1

Recurrent Problems

THIS CHAPTER EXPLORES three sample problems that give a feel for what's to come. They have two traits in common: They've all been investigated repeatedly by mathematicians; and their solutions all use the idea of *recurrence*, in which the solution to each problem depends on the solutions to smaller instances of the same problem.

1.1 THE TOWER OF HANOI

Raise your hand if you've never seen this. OK, the rest of you can cut to equation (1.1).

Let's look first at a neat little puzzle called the Tower of Hanoi, invented by the French mathematician Edouard Lucas in 1883. We are given a tower of eight disks, initially stacked in decreasing size on one of three pegs:

The objective is to transfer the entire tower to one of the other pegs, moving only one disk at a time and never moving a larger one onto a smaller.

Gold — wow. Are our disks made of concrete?

Lucas [260] furnished his toy with a romantic legend about a much larger Tower of Brahma, which supposedly has 64 disks of pure gold resting on three diamond needles. At the beginning of time, he said, God placed these golden disks on the first needle and ordained that a group of priests should transfer them to the third, according to the rules above. The priests reportedly work day and night at their task. When they finish, the Tower will crumble and the world will end.

It's not immediately obvious that the puzzle has a solution, but a little thought (or having seen the problem before) convinces us that it does. Now the question arises: What's the best we can do? That is, how many moves are necessary and sufficient to perform the task?

The best way to tackle a question like this is to generalize it a bit. The Tower of Brahma has 64 disks and the Tower of Hanoi has 8; let's consider what happens if there are n disks.

One advantage of this generalization is that we can scale the problem down even more. In fact, we'll see repeatedly in this book that it's advantageous to LOOK AT SMALL CASES first. It's easy to see how to transfer a tower that contains only one or two disks. And a small amount of experimentation shows how to transfer a tower of three.

The next step in solving the problem is to introduce appropriate notation: NAME AND CONQUER. Let's say that T_n is the minimum number of moves that will transfer n disks from one peg to another under Lucas's rules. Then T_1 is obviously 1, and $T_2 = 3$.

We can also get another piece of data for free, by considering the smallest case of all: Clearly $T_0 = 0$, because no moves at all are needed to transfer a tower of $n = 0$ disks! Smart mathematicians are not ashamed to think small, because general patterns are easier to perceive when the extreme cases are well understood (even when they are trivial).

But now let's change our perspective and try to think big; how can we transfer a large tower? Experiments with three disks show that the winning idea is to transfer the top two disks to the middle peg, then move the third, then bring the other two onto it. This gives us a clue for transferring n disks in general: We first transfer the $n-1$ smallest to a different peg (requiring T_{n-1} moves), then move the largest (requiring one move), and finally transfer the $n-1$ smallest back onto the largest (requiring another T_{n-1} moves). Thus we can transfer n disks (for $n > 0$) in at most $2T_{n-1} + 1$ moves:

$$T_n \leqslant 2T_{n-1} + 1, \qquad \text{for } n > 0.$$

This formula uses '$\leqslant$' instead of '$=$' because our construction proves only that $2T_{n-1} + 1$ moves suffice; we haven't shown that $2T_{n-1} + 1$ moves are necessary. A clever person might be able to think of a shortcut.

But is there a better way? Actually no. At some point we must move the largest disk. When we do, the $n-1$ smallest must be on a single peg, and it has taken at least T_{n-1} moves to put them there. We might move the largest disk more than once, if we're not too alert. But after moving the largest disk for the last time, we must transfer the $n-1$ smallest disks (which must again be on a single peg) back onto the largest; this too requires T_{n-1} moves. Hence

Most of the published "solutions" to Lucas's problem, like the early one of Allardice and Fraser [7], fail to explain why T_n must be $\geqslant 2T_{n-1} + 1$.

$$T_n \geqslant 2T_{n-1} + 1, \qquad \text{for } n > 0.$$

These two inequalities, together with the trivial solution for $n = 0$, yield

$$\begin{aligned} T_0 &= 0\,; \\ T_n &= 2T_{n-1} + 1\,, \qquad \text{for } n > 0. \end{aligned} \tag{1.1}$$

(Notice that these formulas are consistent with the known values $T_1 = 1$ and $T_2 = 3$. Our experience with small cases has not only helped us to discover a general formula, it has also provided a convenient way to check that we haven't made a foolish error. Such checks will be especially valuable when we get into more complicated maneuvers in later chapters.)

Yeah, yeah... I seen that word before.

A set of equalities like (1.1) is called a *recurrence* (a.k.a. recurrence relation or recursion relation). It gives a boundary value and an equation for the general value in terms of earlier ones. Sometimes we refer to the general equation alone as a recurrence, although technically it needs a boundary value to be complete.

The recurrence allows us to compute T_n for any n we like. But nobody really likes to compute from a recurrence, when n is large; it takes too long. The recurrence only gives indirect, local information. A *solution to the recurrence* would make us much happier. That is, we'd like a nice, neat, "closed form" for T_n that lets us compute it quickly, even for large n. With a closed form, we can understand what T_n really is.

So how do we solve a recurrence? One way is to guess the correct solution, then to prove that our guess is correct. And our best hope for guessing the solution is to look (again) at small cases. So we compute, successively, $T_3 = 2\cdot3+1 = 7$; $T_4 = 2\cdot7+1 = 15$; $T_5 = 2\cdot15+1 = 31$; $T_6 = 2\cdot31+1 = 63$. Aha! It certainly looks as if

$$T_n \;=\; 2^n - 1\,, \qquad \text{for } n \geqslant 0. \tag{1.2}$$

At least this works for $n \leqslant 6$.

Mathematical induction is a general way to prove that some statement about the integer n is true for all $n \geqslant n_0$. First we prove the statement when n has its smallest value, n_0; this is called the *basis*. Then we prove the statement for $n > n_0$, assuming that it has already been proved for all values between n_0 and $n-1$, inclusive; this is called the *induction*. Such a proof gives infinitely many results with only a finite amount of work.

