The Josephus Problem: Once More Around

PETER SCHUMER
Department of Mathematics and Computer Science
Middlebury College
Middlebury, VT 05753
schumer@middlebury.edu

The Jewish soldier and historian Josephus Flavius (ca. 37 CE–ca. 95 CE) lived an exciting and tumultuous life and inspired an interesting set of mathematical problems.

Born in Jerusalem, Joseph ben Matthias studied Hebrew and Greek literature as a young child and then spent three years (from the ages of 16 to 19) living an ascetic lifestyle with a fellow hermit in the desert. After further study as a member of the Pharisee sect, he served as delegate to Nero, was chosen governor of Galilee, and rose to the rank of general to help lead the Jewish revolt against Rome in the year 66.

A year later, he was a member of the resistance at the siege of Jotapata that held out for 47 days. According to Josephus [**5**], the doomed soldiers decided to take their own lives rather than be captured by the Romans and suffer an uncertain and inglorious future. Josephus exclaimed, "Let us commit our mutual deaths to determination by lot. He whom the lot falls to first, let him be killed by him that hath the second lot, and thus fortune shall make its progress through us all." By chance or fate or providence, "[Josephus] with another was left to last. And as [Josephus] was very desirous neither to be condemned to the lot, nor, if he had been left to the last, to imbrue his right hand in the blood of his countryman, [Josephus] persuaded him to trust the Roman assurances, and to live as well as himself" [**5**]. Josephus surrendered to Vespasian, traveled extensively with him, and served under Vespasian when the latter became emperor. Josephus also served under the next emperor, Titus, the son of Vespasian, and took his family name of Flavius as his own.

Josephus was in Jerusalem (as a Roman citizen) during the bloodiest battles in the year 70, traveled to Rome for the beginning of the construction of the Coliseum, survived a tragic ship wreck, was married at least three times, and lived a life full of excitement and intrigues. More importantly, he wrote several books including *A History of the Jewish War*, *Contra Apionem* (a response to the anti-Semitic agitator Apion), *Antiquities of the Jews*, and an *Autobiography*.

Differing accounts and new problems

The details of exactly how Josephus's life was spared vary greatly from one source to another. In [**4**] it is stated, "In the Jewish revolt against Rome, Josephus and thirty-nine of his comrades were holding out against the Romans in a cave. With defeat imminent, they resolved that, like the rebels at Masada, they would rather die than be slaves to the Romans. They decided to arrange themselves in a circle. One man was designated as number one, and they proceeded clockwise around the circle of forty men, killing every seventh man. Josephus ... instantly figured out where he ought to sit to be the last to go." (You may wish to verify that he should place himself in position number 24.) In another source [**6**], there are 41 men and every third man in turn is killed. Josephus must figure out immediately where he and a close friend must stand to be the last two chosen. (In this case, the solution is to stand in positions 16 and 31.)

A Medieval version of the "Josephus problem" is recounted [**6**] in which "15 Turks and 15 Christians are on board a storm-ridden ship which is certain to sink unless half the passengers are thrown overboard." All 30 stand in a circle and decide that every ninth person will be tossed to sea. The problem is to determine where the Christians should stand to ensure that all the Turks are first to go.

The most intricate variation of the Josephus problem appears in the Japanese text, *Treatise on Large and Small Numbers* (1627), by Yoshida Koyu. According to [**1**], in this version of the problem there is a family of 30 children, half from a former marriage. To choose one child to inherit the parent's estate, they are arranged in a circle with every tenth child eliminated. The current wife arranges things so that all fifteen children from the first marriage are taken out first. However, after fourteen children are thus eliminated, the father catches on and decides to reverse the order and count in a counterclockwise direction. Even so, a child from the first marriage is eventually chosen.

Some version of the mathematical Josephus problem dates back to Abraham ibn Ezra (ca. 1092–1167), the prolific Jewish scholar and author of works on astrology, the cabala, philosophy, and mathematics. As reported by Smith [**7**], a work from this period entitled *Ta'hbula* contains the Josephus problem and is presumed to be written by Abraham ibn Ezra. Even so, despite the antiquity of the problem, not much attention was paid to mathematical versions of the Josephus problem until the late nineteenth century and scant reference is made to this intriguing problem in modern textbooks.

One very notable exception is a text by Graham, Knuth, and Patashnik, *Concrete Mathematics: A Foundation for Computer Science* [**3**], which makes a thorough study of the "standard" Josephus problem and then extends it in order to discuss general recurrence relations. The standard Josephus problem is to determine where the last survivor stands if there are n people to start and every second person is eliminated. If we let $J(n)$ be the position of the last survivor, the result is that if $n = 2^a + t$, where $0 \leq t < 2^a$, then $J(n) = 2t + 1$. The proof is as elegant as the result and is a very nice application of mathematical induction.

