ITT9132 Concrete Mathematics
Lecture 2 – 7 February 2023

Last update: 7 February 2023

Contents

Next section

The Tower of Hanoi: Description

The Tower of Hanoi puzzle was invented by the French mathematician Édouard Lucas in 1883.

- The board has three pegs.
- The tiles are n disks, all of different sizes, with a hole in the middle so that they can be put on the pegs.
- At the beginning of the game, the disks are all on the first peg, in decreasing order from bottom to top (larger at the bottom, smaller at the top)..
- The aim of the game is to put all the disks on the third peg, using the second peg as a help, so that at no time a disk is above a smaller disk.

The Tower of Hanoi: Solution

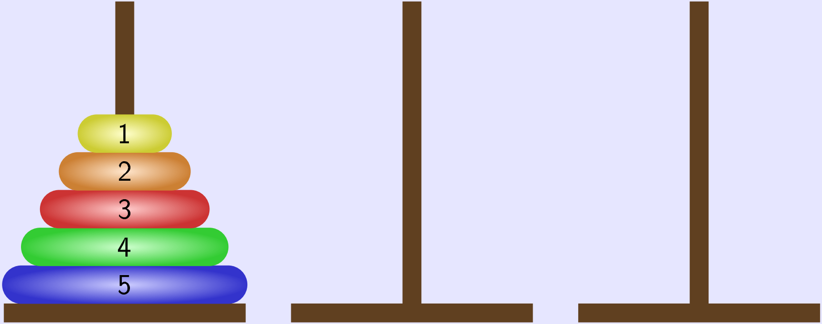
Using mathematical induction the following can be proved:

For the Tower of Hanoi puzzle with $n \geqslant 0$, the minimum number of moves needed is:

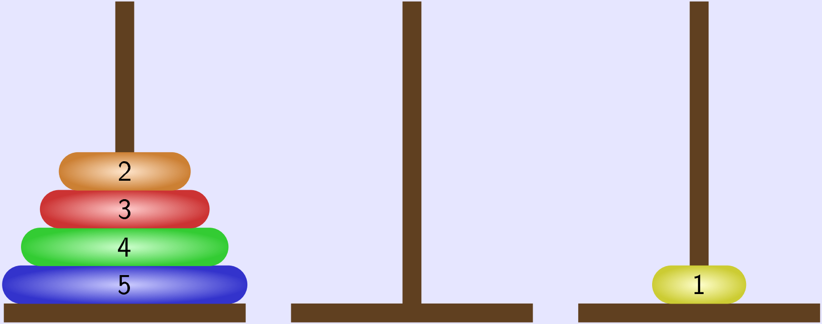
$$T_n = 2^n - 1\,.$$

Let's look at the example borrowed from Martin Hofmann and Berteun Damman.

Tower of Hanoi – 5 Discs

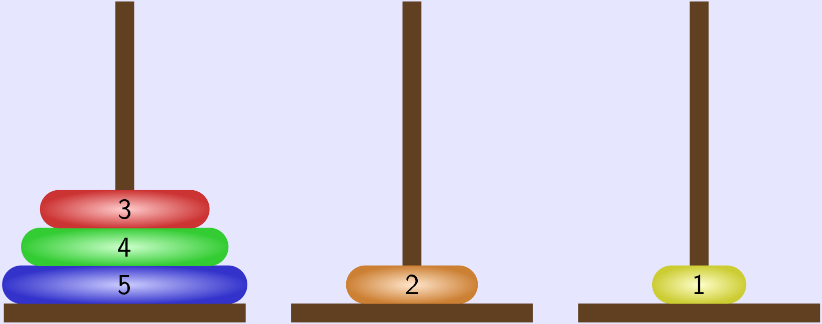


Tower of Hanoi – 5 Discs



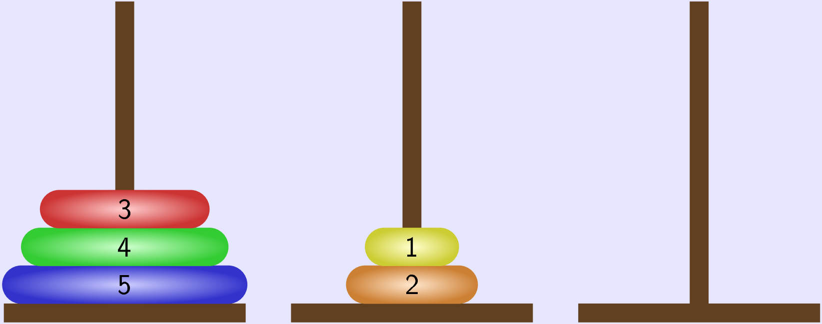
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 5 Discs



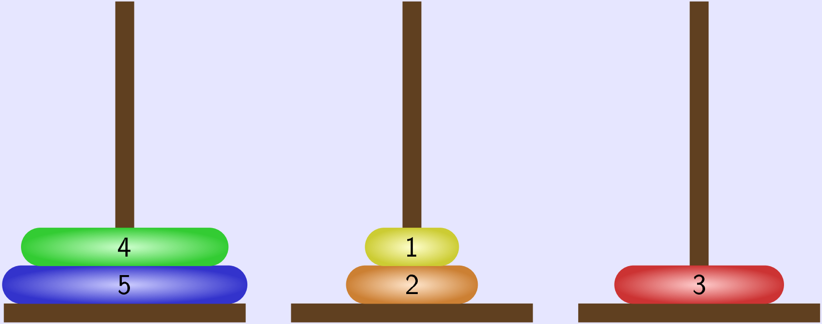
Moved disc from pole 1 to pole 2.

Tower of Hanoi – 5 Discs



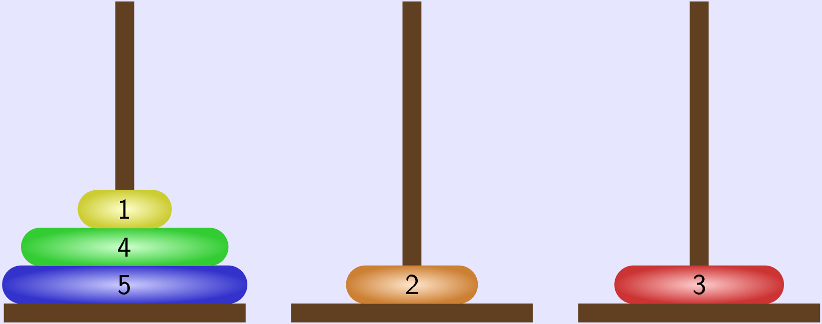
Moved disc from pole 3 to pole 2.