Mathematical induction proves that we can climb as high as we like on a ladder, by proving that we can climb onto the bottom rung (the basis) and that from each rung we can climb up to the next one (the induction).

Recurrences are ideally set up for mathematical induction. In our case, for example, (1.2) follows easily from (1.1): The basis is trivial, since $T_0 = 2^0 - 1 = 0$. And the induction follows for $n > 0$ if we assume that (1.2) holds when n is replaced by $n-1$:

$$T_n \;=\; 2T_{n-1} + 1 \;=\; 2(2^{n-1} - 1) + 1 \;=\; 2^n - 1\,.$$

Hence (1.2) holds for n as well. Good! Our quest for T_n has ended successfully.

Of course the priests' task hasn't ended; they're still dutifully moving disks, and will be for a while, because for $n = 64$ there are $2^{64}-1$ moves (about 18 quintillion). Even at the impossible rate of one move per microsecond, they will need more than 5000 centuries to transfer the Tower of Brahma. Lucas's original puzzle is a bit more practical. It requires $2^8 - 1 = 255$ moves, which takes about four minutes for the quick of hand.

The Tower of Hanoi recurrence is typical of many that arise in applications of all kinds. In finding a closed-form expression for some quantity of interest like T_n we go through three stages:

1 Look at small cases. This gives us insight into the problem and helps us in stages 2 and 3.

2 Find and prove a mathematical expression for the quantity of interest. For the Tower of Hanoi, this is the recurrence (1.1) that allows us, given the inclination, to compute T_n for any n.

What is a proof? "One half of one percent pure alcohol."

3 Find and prove a closed form for our mathematical expression. For the Tower of Hanoi, this is the recurrence solution (1.2).

The third stage is the one we will concentrate on throughout this book. In fact, we'll frequently skip stages 1 and 2 entirely, because a mathematical expression will be given to us as a starting point. But even then, we'll be getting into subproblems whose solutions will take us through all three stages.

Our analysis of the Tower of Hanoi led to the correct answer, but it required an "inductive leap"; we relied on a lucky guess about the answer. One of the main objectives of this book is to explain how a person can solve recurrences *without* being clairvoyant. For example, we'll see that recurrence (1.1) can be simplified by adding 1 to both sides of the equations:

$$\begin{aligned} T_0 + 1 &= 1\,; \\ T_n + 1 &= 2T_{n-1} + 2\,, \qquad \text{for } n > 0. \end{aligned}$$

Now if we let $U_n = T_n + 1$, we have

Interesting: We get rid of the $+1$ in (1.1) by adding, not by subtracting.

$$\begin{aligned} U_0 &= 1\,; \\ U_n &= 2U_{n-1}\,, \qquad \text{for } n > 0. \end{aligned} \tag{1.3}$$

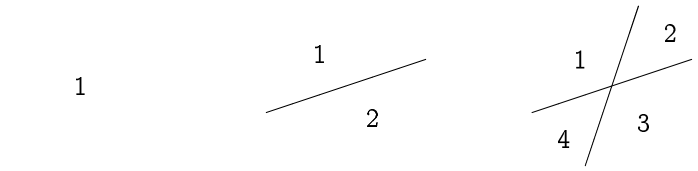
It doesn't take genius to discover that the solution to *this* recurrence is just $U_n = 2^n$; hence $T_n = 2^n - 1$. Even a computer could discover this.

1.2 LINES IN THE PLANE

Our second sample problem has a more geometric flavor: How many slices of pizza can a person obtain by making n straight cuts with a pizza knife? Or, more academically: What is the maximum number L_n of regions defined by n lines in the plane? This problem was first solved in 1826, by the Swiss mathematician Jacob Steiner [338].

(A pizza with Swiss cheese?)

Again we start by looking at small cases, remembering to begin with the smallest of all. The plane with no lines has one region; with one line it has two regions; and with two lines it has four regions:

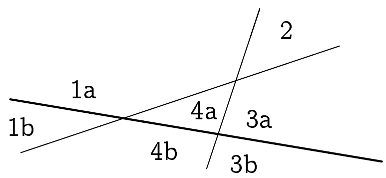


$L_0 = 1$ $\qquad$ $L_1 = 2$ $\qquad$ $L_2 = 4$

(Each line extends infinitely in both directions.)

Sure, we think, $L_n = 2^n$; of course! Adding a new line simply doubles the number of regions. Unfortunately this is wrong. We could achieve the doubling if the nth line would split each old region in two; certainly it can split an old region in at most two pieces, since each old region is convex. (A straight line can split a convex region into at most two new regions, which will also be convex.) But when we add the third line — the thick one in the diagram below — we soon find that it can split at most three of the old regions, no matter how we've placed the first two lines:

A region is convex if it includes all line segments between any two of its points. (That's not what my dictionary says, but it's what mathematicians believe.)



Thus $L_3 = 4 + 3 = 7$ is the best we can do.

And after some thought we realize the appropriate generalization. The nth line (for $n > 0$) increases the number of regions by k if and only if it splits k of the old regions, and it splits k old regions if and only if it hits the previous lines in $k-1$ different places. Two lines can intersect in at most one point. Therefore the new line can intersect the $n-1$ old lines in at most $n-1$ different points, and we must have $k \leqslant n$. We have established the upper bound

$$L_n \leqslant L_{n-1} + n\,, \qquad \text{for } n > 0.$$

Furthermore it's easy to show by induction that we can achieve equality in this formula. We simply place the nth line in such a way that it's not parallel to any of the others (hence it intersects them all), and such that it doesn't go through any of the existing intersection points (hence it intersects them all in different places). The recurrence is therefore

$$\begin{aligned} &L_0 = 1\,; \\ &L_n = L_{n-1} + n\,, \qquad \text{for } n > 0. \end{aligned} \tag{1.4}$$

The known values of L_1, L_2, and L_3 check perfectly here, so we'll buy this.