More generally (and less violently), suppose n people numbered one through n stand around a circle. Person number q knows some gossip and tells it to the person q spaces ahead clockwise around the circle, who then tells it to the next person remaining q spaces ahead, etc. In fact, q may be larger than n, in which case the person numbered d is actually numbered d (modulo n). Here we let $J(n, q)$ denote the position of the last person to hear the latest scoop. (So for example, $J(n) = J(n, 2)$.) Calculation of $J(n, q)$ for various values of n and q can be time-consuming and there doesn't appear to be a nice closed formula in general. However, the following result is most useful.

PROPOSITION 1. *For* $n \geq 1$, $q \geq 1$, $J(n+1, q) \equiv J(n, q) + q \pmod{n+1}$.

Proof. Consider $n+1$ people in a circle with every qth being eliminated in turn. The first person eliminated is person $q \pmod{n+1}$. Now we have reduced the problem to the $J(n, q)$ problem, except that the people are numbered $q+1$, $q+2$, etc. rather than 1, 2, etc. Hence, $J(n+1, q) \equiv J(n, q) + q \pmod{n+1}$. ■

For the standard Josephus problem, $q = 2$, and so Proposition 1 implies that $J(n+1) \equiv J(n) + 2 \pmod{n+1}$, an interesting way to interpret the result stated earlier [**3**]. Note that we use the complete set of residues $\{1, 2, \ldots, n+1\}$ modulo $n+1$.

Here is another example showing the utility of Proposition 1. Suppose we wish to make a chart of $J(n, 5)$ for various values of n, starting with 1. We do not need to draw circle after circle (in some sense reinventing the wheel), one for each successive value of n. Instead, since $J(1, 5) = 1$, we can apply Proposition 1 repeatedly to obtain $J(2, 5) \equiv 1 + 5 \equiv 2 \pmod 2$, $J(3, 5) \equiv 2 + 5 \equiv 1 \pmod 3$, $J(4, 5) \equiv 1 + 5 \equiv 2 \pmod 4$, and so on. See TABLE 1.

TABLE 1:

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

Proposition 1 can be easily extended. Let $J(n, q, k)$ denote the position of the kth from last person to be chosen when there are n people and every qth person is eliminated. So $J(n, q, 1) = J(n, q)$. Then

PROPOSITION 2. *For* $n \geq 1$, $q \geq 1$: $J(n+1, q, k) \equiv J(n, q, k) + q (\text{mod}\, n+1)$.

The proof is identical to the proof of Proposition 1.

By way of illustration, TABLE 2 gives the positions of the second from last person to be eliminated when $q = 3$.

TABLE 2:

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

Josephus permutations

There are a host of interesting variations and questions relating to the Josephus problem. Let us begin by defining the Josephus permutation $P(n, q)$ as the permutation on the numbers 1 through n created by applying the Josephus elimination procedure to every qth number. Alternatively, we can think of this as a "Josephus shuffle" where we take n cards numbered 1 through n and place every qth card face down on a table. The resulting ordering of the cards is the appropriate Josephus permutation.

For example,

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

$$P(8,9) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 6 & 4 & 5 & 2 & 7 & 8 \end{pmatrix}.$$

Are all permutations of 1 to n realizable as Josephus permutations for appropriate q? A simple counting argument shows otherwise. Of course there are $n!$ distinct permutations of the numbers $1, \ldots, n$. However, there are precisely $L(n) = \text{lcm}[1, 2, 3, \ldots, n]$ distinct Josephus permutations. To see this note that $P(n, q) = P(n, q + L(n))$ since at each step (say k) of the elimination $(1 \leq k \leq n)$, we simply spin around the circle $L(n)/(n+1-k)$ times before moving q places beyond our previous position. Furthermore, if $q \neq q' (\text{mod}\, L(n))$, then $P(n, q)$ is not the same as $P(n, q')$. To see this note that there is a k with $1 \leq k \leq n$ such that $q \neq q' (\text{mod}\, k)$. But then on the $(n + 1 - k)$th step with k people remaining, $P(n, q)$ and $P(n, q')$ will differ. In any event, since $n! > L(n)$ for all $n > 3$, there are some permutations which are not Josephus permutations.

More concretely, notice that $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ is not a Josephus permutation $J(4, q)$ for any q. If it were, then $q \equiv 2 (\text{mod}\, 4)$, $q \equiv 1 (\text{mod}\, 3)$, and $q \equiv 1 (\text{mod}\, 2)$. But the first and third congruences would imply that q were simultaneously even and odd respectively, a contradiction.

Subsets marked for elimination

Other variations of the Josephus problem involve eliminating a prescribed half of the participants first. For example, if n is even, say $n = 2k$, can we eliminate the first k people leaving the second k intact? This is easy of course—just let $q = 1$.