Tower of Hanoi – 5 Discs



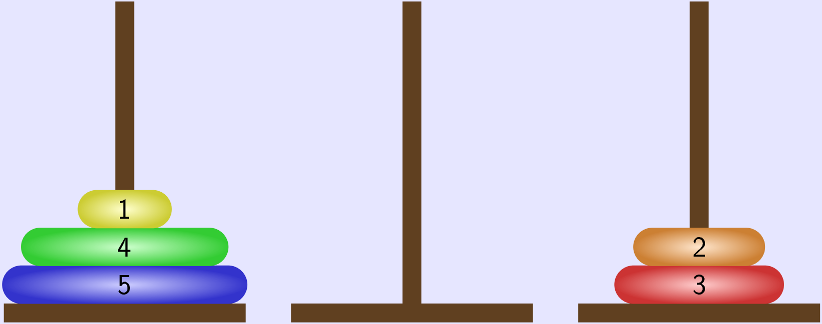
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 5 Discs



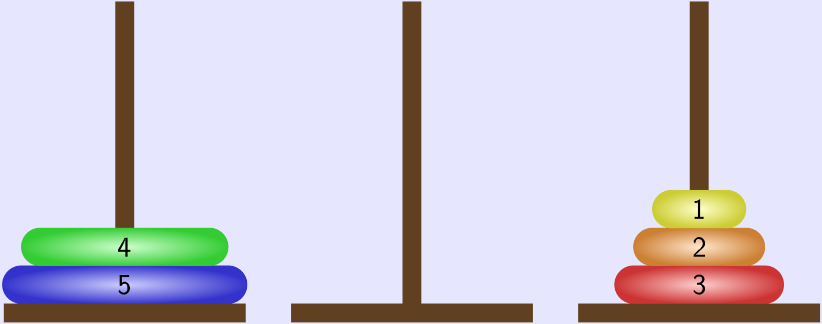
Moved disc from pole 2 to pole 1.

Tower of Hanoi – 5 Discs



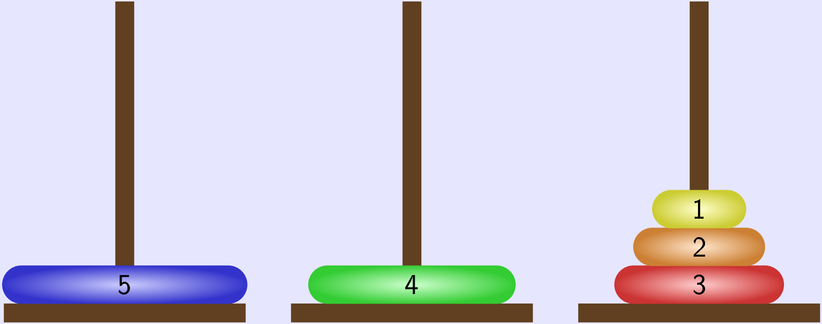
Moved disc from pole 2 to pole 3.

Tower of Hanoi – 5 Discs



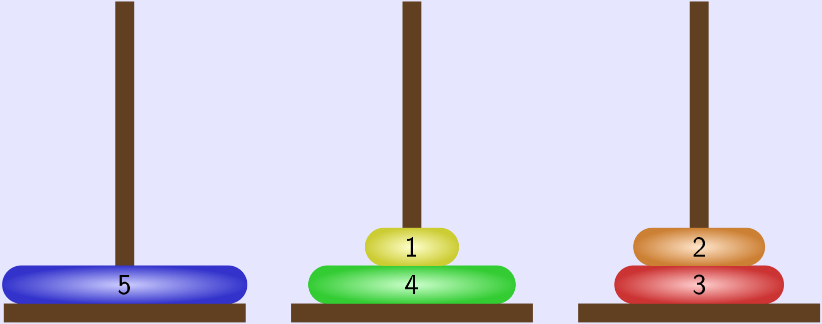
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 5 Discs



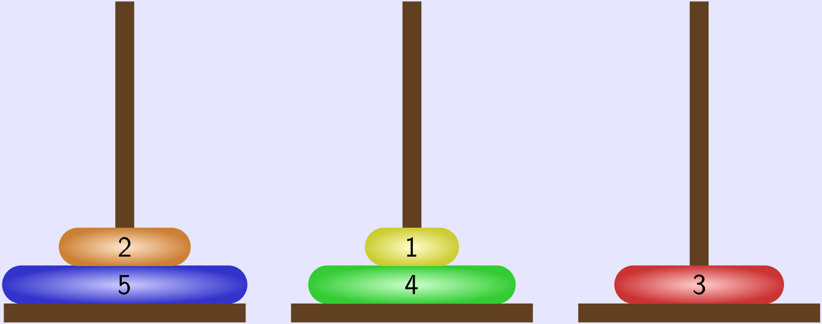
Moved disc from pole 1 to pole 2.

Tower of Hanoi – 5 Discs



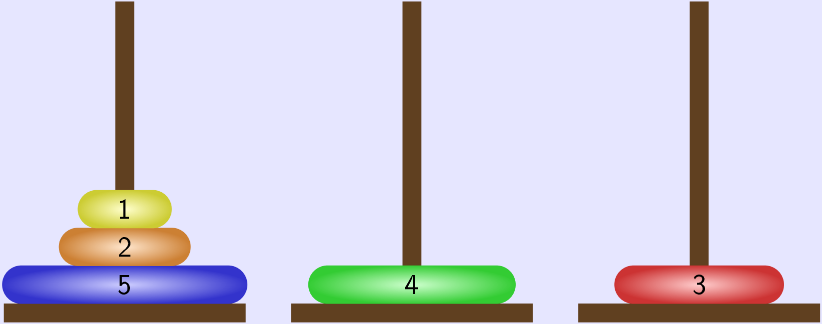
Moved disc from pole 3 to pole 2.

Tower of Hanoi – 5 Discs



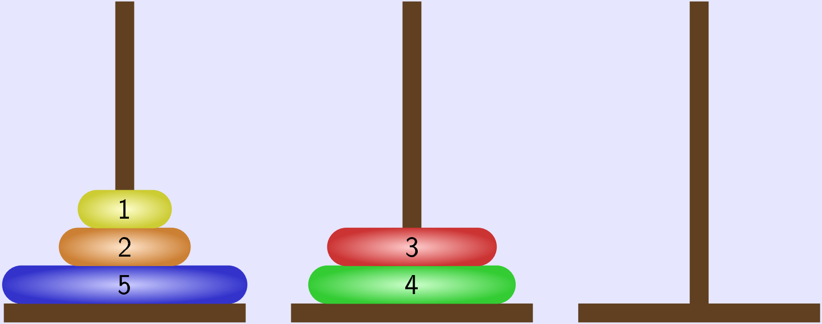
Moved disc from pole 3 to pole 1.