Now we need a closed-form solution. We could play the guessing game again, but 1, 2, 4, 7, 11, 16, ... doesn't look familiar; so let's try another tack. We can often understand a recurrence by "unfolding" or "unwinding" it all the way to the end, as follows:

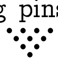
$$\begin{aligned} L_n &= L_{n-1} + n \\ &= L_{n-2} + (n-1) + n \\ &= L_{n-3} + (n-2) + (n-1) + n \\ &\quad\vdots \\ &= L_0 + 1 + 2 + \cdots + (n-2) + (n-1) + n \\ &= 1 \;+\; S_n\,, \qquad \text{where } S_n = 1 + 2 + 3 + \cdots + (n-1) + n. \end{aligned}$$

Unfolding? I'd call this "plugging in."

In other words, L_n is one more than the sum S_n of the first n positive integers.

The quantity S_n pops up now and again, so it's worth making a table of small values. Then we might recognize such numbers more easily when we see them the next time:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
S_n	1	3	6	10	15	21	28	36	45	55	66	78	91	105

These values are also called the *triangular numbers*, because S_n is the number of bowling pins in an n-row triangular array. For example, the usual four-row array  has $S_4 = 10$ pins.

To evaluate S_n we can use a trick that Gauss reportedly came up with in 1786, when he was nine years old [88] (see also Euler [114, part 1, §415]):

It seems a lot of stuff is attributed to Gauss — either he was really smart or he had a great press agent.

$$\begin{array}{rcccccccccccc} S_n &=& 1 &+& 2 &+& 3 &+& \cdots &+& (n-1) &+& n \\ +\,S_n &=& n &+& (n-1) &+& (n-2) &+& \cdots &+& 2 &+& 1 \\ \hline 2S_n &=& (n+1) &+& (n+1) &+& (n+1) &+& \cdots &+& (n+1) &+& (n+1) \end{array}$$

We merely add S_n to its reversal, so that each of the n columns on the right sums to $n+1$. Simplifying,

Maybe he just had a magnetic personality.

$$S_n = \frac{n(n+1)}{2}\,, \qquad \text{for } n \geqslant 0. \tag{1.5}$$

Actually Gauss is often called the greatest mathematician of all time. So it's nice to be able to understand at least one of his discoveries.

OK, we have our solution:

$$L_n = \frac{n(n+1)}{2} + 1, \qquad \text{for } n \geqslant 0. \tag{1.6}$$

As experts, we might be satisfied with this derivation and consider it a proof, even though we waved our hands a bit when doing the unfolding and reflecting. But students of mathematics should be able to meet stricter standards; so it's a good idea to construct a rigorous proof by induction. The key induction step is

$$L_n = L_{n-1} + n = \left(\tfrac{1}{2}(n-1)n + 1\right) + n = \tfrac{1}{2}n(n+1) + 1 .$$

Now there can be no doubt about the closed form (1.6).

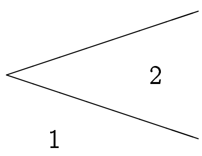
When in doubt, look at the words. Why is it "closed," as opposed to "open"? What image does it bring to mind? Answer: The equation is "closed," not defined in terms of itself — not leading to recurrence. The case is "closed" — it won't happen again. Metaphors are the key.

Incidentally we've been talking about "closed forms" without explicitly saying what we mean. Usually it's pretty clear. Recurrences like (1.1) and (1.4) are not in closed form — they express a quantity in terms of itself; but solutions like (1.2) and (1.6) are. Sums like $1 + 2 + \cdots + n$ are not in closed form — they cheat by using '$\cdots$'; but expressions like $n(n+1)/2$ are. We could give a rough definition like this: An expression for a quantity $f(n)$ is in closed form if we can compute it using at most a fixed number of "well known" standard operations, independent of n. For example, $2^n - 1$ and $n(n+1)/2$ are closed forms because they involve only addition, subtraction, multiplication, division, and exponentiation, in explicit ways.

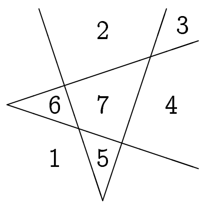
The total number of simple closed forms is limited, and there are recurrences that don't have simple closed forms. When such recurrences turn out to be important, because they arise repeatedly, we add new operations to our repertoire; this can greatly extend the range of problems solvable in "simple" closed form. For example, the product of the first n integers, $n!$, has proved to be so important that we now consider it a basic operation. The formula '$n!$' is therefore in closed form, although its equivalent '$1 \cdot 2 \cdot \ldots \cdot n$' is not.

Is "zig" a technical term?

And now, briefly, a variation of the lines-in-the-plane problem: Suppose that instead of straight lines we use bent lines, each containing one "zig." What is the maximum number Z_n of regions determined by n such bent lines in the plane? We might expect Z_n to be about twice as big as L_n, or maybe three times as big. Let's see:



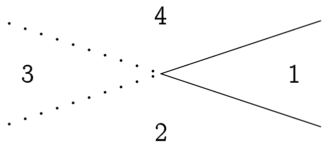
$Z_1 = 2$



$Z_2 = 7$

From these small cases, and after a little thought, we realize that a bent line is like two straight lines except that regions merge when the "two" lines don't extend past their intersection point.

... and a little afterthought...



Regions 2, 3, and 4, which would be distinct with two lines, become a single region when there's a bent line; we lose two regions. However, if we arrange things properly — the zig point must lie "beyond" the intersections with the other lines — that's all we lose; that is, we lose only two regions per line. Thus

Exercise 18 has the details.

$$\begin{aligned} Z_n \;=\; L_{2n} - 2n \;&=\; 2n(2n+1)/2 + 1 - 2n \\ &=\; 2n^2 - n + 1\,, \qquad \text{for } n \geqslant 0. \end{aligned} \tag{1.7}$$

Comparing the closed forms (1.6) and (1.7), we find that for large n,

$$\begin{aligned} L_n \;&\sim\; \tfrac{1}{2}n^2\,, \\ Z_n \;&\sim\; 2n^2\,; \end{aligned}$$

so we get about four times as many regions with bent lines as with straight lines. (In later chapters we'll be discussing how to analyze the approximate behavior of integer functions when n is large. The '$\sim$' symbol is defined in Section 9.1.)

