations by adding the step sizes associated with each (mod $l(n)$) and interpreting their "product" as that Josephus permutation associated with the sum of step sizes. However, this operation does not seem to have many ties with a more conventional permutation product.

References

1. W. Ahrens, "Mathematische Uterhaltungen und Spiele", Leipzig, 1918, pp. 118–169.
2. C.G. Bachet, "Problèmes Plaisants et Delectables qui se font par les Nombres", 1612, p. 174.
3. A. Booth, *Idiot's roulette revisited*, Fibonacci Quarterly **13** (1975), 181–184.
4. E. Busche, *Euber die Schubert'sche Lösungen eines Bachet'schen Problems*, Math. Ann. **47** (1896), 105–112.
5. W.W. Rouse Ball and H.S.M. Coxeter, "Mathematical Recreations and Essays", Toronto, 1972, pp. 32–36.
6. A.P. Domóryad (translated by Halina Moss), "Mathematical Games and Pastimes", Pergamon Press, The Macmillan Company, New York, 1964, pp. 124–126.
7. L. Euler, *Observationes circa novum et singulare progressionum genus*, Opera Omnia Series Prima, Opera Mathematica **7** (MCMXXIII), 246–261.
8. F. Jakóbczyk, *On the generalized Josephus problem*, Glasgow Mathematical Journal **14** (1973), 168–173.
9. Flavius Josephus (translated by H. St. Thackeray), "De Bello Judaico (The Jewish War), Book III", Heinemann, 1927, pp. 341–360 and 387–391.
10. D. Knuth, "The Art of Computer Programming, v. 1 Fundamental Algorithms", Addison-Wesley, Reading, Massachusetts, 1968, pp. 158–159 and 181.
11. R.A. Rankin, *Aireamh Muinntir Fhinn is Dhubhain, agus sgeul Iosephuis is an dà fhichead Iudhaich*, Proc. Roy. Irish Acad. Sec. A **52** (1948), 87–93.
12. H. Schubert, "Zwolf Geduldspiele (neue ausgabe)", Leipzig, 1899, pp. 120–132.
13. P.G. Tait, *On the generalization of the Josephus problem*, Collected Scientific Papers **II** (1900), 432–435, Cambridge.
14. D. Woodhouse, *The extended Josephus problem*, Revista Math. Hisp.-Amer. (4) **33** (1973), 207–218.
15. S.L. Zabell, *Letter to the editor*, Fibonacci Quarterly **14** (1976), p. 48 and 51.