Well then, given $n = 2k$ people, can we find a value of q that eliminates the second half of the circle first? This is not as simple, but if we let

$$q = L(n) = \operatorname{lcm}[1, 2, \ldots, n], \quad \text{then} \quad P(n, q) = \begin{pmatrix} 1 & 2 & \cdots & 2k-1 & 2k \\ 2k & 2k-1 & \cdots & 2 & 1 \end{pmatrix}$$

and so the people are eliminated in reverse order, thus removing the second half of the circle first.

With n even, can we eliminate all the even-numbered people first without disturbing any of the odd-numbered people? Again the solution is straightforward, just let $q = 2$, as we have discussed previously.

But what if $n = 2k$ and we want to eliminate all the odd-numbered people first? This is more interesting. If we want to eliminate the odd-numbered people in ascending order, then for $n = 4$, we immediately discover $P(4, 5) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{smallmatrix}\right)$. But if $P(6, q)$ were to be of the form $P(6, q) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & E & E & E \end{smallmatrix}\right)$ where E stands for an unspecified even number, it must be the case that $q \equiv 1 \pmod 6$, $q \equiv 2 \pmod 5$, and $q \equiv 2 \pmod 4$. Then q is both odd and even, an impossibility. Yet we can still eliminate the odd numbers first as demonstrated by $P(6, 19) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 6 & 2 \end{smallmatrix}\right)$. Similarly, one can discover "by hand" that $P(8, 27) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 7 & 4 & 2 & 6 & 8 \end{smallmatrix}\right)$ and $P(10, 87) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 3 & 1 & 5 & 9 & 2 & 8 & 6 & 10 & 4 \end{smallmatrix}\right)$. In fact, we have given the smallest value of q that does the trick for each appropriate n. Since there are $k!$ ways to permute the k odd numbers $1, 3, 5, \ldots, 2k-1$, and many permutations lead to contradictory congruences for q, the situation quickly becomes computationally more difficult. Even so, let's go a bit further.

With some work, for the case $n = 12$, we discover that $q \equiv 5 \pmod{12}$, $q \equiv 8 \pmod{11}$, $q \equiv 5 \pmod{10}$, $q \equiv 2 \pmod 9$, $q \equiv 5 \pmod 8$, and $q \equiv 5 \pmod 7$ is consistent in that it follows that $q \equiv 1 \pmod 2$, $q \equiv 2 \pmod 3$, and $q \equiv 1 \pmod 4$. The Chinese remainder theorem guarantees a unique solution modulo $\operatorname{lcm}[12, 11, 10, 9, 8, 7] = L(12) = 27{,}720$. In fact, $q = 16{,}805$ works. The resulting permutation is

$$P(12, 16805) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 1 & 7 & 9 & 3 & 11 & 8 & 6 & 10 & 2 & 4 & 12 \end{pmatrix}.$$

Similarly, for the case $n = 14$, requiring $q \equiv 13 \pmod{14}$, $q \equiv 8 \pmod{13}$, $q \equiv 9 \pmod{12}$, $q \equiv 2 \pmod{11}$, $q \equiv 5 \pmod{10}$, $q \equiv 3 \pmod 9$, and $q \equiv 1 \pmod 4$ leads to a consistent set of simultaneous congruences that together eliminate all odd numbered positions first. Here we get $q = 167{,}565 \pmod{360{,}360}$. The resulting permutation is

$$P(14, 167565) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 13 & 7 & 3 & 5 & 11 & 1 & 9 & 6 & 12 & 10 & 14 & 8 & 2 & 4 \end{pmatrix}.$$

In the last two examples, there was no guarantee that the values of q found were the smallest values that would eliminate all the odd numbers first. My colleague at Middlebury College, Frank Swenton, made a computer search to find just that. His initial results are shown in TABLE 3.

In fact, there is a complete solution to the problem of eliminating all odd numbers first if we aren't concerned with finding the smallest solution. If $n = 2k$, the

TABLE 3:

n	smallest q that eliminates odds first
2	1
4	5
6	19
8	27
10	87
12	989
14	3,119
16	5,399
18	8,189
20	99,663
22	57,455
24	222,397
26	2,603,047
28	8,476,649
30	117,917,347
32	290,190,179
34	360,064,247
36	1,344,262,919
38	3,181,391,639
40	? (larger than 10 billion)

idea is to find a value of q for which $q \equiv -1 (\bmod 2k), q \equiv -1 (\bmod 2k-1)$, $q \equiv -1 (\bmod 2k-2), \ldots, q \equiv -1 (\bmod k+1)$. Such a value of q would have the effect of eliminating all the odd numbers in descending order beginning with $2k-1$ before eliminating any even numbers.