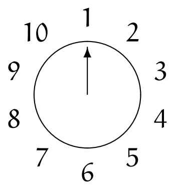
1.3 THE JOSEPHUS PROBLEM

Our final introductory example is a variant of an ancient problem named for Flavius Josephus, a famous historian of the first century. Legend has it that Josephus wouldn't have lived to become famous without his mathematical talents. During the Jewish–Roman war, he was among a band of 41 Jewish rebels trapped in a cave by the Romans. Preferring suicide to capture, the rebels decided to form a circle and, proceeding around it, to kill every third remaining person until no one was left. But Josephus, along with an unindicted co-conspirator, wanted none of this suicide nonsense; so he quickly calculated where he and his friend should stand in the vicious circle.

(Ahrens [5, vol. 2] and Herstein and Kaplansky [187] discuss the interesting history of this problem. Josephus himself [197] is a bit vague.)

... thereby saving his tale for us to hear.

In our variation, we start with n people numbered 1 to n around a circle, and we eliminate every *second* remaining person until only one survives. For example, here's the starting configuration for $n = 10$:



The elimination order is 2, 4, 6, 8, 10, 3, 7, 1, 9, so 5 survives. The problem: Determine the survivor's number, $J(n)$.

Here's a case where $n = 0$ makes no sense.

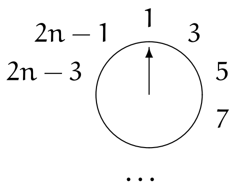
We just saw that $J(10) = 5$. We might conjecture that $J(n) = n/2$ when n is even; and the case $n = 2$ supports the conjecture: $J(2) = 1$. But a few other small cases dissuade us — the conjecture fails for $n = 4$ and $n = 6$.

n	1	2	3	4	5	6
$J(n)$	1	1	3	1	3	5

Even so, a bad guess isn't a waste of time, because it gets us involved in the problem.

It's back to the drawing board; let's try to make a better guess. Hmmm ... $J(n)$ always seems to be odd. And in fact, there's a good reason for this: The first trip around the circle eliminates all the even numbers. Furthermore, if n itself is an even number, we arrive at a situation similar to what we began with, except that there are only half as many people, and their numbers have changed.

So let's suppose that we have $2n$ people originally. After the first go-round, we're left with



and 3 will be the next to go. This is just like starting out with n people, except that each person's number has been doubled and decreased by 1. That is,

This is the tricky part: We have $J(2n) = \mathit{newnumber}(J(n))$, where $\mathit{newnumber}(k) = 2k - 1$.

$$J(2n) \;=\; 2J(n) - 1\,, \qquad \text{for } n \geqslant 1.$$

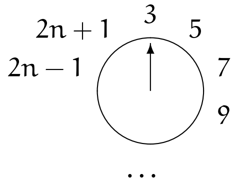
We can now go quickly to large n. For example, we know that $J(10) = 5$, so

$$J(20) \;=\; 2J(10) - 1 \;=\; 2\cdot 5 - 1 \;=\; 9\,.$$

Similarly $J(40) = 17$, and we can deduce that $J(5\cdot 2^m) = 2^{m+1} + 1$.

But what about the odd case? With $2n+1$ people, it turns out that person number 1 is wiped out just after person number $2n$, and we're left with

Odd case? Hey, leave my brother out of it.



Again we almost have the original situation with n people, but this time their numbers are doubled and *increased* by 1. Thus

$$J(2n+1) \;=\; 2J(n)+1\,, \qquad \text{for } n \geqslant 1.$$

Combining these equations with $J(1)=1$ gives us a recurrence that defines J in all cases:

$$\begin{aligned} J(1) &= 1\,; \\ J(2n) &= 2J(n)-1\,, && \text{for } n \geqslant 1; \\ J(2n+1) &= 2J(n)+1\,, && \text{for } n \geqslant 1. \end{aligned} \qquad (1.8)$$

Instead of getting $J(n)$ from $J(n-1)$, this recurrence is much more "efficient," because it reduces n by a factor of 2 or more each time it's applied. We could compute $J(1000000)$, say, with only 19 applications of (1.8). But still, we seek a closed form, because that will be even quicker and more informative. After all, this is a matter of life or death.

Our recurrence makes it possible to build a table of small values very quickly. Perhaps we'll be able to spot a pattern and guess the answer.

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

Voilà! It seems we can group by powers of 2 (marked by vertical lines in the table); $J(n)$ is always 1 at the beginning of a group and it increases by 2 within a group. So if we write n in the form $n = 2^m + l$, where 2^m is the largest power of 2 not exceeding n and where l is what's left, the solution to our recurrence seems to be

$$J(2^m+l) \;=\; 2l+1\,, \qquad \text{for } m \geqslant 0 \text{ and } 0 \leqslant l < 2^m. \qquad (1.9)$$

(Notice that if $2^m \leqslant n < 2^{m+1}$, the remainder $l = n - 2^m$ satisfies $0 \leqslant l < 2^{m+1} - 2^m = 2^m$.)

We must now prove (1.9). As in the past we use induction, but this time the induction is on m. When $m = 0$ we must have $l = 0$; thus the basis of

But there's a simpler way! The key fact is that $J(2^m) = 1$ for all m, and this follows immediately from our first equation,

$J(2n) = 2J(n)-1.$

Hence we know that the first person will survive whenever n is a power of 2. And in the general case, when $n = 2^m + l$, the number of people is reduced to a power of 2 after there have been l executions. The first remaining person at this point, the survivor, is number $2l+1$.

(1.9) reduces to $J(1) = 1$, which is true. The induction step has two parts, depending on whether l is even or odd. If $m > 0$ and $2^m + l = 2n$, then l is even and

$$J(2^m + l) \;=\; 2J(2^{m-1} + l/2) - 1 \;=\; 2(2l/2 + 1) - 1 \;=\; 2l + 1\,,$$

by (1.8) and the induction hypothesis; this is exactly what we want. A similar proof works in the odd case, when $2^m + l = 2n + 1$. We might also note that (1.8) implies the relation

$$J(2n+1) - J(2n) \;=\; 2.$$

Either way, the induction is complete and (1.9) is established.