Tower of Hanoi – 5 Discs



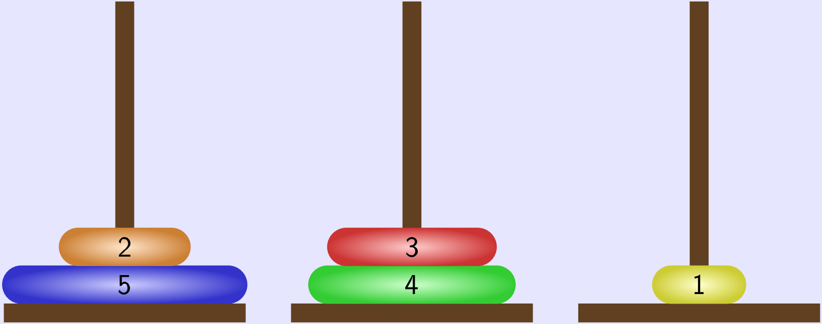
Moved disc from pole 2 to pole 1.

Tower of Hanoi – 5 Discs



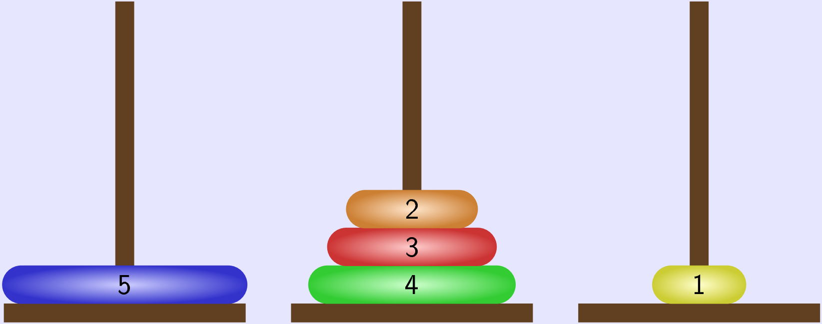
Moved disc from pole 3 to pole 2.

Tower of Hanoi – 5 Discs



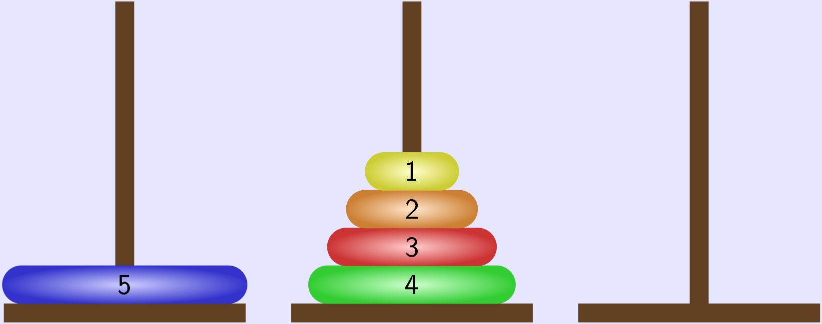
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 5 Discs



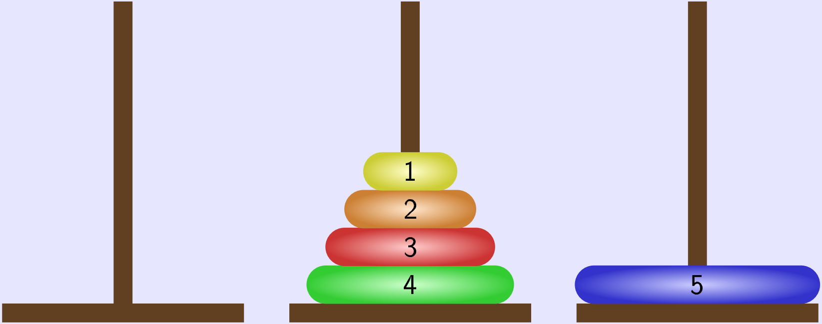
Moved disc from pole 1 to pole 2.

Tower of Hanoi – 5 Discs



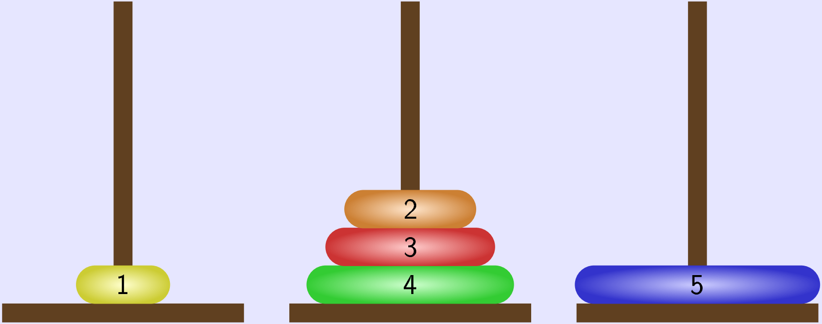
Moved disc from pole 3 to pole 2.

Tower of Hanoi – 5 Discs



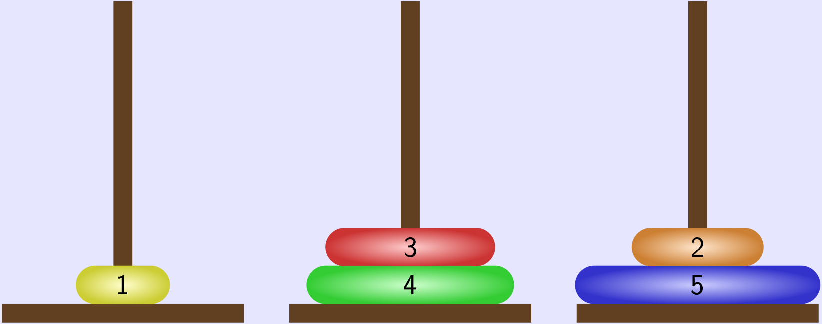
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 5 Discs



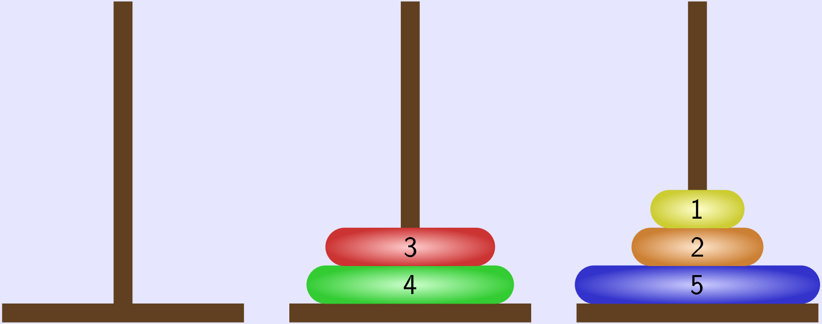
Moved disc from pole 2 to pole 1.