PROPOSITION 3. *Given $n = 2k$, let $q = L(n) - 1$ where $L(n) = \operatorname{lcm}[1, 2, \ldots, n]$. Then*

$$P(n, q) = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & 2k \\ 2k-1 & 2k-3 & \cdots & 1 & E & \cdots & E \end{pmatrix}.$$

Proof. Let d denote the dth stage of the Josephus process for $1 \leq d \leq k$. We use induction on d. The first number eliminated is $2k-1$ and so the result holds for $d = 1$. Assume it holds for all values up to some value d. At this point we last eliminated the odd number $2k - 2d + 1$, all larger odd numbers have been eliminated, and all other numbers between 1 and $2k$ inclusive remain. The qth number is now two places behind the last number removed and so the $(d+1)$st number eliminated is $2k - 2(d+1) + 1$ as required. ■

For example, if $n = 16$ then $q = L(16) - 1 = 720{,}719$ and

$$P(16, 720719) =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 15 & 13 & 11 & 9 & 7 & 5 & 3 & 1 & 14 & 10 & 6 & 2 & 12 & 4 & 8 & 16 \end{pmatrix}.$$

Of course the even-numbered people might collapse from exhaustion before ever being chosen.

Another interesting question is this: Given n (the total number of people) and m (the position you find yourself), is there always a q for which $J(n, q) = m$? In other words, can you always save yourself if you are allowed to specify the value of q?

The answer is yes and the solution can be found in [**3**]. Briefly the solution goes as follows: Let $L(n) = \text{lcm}[1, \ldots, n]$ as before. Assume (for now) that $m > n/2$. By Bertrand's Postulate (conjectured by Bertrand in 1845 and proved by Chebyshev in 1850), there is a prime p with $n/2 < p < n$. Choose q with $q \equiv 1 (\text{mod}\, L/p)$ and $q \equiv m + 1 - n (\text{mod}\, p)$. Since p and L/p are relatively prime, by the Chinese remainder theorem, there is a simultaneous solution mod L. For this value of q, the Josephus process removes the people in the order $1, 2, \ldots, n - p$, and then everyone else starting at person $m + 1$ and moving clockwise around the circle, hence ending at person m. (A slight modification can be made to handle the case when $m \leq n/2$.)

Further circlings

The Josephus problem and its many variants would make a nice chapter in many mathematics and computer science courses. The standard Josephus problem ($q = 2$) has a very elegant interpretation in terms of the binary representation of n. Take a moment to discover it for yourself.

The Josephus permutations are beautiful and concrete examples of permutations in an abstract algebra course. It may be of interest to note that the set of such permutations form a subgroup of the full symmetric group on n for $n = 3$, 4, and 5. However, Frank Swenton again, has confirmed that this pattern does not carry over beyond $n = 5$. Even so, the cycle structure of $P(n, q)$ has been studied for some special cases (see Herstein and Kaplansky [**4**]).

Another question: how many fixed points can we expect in a Josephus permutation (equivalently, a Josephus shuffle)? If we randomly shuffle an n-card deck we expect to have one fixed point, that is, a single card remaining in its original position. To see this, let the random variable X_i be 1 if after shuffling the ith card ends up in the ith place and 0 if the ith card ends up elsewhere. Then the expected value of X_i is simply $E(X_i) = 1(1/n) + 0(1 - 1/n) = 1/n$. Since expectation is linear, $E(\sum X_i) = \sum E(X_i)$, and we have that $E(\sum X_i) = n(1/n) = 1$.

However, in the Josephus shuffle we can set things up so that there are no fixed points for arbitrarily large values of n—just let $q = L(n)$ for even n resulting in the cards' order being completely reversed. In the other direction, the example $P(8, 9)$ given earlier had five fixed points. For $q > 1$ (and not congruent to 1 modulo $L(n)$), how large (relative to n) can the number of fixed points be? There are lots of interesting combinatorial and number theoretic problems circling around for the mathematically brave!

REFERENCES

1. R. Cooke, *The History of Mathematics: A Brief Course*, Wiley, 1997, 247–248.
2. W. Durant, *The Story of Civilization III: Caesar and Christ*, Simon and Schuster, New York, 1944, 543–546.
3. R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison Wesley, 1989, 8–20.
4. I. N. Herstein, I. Kaplansky, *Matters Mathematical*, Harper and Row, 1974, 121–126.
5. F. Josephus, *The Great Roman-Jewish War:* A.D. *66–70*, Peter Smith, Gloucester, 1970, 138–139.
6. J. R. Newman, *The World of Mathematics* (Vol. 4), Tempus, 1988, 4: 2403–2405.
7. D. E. Smith, *History of Mathematics* (Vol. 1), Dover, 1958, 207–208.