To illustrate solution (1.9), let's compute $J(100)$. In this case we have $100 = 2^6 + 36$, so $J(100) = 2 \cdot 36 + 1 = 73$.

Now that we've done the hard stuff (solved the problem) we seek the soft: Every solution to a problem can be generalized so that it applies to a wider class of problems. Once we've learned a technique, it's instructive to look at it closely and see how far we can go with it. Hence, for the rest of this section, we will examine the solution (1.9) and explore some generalizations of the recurrence (1.8). These explorations will uncover the structure that underlies all such problems.

Powers of 2 played an important role in our finding the solution, so it's natural to look at the radix 2 representations of n and $J(n)$. Suppose n's binary expansion is

$$n \;=\; (b_m\, b_{m-1} \ldots b_1\, b_0)_2\,;$$

that is,

$$n \;=\; b_m 2^m \;+\; b_{m-1} 2^{m-1} \;+\; \cdots \;+\; b_1 2 \;+\; b_0\,,$$

where each b_i is either 0 or 1 and where the leading bit b_m is 1. Recalling that $n = 2^m + l$, we have, successively,

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

(The last step follows because $J(n) = 2l + 1$ and because $b_m = 1$.) We have proved that

$$J\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) \;=\; (b_{m-1} \ldots b_1\, b_0\, b_m)_2\,; \tag{1.10}$$

that is, in the lingo of computer programming, we get $J(n)$ from n by doing a one-bit cyclic shift left! Magic. For example, if $n = 100 = (1100100)_2$ then $J(n) = J\big((1100100)_2\big) = (1001001)_2$, which is $64+8+1 = 73$. If we had been working all along in binary notation, we probably would have spotted this pattern immediately.

If we start with n and iterate the J function $m+1$ times, we're doing $m+1$ one-bit cyclic shifts; so, since n is an $(m{+}1)$-bit number, we might expect to end up with n again. But this doesn't quite work. For instance if $n = 13$ we have $J\big((1101)_2\big) = (1011)_2$, but then $J\big((1011)_2\big) = (111)_2$ and the process breaks down; the 0 disappears when it becomes the leading bit. In fact, $J(n)$ must always be $\leqslant n$ by definition, since $J(n)$ is the survivor's number; hence if $J(n) < n$ we can never get back up to n by continuing to iterate.

("Iteration" here means applying a function to itself.)

Repeated application of J produces a sequence of decreasing values that eventually reach a "fixed point," where $J(n) = n$. The cyclic shift property makes it easy to see what that fixed point will be: Iterating the function enough times will always produce a pattern of all 1's whose value is $2^{\nu(n)} - 1$, where $\nu(n)$ is the number of 1 bits in the binary representation of n. Thus, since $\nu(13) = 3$, we have

$$\overbrace{J(J(\ldots J}^{\text{2 or more } J\text{'s}}(13)\ldots)) \;=\; 2^3 - 1 \;=\; 7\,;$$

similarly

$$\overbrace{J(J(\ldots J}^{\text{8 or more}}((101101101101011)_2)\ldots)) \;=\; 2^{10} - 1 \;=\; 1023\,.$$

Curious, but true.

Curiously enough, if M is a compact C^∞ n-manifold ($n > 1$), there exists a differentiable immersion of M into $\mathbf{R}^{2n-\nu(n)}$ but not necessarily into $\mathbf{R}^{2n-\nu(n)-1}$. I wonder if Josephus was secretly a topologist?

Let's return briefly to our first guess, that $J(n) = n/2$ when n is even. This is obviously not true in general, but we can now determine exactly when it *is* true:

$$\begin{aligned} J(n) &= n/2\,,\\ 2l+1 &= (2^m + l)/2\,,\\ l &= \tfrac{1}{3}(2^m - 2)\,. \end{aligned}$$

If this number $l = \frac{1}{3}(2^m - 2)$ is an integer, then $n = 2^m + l$ will be a solution, because l will be less than 2^m. It's not hard to verify that $2^m - 2$ is a multiple of 3 when m is odd, but not when m is even. (We will study such things in Chapter 4.) Therefore there are infinitely many solutions to the equation

$J(n) = n/2$, beginning as follows:

m	l	$n = 2^m + l$	$J(n) = 2l + 1 = n/2$	n (binary)
1	0	2	1	10
3	2	10	5	1010
5	10	42	21	101010
7	42	170	85	10101010

Notice the pattern in the rightmost column. These are the binary numbers for which cyclic-shifting one place left produces the same result as ordinary-shifting one place right (halving).

OK, we understand the J function pretty well; the next step is to generalize it. What would have happened if our problem had produced a recurrence that was something like (1.8), but with different constants? Then we might not have been lucky enough to guess the solution, because the solution might have been really weird. Let's investigate this by introducing constants α, β, and γ and trying to find a closed form for the more general recurrence

Looks like Greek to me.

$$\begin{aligned} f(1) &= \alpha\,; \\ f(2n) &= 2f(n) + \beta\,, && \text{for } n \geqslant 1; \\ f(2n+1) &= 2f(n) + \gamma\,, && \text{for } n \geqslant 1. \end{aligned} \tag{1.11}$$

(Our original recurrence had $\alpha = 1$, $\beta = -1$, and $\gamma = 1$.) Starting with $f(1) = \alpha$ and working our way up, we can construct the following general table for small values of n:

$$\begin{array}{c|l} n & f(n) \\ \hline 1 & \alpha \\ \hline 2 & 2\alpha + \beta \\ 3 & 2\alpha \qquad\; + \gamma \\ \hline 4 & 4\alpha + 3\beta \\ 5 & 4\alpha + 2\beta + \gamma \\ 6 & 4\alpha + \beta + 2\gamma \\ 7 & 4\alpha \qquad\; + 3\gamma \\ \hline 8 & 8\alpha + 7\beta \\ 9 & 8\alpha + 6\beta + \gamma \end{array} \tag{1.12}$$

It seems that α's coefficient is n's largest power of 2. Furthermore, between powers of 2, β's coefficient decreases by 1 down to 0 and γ's increases by 1 up from 0. Therefore if we express $f(n)$ in the form

$$f(n) \;=\; A(n)\,\alpha \;+\; B(n)\,\beta \;+\; C(n)\,\gamma\,, \tag{1.13}$$

by separating out its dependence on α, β, and γ, it seems that

$$\begin{aligned} A(n) &= 2^m\,; \\ B(n) &= 2^m - 1 - l\,; \\ C(n) &= l\,. \end{aligned} \tag{1.14}$$

Here, as usual, $n = 2^m + l$ and $0 \leqslant l < 2^m$, for $n \geqslant 1$.