Tower of Hanoi – 5 Discs



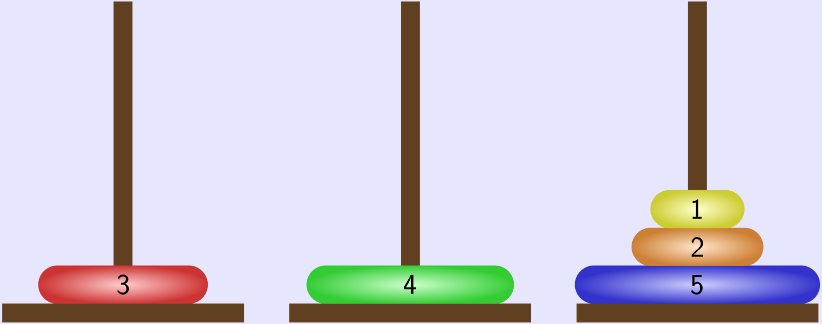
Moved disc from pole 2 to pole 3.

Tower of Hanoi – 5 Discs



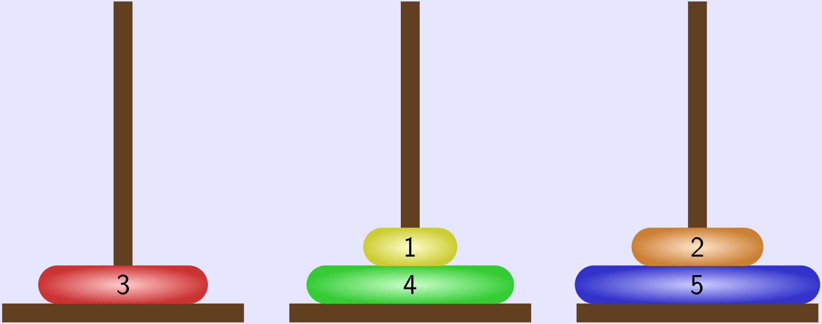
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 5 Discs



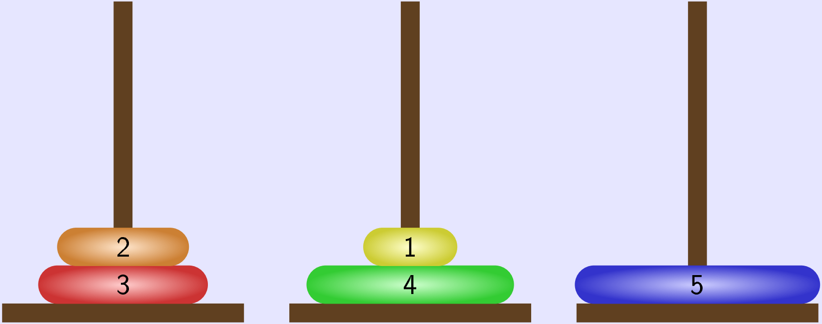
Moved disc from pole 2 to pole 1.

Tower of Hanoi – 5 Discs



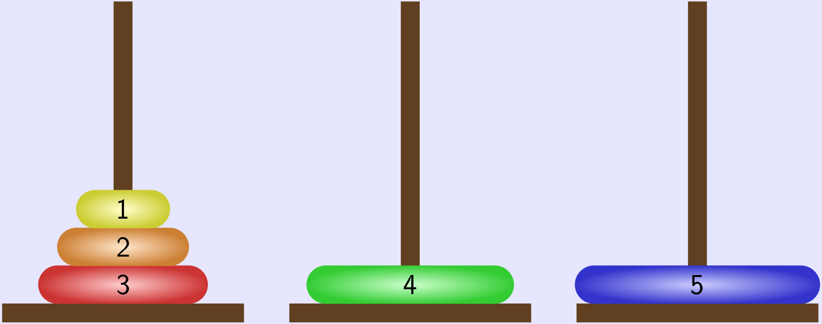
Moved disc from pole 3 to pole 2.

Tower of Hanoi – 5 Discs



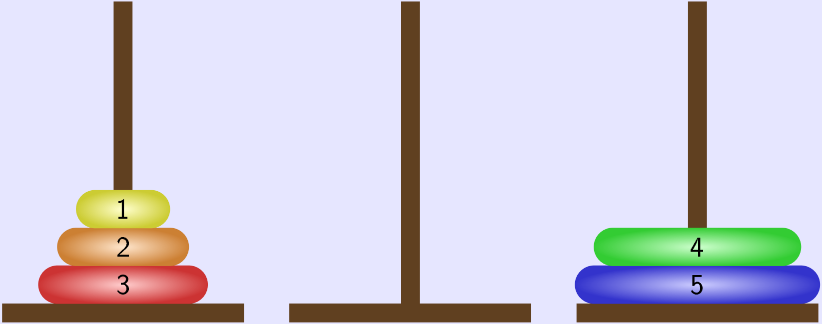
Moved disc from pole 3 to pole 1.

Tower of Hanoi – 5 Discs



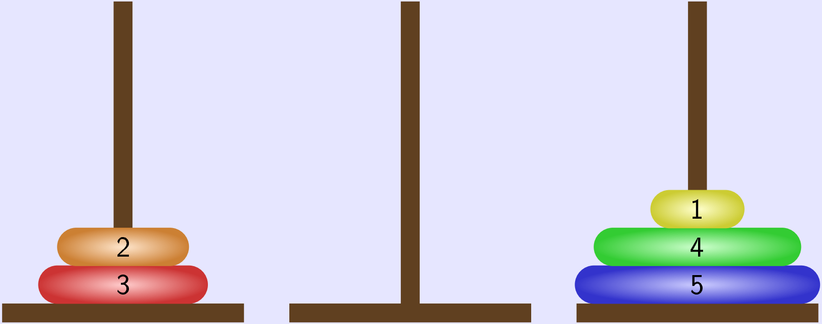
Moved disc from pole 2 to pole 1.

Tower of Hanoi – 5 Discs



Moved disc from pole 2 to pole 3.

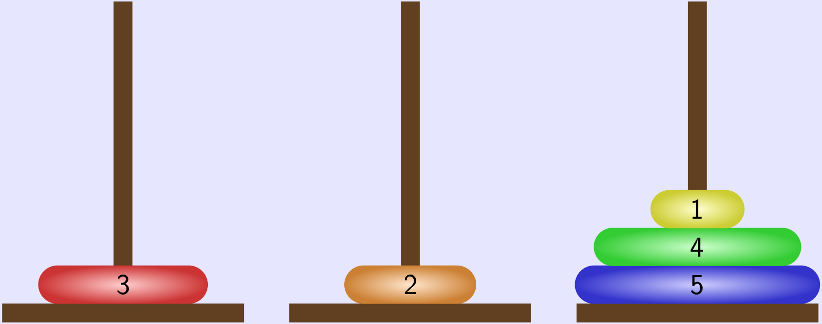
Tower of Hanoi – 5 Discs



Moved disc from pole 1 to pole 3.