It's not terribly hard to prove (1.13) and (1.14) by induction, but the calculations are messy and uninformative. Fortunately there's a better way to proceed, by choosing particular values and then combining them. Let's illustrate this by considering the special case $\alpha = 1$, $\beta = \gamma = 0$, when $f(n)$ is supposed to be equal to $A(n)$: Recurrence (1.11) becomes

Hold onto your hats, this next part is new stuff.

$$\begin{aligned} A(1) &= 1\,; \\ A(2n) &= 2A(n)\,, \qquad \text{for } n \geqslant 1; \\ A(2n+1) &= 2A(n)\,, \qquad \text{for } n \geqslant 1. \end{aligned}$$

Sure enough, it's true (by induction on m) that $A(2^m + l) = 2^m$.

Next, let's use recurrence (1.11) and solution (1.13) *in reverse*, by starting with a simple function $f(n)$ and seeing if there are any constants (α, β, γ) that will define it. Plugging the constant function $f(n) = 1$ into (1.11) says that

A neat idea!

$$\begin{aligned} 1 &= \alpha; \\ 1 &= 2\cdot 1 + \beta; \\ 1 &= 2\cdot 1 + \gamma; \end{aligned}$$

hence the values $(\alpha, \beta, \gamma) = (1, -1, -1)$ satisfying these equations will yield $A(n) - B(n) - C(n) = f(n) = 1$. Similarly, we can plug in $f(n) = n$:

$$\begin{aligned} 1 &= \alpha; \\ 2n &= 2\cdot n + \beta; \\ 2n+1 &= 2\cdot n + \gamma; \end{aligned}$$

These equations hold for all n when $\alpha = 1$, $\beta = 0$, and $\gamma = 1$, so we don't need to prove by induction that these parameters will yield $f(n) = n$. We already *know* that $f(n) = n$ will be the solution in such a case, because the recurrence (1.11) uniquely defines $f(n)$ for every value of n.

And now we're essentially done! We have shown that the functions $A(n)$, $B(n)$, and $C(n)$ of (1.13), which solve (1.11) in general, satisfy the equations

$$\begin{aligned} A(n) &= 2^m\,, \qquad \text{where } n = 2^m + l \text{ and } 0 \leqslant l < 2^m; \\ A(n) - B(n) - C(n) &= 1\,; \\ A(n) + C(n) &= n\,. \end{aligned}$$

Our conjectures in (1.14) follow immediately, since we can solve these equations to get $C(n) = n - A(n) = l$ and $B(n) = A(n) - 1 - C(n) = 2^m - 1 - l$.

Beware: The authors are expecting us to figure out the idea of the repertoire method from seat-of-the-pants examples, instead of giving us a top-down presentation. The method works best with recurrences that are "linear," in the sense that the solutions can be expressed as a sum of arbitrary parameters multiplied by functions of n, as in (1.13). Equation (1.13) is the key.

This approach illustrates a surprisingly useful *repertoire method* for solving recurrences. First we find settings of general parameters for which we know the solution; this gives us a repertoire of special cases that we can solve. Then we obtain the general case by combining the special cases. We need as many independent special solutions as there are independent parameters (in this case three, for α, β, and γ). Exercises 16 and 20 provide further examples of the repertoire approach.

We know that the original J-recurrence has a magical solution, in binary:

$$J\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) \;=\; (b_{m-1} \ldots b_1\, b_0\, b_m)_2\,, \qquad \text{where } b_m = 1.$$

Does the generalized Josephus recurrence admit of such magic?

Sure, why not? We can rewrite the generalized recurrence (1.11) as

$$\begin{aligned} f(1) &= \alpha\,; \\ f(2n+j) &= 2f(n) + \beta_j\,, \qquad \text{for } j = 0,1 \quad \text{and} \quad n \geqslant 1, \end{aligned} \tag{1.15}$$

if we let $\beta_0 = \beta$ and $\beta_1 = \gamma$. And this recurrence unfolds, binary-wise:

$$\begin{aligned} f\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) &= 2f\big((b_m\, b_{m-1} \ldots b_1)_2\big) + \beta_{b_0} \\ &= 4f\big((b_m\, b_{m-1} \ldots b_2)_2\big) + 2\beta_{b_1} + \beta_{b_0} \\ &\;\;\vdots \\ &= 2^m f\big((b_m)_2\big) + 2^{m-1}\beta_{b_{m-1}} + \cdots + 2\beta_{b_1} + \beta_{b_0} \\ &= 2^m\alpha \,+\, 2^{m-1}\beta_{b_{m-1}} \,+\, \cdots \,+\, 2\beta_{b_1} \,+\, \beta_{b_0}\,. \end{aligned}$$

('relax' = 'destroy')

Suppose we now relax the radix 2 notation to allow arbitrary digits instead of just 0 and 1. The derivation above tells us that

$$f\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) \;=\; (\alpha\, \beta_{b_{m-1}}\, \beta_{b_{m-2}} \ldots \beta_{b_1}\, \beta_{b_0})_2\,. \tag{1.16}$$

Nice. We would have seen this pattern earlier if we had written (1.12) in another way:

I think I get it: The binary representations of $A(n)$, $B(n)$, and $C(n)$ have 1's in different positions.

n	$f(n)$
1	α
2	$2\alpha + \beta$
3	$2\alpha + \gamma$
4	$4\alpha + 2\beta + \beta$
5	$4\alpha + 2\beta + \gamma$
6	$4\alpha + 2\gamma + \beta$
7	$4\alpha + 2\gamma + \gamma$

For example, when $n = 100 = (1100100)_2$, our original Josephus values $\alpha = 1$, $\beta = -1$, and $\gamma = 1$ yield

$$\begin{array}{rcccccccrr} n = & (1 & 1 & 0 & 0 & 1 & 0 & 0\,)_2 & = & 100 \\ \hline f(n) = & (1 & 1 & -1 & -1 & 1 & -1 & -1\,)_2 & & \\ = & +64 & +32 & -16 & -8 & +4 & -2 & -1 & = & 73 \end{array}$$

as before. The cyclic-shift property follows because each block of binary digits $(1\,0\ldots0\,0)_2$ in the representation of n is transformed into

$$(1\,{-1}\,\ldots\,{-1}\,{-1})_2 \;=\; (0\,0\ldots0\,1)_2\,.$$

So our change of notation has given us the compact solution (1.16) to the general recurrence (1.15). If we're really uninhibited we can now generalize even more. The recurrence

$$\begin{aligned} f(j) &= \alpha_j\,, && \text{for } 1 \leqslant j < d; \\ f(dn+j) &= cf(n) + \beta_j\,, && \text{for } 0 \leqslant j < d \quad \text{and} \quad n \geqslant 1, \end{aligned} \tag{1.17}$$

is the same as the previous one except that we start with numbers in radix d and produce values in radix c. That is, it has the radix-changing solution

$$f\big((b_m\,b_{m-1}\ldots b_1\,b_0)_d\big) \;=\; (\alpha_{b_m}\,\beta_{b_{m-1}}\,\beta_{b_{m-2}}\ldots\beta_{b_1}\,\beta_{b_0})_c\,. \tag{1.18}$$

For example, suppose that by some stroke of luck we're given the recurrence

$$\begin{aligned} f(1) &= 34\,, \\ f(2) &= 5\,, \\ f(3n) &= 10f(n) + 76\,, && \text{for } n \geqslant 1, \\ f(3n+1) &= 10f(n) - 2\,, && \text{for } n \geqslant 1, \\ f(3n+2) &= 10f(n) + 8\,, && \text{for } n \geqslant 1, \end{aligned}$$

and suppose we want to compute $f(19)$. Here we have $d = 3$ and $c = 10$. Now $19 = (201)_3$, and the radix-changing solution tells us to perform a digit-by-digit replacement from radix 3 to radix 10. So the leading 2 becomes a 5, and the 0 and 1 become 76 and -2, giving

$$f(19) \;=\; f\big((201)_3\big) \;=\; (5\;76\;{-2})_{10} \;=\; 1258\,,$$

which is our answer.

Thus Josephus and the Jewish–Roman war have led us to some interesting general recurrences.

"There are two kinds of generalizations. One is cheap and the other is valuable. It is easy to generalize by diluting a little idea with a big terminology. It is much more difficult to prepare a refined and condensed extract from several good ingredients."
— G. Pólya [297]

Perhaps this was a stroke of bad luck.

But in general I'm against recurrences of war.

Exercises

Warmups

Please do all the warmups in all the chapters!
— The Mgm't

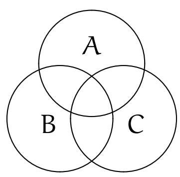
1 All horses are the same color; we can prove this by induction on the number of horses in a given set. Here's how: "If there's just one horse then it's the same color as itself, so the basis is trivial. For the induction step, assume that there are n horses numbered 1 to n. By the induction hypothesis, horses 1 through $n-1$ are the same color, and similarly horses 2 through n are the same color. But the middle horses, 2 through $n-1$, can't change color when they're in different groups; these are horses, not chameleons. So horses 1 and n must be the same color as well, by transitivity. Thus all n horses are the same color; QED." What, if anything, is wrong with this reasoning?

2 Find the shortest sequence of moves that transfers a tower of n disks from the left peg A to the right peg B, if direct moves between A and B are disallowed. (Each move must be to or from the middle peg. As usual, a larger disk must never appear above a smaller one.)

3 Show that, in the process of transferring a tower under the restrictions of the preceding exercise, we will actually encounter every properly stacked arrangement of n disks on three pegs.

4 Are there any starting and ending configurations of n disks on three pegs that are more than $2^n - 1$ moves apart, under Lucas's original rules?

5 A "Venn diagram" with three overlapping circles is often used to illustrate the eight possible subsets associated with three given sets:



Can the sixteen possibilities that arise with four given sets be illustrated by four overlapping circles?

6 Some of the regions defined by n lines in the plane are infinite, while others are bounded. What's the maximum possible number of bounded regions?

7 Let $H(n) = J(n+1) - J(n)$. Equation (1.8) tells us that $H(2n) = 2$, and $H(2n+1) = J(2n+2) - J(2n+1) = \big(2J(n+1)-1\big) - \big(2J(n)+1\big) = 2H(n) - 2$, for all $n \geqslant 1$. Therefore it seems possible to prove that $H(n) = 2$ for all n, by induction on n. What's wrong here?

Homework exercises

8 Solve the recurrence

$$\begin{aligned} Q_0 &= \alpha\,; \qquad Q_1 = \beta\,; \\ Q_n &= (1+Q_{n-1})/Q_{n-2}\,, \qquad \text{for } n>1. \end{aligned}$$

Assume that $Q_n \neq 0$ for all $n \geqslant 0$. *Hint:* $Q_4 = (1+\alpha)/\beta$.

9 Sometimes it's possible to use induction backwards, proving things from n to $n-1$ instead of vice versa! For example, consider the statement

... now that's a horse of a different color.

$$P(n)\ :\qquad x_1 \ldots x_n \leqslant \left(\frac{x_1+\cdots+x_n}{n}\right)^n, \quad \text{if } x_1,\ldots,x_n \geqslant 0.$$

This is true when $n=2$, since $(x_1+x_2)^2 - 4x_1x_2 = (x_1-x_2)^2 \geqslant 0$.

a By setting $x_n = (x_1+\cdots+x_{n-1})/(n-1)$, prove that $P(n)$ implies $P(n-1)$ whenever $n>1$.

b Show that $P(n)$ and $P(2)$ imply $P(2n)$.

c Explain why this implies the truth of $P(n)$ for all n.