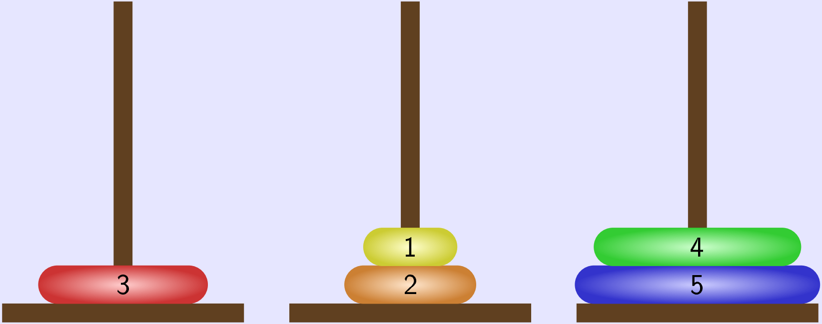
TAL TECH

Tower of Hanoi – 5 Discs



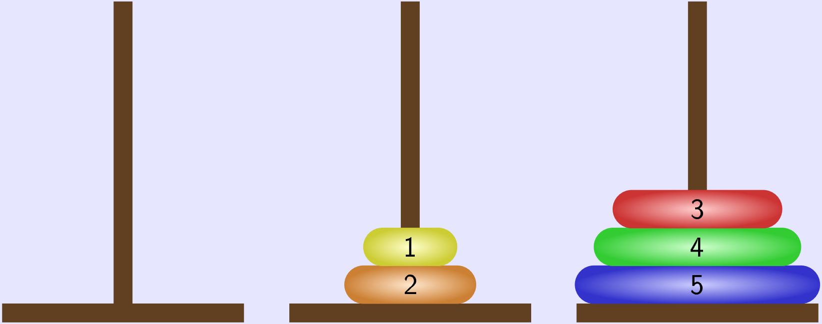
Moved disc from pole 1 to pole 2.

Tower of Hanoi – 5 Discs



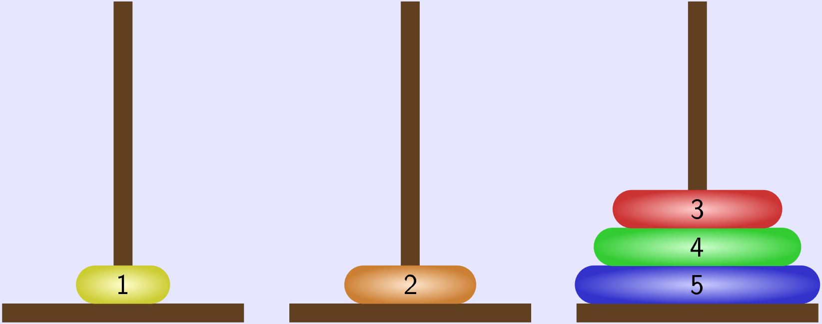
Moved disc from pole 3 to pole 2.

Tower of Hanoi – 5 Discs



Moved disc from pole 1 to pole 3.

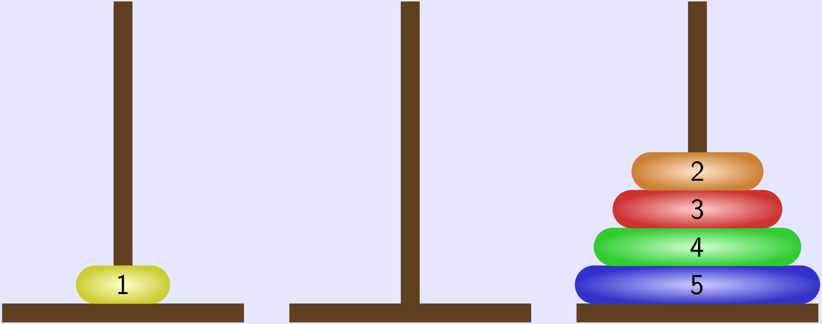
Tower of Hanoi – 5 Discs



Moved disc from pole 2 to pole 1.

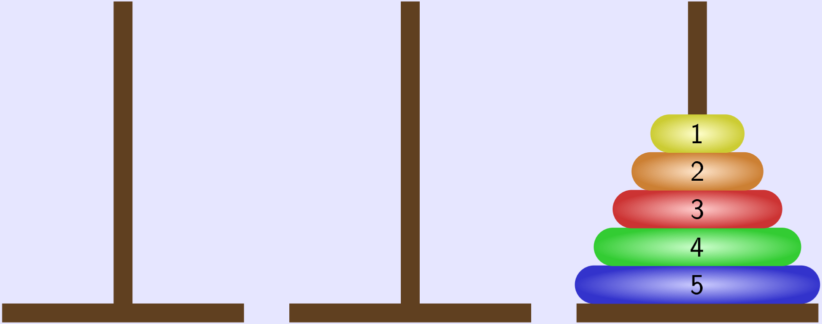
TAL TECH

Tower of Hanoi – 5 Discs



Moved disc from pole 2 to pole 3.

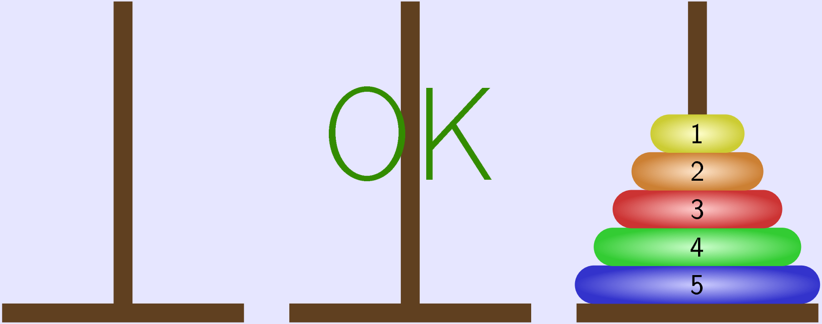
Tower of Hanoi – 5 Discs



Moved disc from pole 1 to pole 3.

TAL TECH

Tower of Hanoi – 5 Discs



A reminder: The Principle of Mathematical Induction

Let $P(n)$ be a predicate whose truth or falsehood depends on the value taken by a variable n in the set $\mathbb{N}$ of nonnegative integers.
Suppose the following happen:

1. For some $k \in \mathbb{N}$, $P(k)$ is true.
2. For every $n \geqslant k$, the implication $P(n) \longrightarrow P(n+1)$ holds: that is, if $P(n)$ is true, then $P(n+1)$ is also true.