10 Let Q_n be the minimum number of moves needed to transfer a tower of n disks from A to B if all moves must be *clockwise* — that is, from A to B, or from B to the other peg, or from the other peg to A. Also let R_n be the minimum number of moves needed to go from B back to A under this restriction. Prove that

$$Q_n = \begin{cases} 0, & \text{if } n=0; \\ 2R_{n-1}+1, & \text{if } n>0; \end{cases} \qquad R_n = \begin{cases} 0, & \text{if } n=0; \\ Q_n+Q_{n-1}+1, & \text{if } n>0. \end{cases}$$

(You need not solve these recurrences; we'll see how to do that in Chapter 7.)

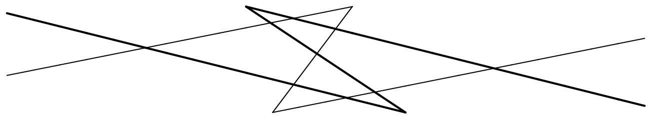
11 A Double Tower of Hanoi contains $2n$ disks of n different sizes, two of each size. As usual, we're required to move only one disk at a time, without putting a larger one over a smaller one.

a How many moves does it take to transfer a double tower from one peg to another, if disks of equal size are indistinguishable from each other?

b What if we are required to reproduce the original top-to-bottom order of all the equal-size disks in the final arrangement? [*Hint:* This is difficult—it's really a "bonus problem."]

12 Let's generalize exercise 11a even further, by assuming that there are n different sizes of disks and exactly m_k disks of size k. Determine $A(m_1,\ldots,m_n)$, the minimum number of moves needed to transfer a tower when equal-size disks are considered to be indistinguishable.

13 What's the maximum number of regions definable by n zig-zag lines,



$ZZ_2 = 12$

each of which consists of two parallel infinite half-lines joined by a straight segment?

14 How many pieces of cheese can you obtain from a single thick piece by making five straight slices? (The cheese must stay in its original position while you do all the cutting, and each slice must correspond to a plane in 3D.) Find a recurrence relation for P_n, the maximum number of three-dimensional regions that can be defined by n different planes.

Good luck keeping the cheese in position.

15 Josephus had a friend who was saved by getting into the next-to-last position. What is $I(n)$, the number of the penultimate survivor when every second person is executed?

16 Use the repertoire method to solve the general four-parameter recurrence

$$\begin{aligned} g(1) &= \alpha; \\ g(2n+j) &= 3g(n) + \gamma n + \beta_j, \qquad \text{for } j = 0, 1 \quad \text{and} \quad n \geqslant 1. \end{aligned}$$

Hint: Try the function $g(n) = n$.

Exam problems

17 If W_n is the minimum number of moves needed to transfer a tower of n disks from one peg to another when there are four pegs instead of three, show that

$$W_{n(n+1)/2} \leqslant 2W_{n(n-1)/2} + T_n, \qquad \text{for } n > 0.$$

(Here $T_n = 2^n - 1$ is the ordinary three-peg number.) Use this to find a closed form $f(n)$ such that $W_{n(n+1)/2} \leqslant f(n)$ for all $n \geqslant 0$.

18 Show that the following set of n bent lines defines Z_n regions, where Z_n is defined in (1.7): The jth bent line, for $1 \leqslant j \leqslant n$, has its zig at $(n^{2j}, 0)$ and goes up through the points $(n^{2j} - n^j, 1)$ and $(n^{2j} - n^j - n^{-n}, 1)$.

19 Is it possible to obtain Z_n regions with n bent lines when the angle at each zig is $30°$?

20 Use the repertoire method to solve the general five-parameter recurrence

Is this like a five-star general recurrence?

$$\begin{aligned} h(1) &= \alpha; \\ h(2n+j) &= 4h(n) + \gamma_j n + \beta_j, \qquad \text{for } j = 0, 1 \quad \text{and} \quad n \geqslant 1. \end{aligned}$$

Hint: Try the functions $h(n) = n$ and $h(n) = n^2$.

21 Suppose there are $2n$ people in a circle; the first n are "good guys" and the last n are "bad guys." Show that there is always an integer m (depending on n) such that, if we go around the circle executing every mth person, all the bad guys are first to go. (For example, when $n = 3$ we can take $m = 5$; when $n = 4$ we can take $m = 30$.)

Bonus problems

22 Show that it's possible to construct a Venn diagram for all 2^n possible subsets of n given sets, using n convex polygons that are congruent to each other and rotated about a common center.

23 Suppose that Josephus finds himself in a given position j, but he has a chance to name the elimination parameter q such that every qth person is executed. Can he always save himself?

Research problems

24 Find all recurrence relations of the form

$$X_n = \frac{1 + a_1 X_{n-1} + \cdots + a_k X_{n-k}}{b_1 X_{n-1} + \cdots + b_k X_{n-k}}$$

whose solution is periodic.

25 Solve infinitely many cases of the four-peg Tower of Hanoi problem by proving that equality holds in the relation of exercise 17.

26 Generalizing exercise 23, let's say that a *Josephus subset* of $\{1, 2, \ldots, n\}$ is a set of k numbers such that, for some q, the people with the other $n-k$ numbers will be eliminated first. (These are the k positions of the "good guys" Josephus wants to save.) It turns out that when $n = 9$, three of the 2^9 possible subsets are non-Josephus, namely $\{1, 2, 5, 8, 9\}$, $\{2, 3, 4, 5, 8\}$, and $\{2, 5, 6, 7, 8\}$. There are 13 non-Josephus sets when $n = 12$, none for any other values of $n \leqslant 12$. Are non-Josephus subsets rare for large n?

Yes, and well done if you find them.