Then $P(n)$ is true for every $n \geqslant k$.

The idea behind the recursive algorithm

The game requires to move the tower from peg 1 to peg 3, using peg 2 as a “spool”.

- Of course, the big issue is to put the largest disc on peg 3.
- This requires moving all the other discs from peg 1 to peg 2, using peg 3 as a spool.
- But this is just another Hanoi Tower game with one less disc and the role of the pegs changed!
- After the largest disc is on peg 3, we must move all the other discs from peg 2 to peg 3, using peg 1 as a spool.
- Again, this is just another Hanoi Tower game with one less disc and the role of the pegs changed.

A recursive solution in Python

```python
#!/usr/bin/env python3

import os

def hanoi(n, start='1', step='2', stop='3'):
    '''Solve the Hanoi tower with n disks, from start
    peg to stop peg, using step peg as a spool'''
    if n > 0:
        hanoi(n-1, start, stop, step)
        move(n, start, stop)
        hanoi(n-1, step, start, stop)

def move(n, start, stop):
    '''Display move of disk n from start to stop'''
    print("Disk %d: %s -> %s" % (n, start, stop))

if __name__ == '__main__':
    n = int(input('How many disks? '))
    hanoi(n, '1', '2', '3')
```

A recursive solution in Python

```
#!/usr/bin/env python3

import os

def hanoi(n, start='1', step='2', stop='3'):
    '''Solve the Hanoi tower with n disks, from start
    peg to stop peg, using step peg as a spool'''
    if n > 0:
        hanoi(n-1, start, stop, step)
        move(n, start, stop)
        hanoi(n-1, step, start, stop)

def move(n, start, stop):
    '''Display move of disk n from start to stop'''
    print("Disk %d: %s -> %s" % (n, start, stop))

if __name__ == '__main__':
    n = int(input('How many disks? '))
    hanoi(n, '1', '2', '3')
```

Question: why does this program show that $T_n = 2^n - 1$?

Tower of Hanoi: Running time

Base case: $n = 1$.

- Then the Python script only performs `move('1', '3')`, so $T_1 = 1 = 2^1 - 1$.

Inductive step: n disks require $2^n - 1$ steps. We play a game with $n+1$ disks.

- Then the Python script performs:
  - `hanoi(n, '1', '3', '2')`
  - `move('1', '3')`
  - `hanoi(n, '2', '1', '3')`

  which, by inductive hypothesis, requires:

  $$T_{n+1} = (2^n - 1) + 1 + (2^n - 1) = 2^{n+1} - 1$$

  moves.

What we have proved, is that $T_n = 2^n - 1$ is the solution of the recursion:

$$T_n = 2T_{n-1} + 1 \text{ for every } n \geq 2$$

with the initial condition $T_1 = 1$.

A little tweak for a simpler recurrence

We now change the rules a little bit by saying that, when we complete the game, we say "Hurrah!" as a final move.

- Let U_n be the number of moves required by this variant. Clearly, $U_n = T_n + 1$.
- Of course, $U_1 = 2$.
- This time, when we play on n disks, we do this:
  - We play the game on $n-1$ disks from peg 1 to peg 2.
  - Instead of saying "Hurrah!", we move the largest disk to peg 3.
  - We play the game on $n-1$ disks from peg 2 to peg 3.
  - We say "Hurrah!"
- Then U_n is the solution of the recurrence:

$$U_n = 2U_{n-1} \text{ for every } n \geq 2$$

  with the initial condition $U_1 = 2$.
- It is easy to see that $U_n = 2^n$.

TAL TECH

Warmup: What is wrong with this "proof by induction"?

Theorem

All children have the same color of eyes.

"Proof"

The thesis is clearly true for $n = 1$, so let $n > 1$.

1. Put the n children on a line.
2. By inductive hypothesis, the $n-1$ *leftmost* children have the same color of eyes, and so do the $n-1$ *rightmost* children.
3. Then the $n-2$ children *in the middle* have the same color of eyes.
4. The first and last child must then have *that* color of eyes.

Warmup: What is wrong with this “proof by induction”?

Theorem

All children have the same color of eyes.

Solution

The problem is with:

- Then the $n-2$ children *in the middle* have the same color of eyes.

For $n=2$ there are no “$n-2$ children in the middle”.
So the implication $P(n) \longrightarrow P(n+1)$ is not true for every $n \geq 1$.

Next section

Lines in the Plane

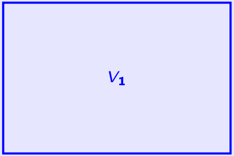
Problem

Popularly: How many slices of pizza can a person obtain by making n straight cuts with a pizza knife?

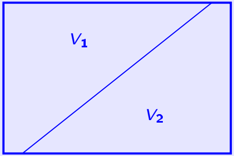
Academically: What is the maximum number L_n of regions defined by n lines in the plane?

Solved first in 1826, by the Swiss mathematician Jacob Steiner.

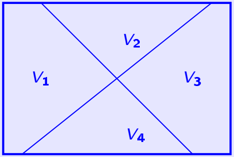
Lines in the Plane – small cases



$L_0 = 1$



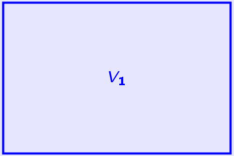
$L_1 = 2$



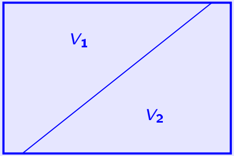
$L_2 = 4$

$L_3 = L_2 + 3 = 7$

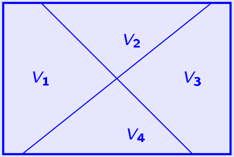
Lines in the Plane – small cases



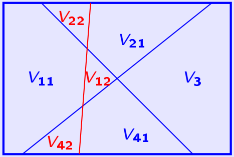
$L_0 = 1$



$L_1 = 2$



$L_2 = 4$



$L_3 = L_2 + 3 = 7$

Lines in the Plane – generalization

Observation:

The n-th line (for $n > 0$) increases the number of regions by k

iff it splits k of the "old regions"

iff it hits the previous lines in $k-1$ different places.

Lines in the Plane – generalization

Observation:

The n-th line (for $n > 0$) increases the number of regions by k

iff it splits k of the “old regions”

iff it hits the previous lines in $k-1$ different places.

Then k must be less or equal to n. – Why?

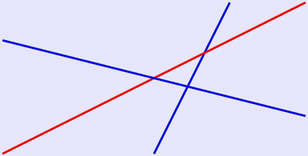
Lines in the Plane – generalization

Observation:

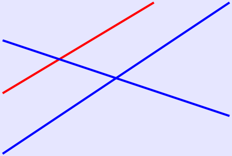
The n-th line (for $n > 0$) increases the number of regions by k

iff it splits k of the "old regions"

iff it hits the previous lines in $k-1$ different places.



$k = 3$; 2 places



$k = 2$; 1 place

Lines in the Plane – generalization (2)

Therefore the new line can intersect the $n-1$ “old” lines in at most $n-1$ different points.
We have thus established the upper bound:

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

If the nth line:

1. is not parallel to any of the others (hence it intersects them all), and
2. doesn't go through any of the existing intersection points (hence it intersects each one of the others in different places)

then we can reach the upper bound (which becomes a maximum) and obtain the recurrence:

$$L_0 = 1;$$
$$L_n = L_{n-1} + n \qquad \text{for } n > 0.$$

For example, we could place the nth line outside the convex hull of the intersections fo the previous $n-1$ lines.

n	0	1	2	3	4	5	6	7	8	9	$\cdots$
L_n	1	2	4	7	11	16	22	29	37	46	$\cdots$

Lines in the Plane – solving recurrence

Observation:

$$
\begin{aligned}
L_n &= L_{n-1} + n \\
&= L_{n-2} + (n-1) + n \\
&= L_{n-3} + (n-2) + (n-1) + n \\
&= \cdots \\
&= L_0 + 1 + 2 + \ldots + (n-2) + (n-1) + n \\
&= 1 + S_n\,,
\end{aligned}
$$

where $S_n = 1 + 2 + 3 + \ldots + (n-1) + n$.

Lines in the Plane – solving recurrence (2)

Evaluation of $S_n = 1 + 2 + \cdots + (n-1) + n$.

Recurrent equation:

$$\begin{aligned} S_0 &= 0\,; \\ S_n &= S_{n-1} + n \text{ for every } n \geq 1\,. \end{aligned}$$

Solution (Gauss, 1786):

$$\begin{array}{cccccccccccc} S_n & = & 1 & + & 2 & + & \ldots & + & (n-1) & + & n \\ +S_n & = & n & + & (n-1) & + & \ldots & + & 2 & + & 1 \\ \hline 2S_n & = & (n+1) & + & (n+1) & + & \ldots & + & (n+1) & + & (n+1) \end{array}$$

Then $2S_n = n \cdot (n+1)$, so that $S_n = \dfrac{n(n+1)}{2}$.

Lines in the Plane – solving recurrence (2)

Evaluation of $S_n = 1+2+\cdots+(n-1)+n$.

Recurrent equation:

$$\begin{aligned} S_0 &= 0\,; \\ S_n &= S_{n-1}+n \text{ for every } n \geq 1\,. \end{aligned}$$

Solution (Gauss, 1786):

$$\begin{array}{ccccccccccc} S_n & = & 1 & + & 2 & + & \ldots & + & (n-1) & + & n \\ +S_n & = & n & + & (n-1) & + & \ldots & + & 2 & + & 1 \\ \hline 2S_n & = & (n+1) & + & (n+1) & + & \ldots & + & (n+1) & + & (n+1) \end{array}$$

Then $2S_n = n \cdot (n+1)$, so that $S_n = \dfrac{n(n+1)}{2}$.

Lines in the Plane – solving recurrence (3)

Theorem: Closed formula for L_n

$$L_n = \frac{n(n+1)}{2} + 1 \text{ for every } n \geq 0\,.$$

Proof (by induction).

Base: $L_0 = 1 = \frac{0(0+1)}{2} + 1$.

Step: Let's assume $L_n = \frac{n(n+1)}{2} + 1$ and evaluate

$$\begin{aligned} L_{n+1} &= L_n + n + 1 \\ &= \frac{n(n+1)}{2} + 1 + n + 1 \\ &= \frac{n(n+1) + 2 + 2n}{2} + 1 \\ &= \frac{n(n+1) + 2(n+1)}{2} + 1 \\ &= \frac{(n+1)(n+2)}{2} + 1\,. \end{aligned}$$

Q.E.D.

Triangular numbers

The nth triangular number is defined as:

$$T_n = \frac{n(n+1)}{2} \text{ for every } n \geq 0$$

- Then T_n is the solution of the first order recurrence equation:

$$a_n = a_{n-1} + n \text{ for every } n \geq 1$$

  with the initial condition $a_0 = 0$.
- The numbers L_n are the solution of the same recurrence, but with initial condition $a_0 = 1$.

Next section

The Josephus Problem

The legend

During the Jewish-Roman war, Flavius Josephus, a famous historian of the first century, 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, together with his friend, wanted to avoid being killed. So he quickly calculated where he and his friend should stand in the vicious circle

The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person
  until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.

The elimination order is
2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

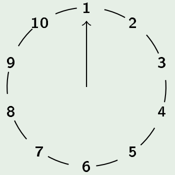
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person
  until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is
2, 4, 6, 8, 10, 3, 7, 1, 9 . So, we have $J(10) = 5$

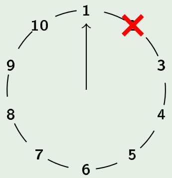
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is 2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

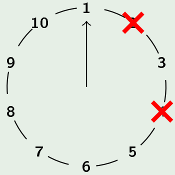
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is

2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

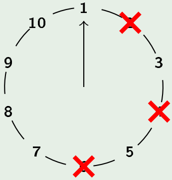
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person
  until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is

2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

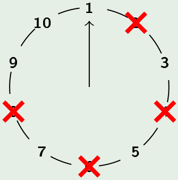
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is

2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

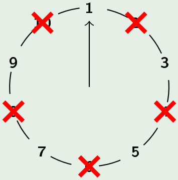
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is 2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

TAL TECH

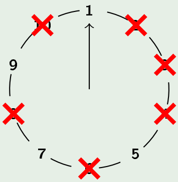
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person
  until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is

2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

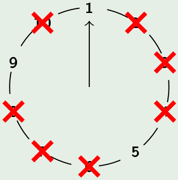
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is 2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

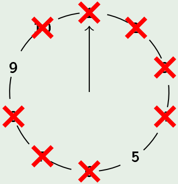
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is 2, 4, 6, 8, 10, 3, 7, 1, 9 . So, we have $J(10) = 5$

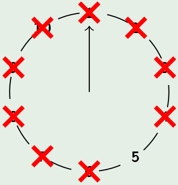
The Josephus Problem

Our variation of the problem:

- We start with n people numbered 1 to n around a circle.
- We eliminate every second remaining person until only one survives.

Task is to compute the survivor's number, $J(n)$

Example, $n = 10$.



The elimination order is 2, 4, 6, 8, 10, 3, 7, 1, 9. So, we have $J(10) = 5$

The Josephus Problem – small numbers

Evaluate $J(n)$ for small n:

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

The Josephus Problem – small numbers

Evaluate $J(n)$ for small n:

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

Properties

1. $J(n)$ is always odd.
2. The recurrence equation:

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

   is still a recurrence in the sense given in the introduction, with:

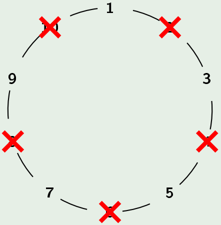
$$f_n(n; a_{n-1}, \ldots, a_1) = \begin{cases} a_{\frac{n}{2}} - 1 & \text{if } n \text{ is even}, \\ a_{\frac{n-1}{2}} + 1 & \text{if } n \text{ is odd} \end{cases} \quad \text{for every } n \geq 2$$

3. We will show that the collowing closed formula holds:

$$J(2^m + \ell) = 2\ell + 1 \quad \text{for } m \geqslant 0 \text{ and } 0 \leqslant \ell < 2^m\,.$$

The Josephus Problem – recurrent equation (1)

Case $n = 2m$.



First trip eliminates all even numbers. Then we change numbers and repeat:

Old number k	1	3	5	7	9
New number k'	1	2	3	4	5

or

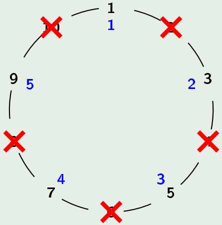
$$k = 2k' - 1\,.$$

That correspondance between "old" and "new number" gives us that:

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

The Josephus Problem – recurrent equation (1)

Case $n = 2m$.



First trip eliminates all even numbers. Then we change numbers and repeat:

Old number k	1	3	5	7	9
New number k'	1	2	3	4	5

or

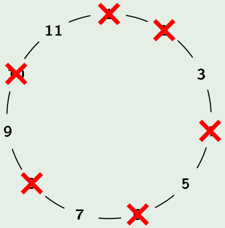
$$k = 2k' - 1\,.$$

That correspondance between "old" and "new number" gives us that:

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

The Josephus Problem – recurrent equation (2)

Case $n = 2m + 1$.



First trip eliminates all even numbers. Then we eliminate number 1. Then we change numbers and repeat:

Old number k	3	5	7	9	11
New number k'	1	2	3	4	5

or

$$k = 2k' + 1$$

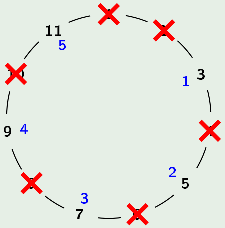
That correspondence between "old" and "new" numbers givs us that:

$J(2n+1) = 2J(n) + 1$

.

The Josephus Problem – recurrent equation (2)

Case $n = 2m + 1$.



First trip eliminates all even numbers. Then we eliminate number 1. Then we change numbers and repeat:

Old number k	3	5	7	9	11
New number k'	1	2	3	4	5

or

$$k = 2k' + 1$$

That correspondence between "old" and "new" numbers givs us that:

$J(2n+1) = 2J(n) + 1$

.

The Josephus Problem – application of recurrence

The equation

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

can be used for computing function for large arguments.

For example

$$\begin{aligned} J(86) &= 2J(43)-1 &= 45 \\ J(43) &= 2J(21)+1 &= 23 \\ J(21) &= 2J(10)+1 &= 11 \\ J(10) &= 5 \end{aligned}$$

The Josephus Problem – closed formula

Theorem

$$J(2^m + \ell) = 2\ell + 1 \text{ for } m \geqslant 0 \text{ and } 0 \leqslant \ell < 2^m .$$

Proof by induction over m:

Base If $m = 0$ then also $\ell = 0$, and $J(1) = 1$.

Step

- If $m > 0$ and $2^m + \ell = 2n$, then ℓ is even and:

$$J(2^m + \ell) = 2J(2^{m-1} + \ell/2) - 1 = 2(2\ell/2 + 1) - 1 = 2\ell + 1 .$$

- If $2^m + \ell = 2n + 1$, then:

$$J(2n+1) = 2 + J(2n) = 2 + 2(\ell - 1) + 1 = 2\ell + 1$$

Q.E.D.

Next section

Structural induction

Premises

Let S be a set having the following features:

1. A set S_B of base cases is contained in S.
2. Finitely many operations $u_i : S^{m_i} \to S$, $i = 1, \ldots, n$, exist such that, if $x_1, \ldots, x_{m_i} \in S$, then $u_i(x_1, \ldots, x_{m_i}) \in S$.
   The operations u_i are also called *constructors*.
3. Nothing else belongs to S.

The Principle of Structural Induction

Let P be a property such that:

1. each base case $x \in S_B$ has property P; and
2. for every $i = 1, \ldots, n$ and every $x_1, \ldots, x_{m_i} \in S$, if each object $x_1, \ldots, x_{m_i}$ has property P, then $u_i(x_1, \ldots, x_{m_i})$ has property P.

Then every element of S has property P.

Mathematical induction as structural induction

Natural numbers as a recursive data type

The set $S = \mathbb{N}$ of natural numbers is constructed as follows:

1. A set $S_B = \{0\}$ of basic cases is contained in $\mathbb{N}$.
2. A single operation, the *successor*, $s : \mathbb{N} \to \mathbb{N}$, exists such that, if $n \in \mathbb{N}$, then $s(n) \in \mathbb{N}$.
3. Nothing else belongs to $\mathbb{N}$.

Structural induction on the natural numbers = Mathematical induction

Let P be a property such that:

1. 0 has property P; and
2. for every $n \in \mathbb{N}$, if n has property P, then $s(n)$ has property P.

Then every $n \in \mathbb{N}$ has property P.

Structural induction on positive integers

Positive integers as a recursive data type

The set $S = \mathbb{Z}_+$ of positive integers is constructed as follows:

1. A set $S_B = \{1\}$ of basic cases is contained in $\mathbb{Z}_+$.
2. Two operations:
   1. doubling $d : \mathbb{Z}_+ \to \mathbb{Z}_+, d(n) = 2n$;
   2. doubling increased $sd : \mathbb{Z}_+ \to \mathbb{Z}_+, sd(n) = 2n+1$

   exist such that, if $n \in \mathbb{Z}_+$, then $d(n), sd(n) \in \mathbb{Z}_+$.
3. Nothing else belongs to $\mathbb{Z}_+$.

Structural induction on the positive integers

Let P be a property such that

1. 1 has property P.
2. For every $n \in \mathbb{Z}_+$, if n has property P, then $d(n)$ and $sd(n)$ have property P.

Then every $n \in \mathbb{Z}_+$ has property P.

Next section

Binary expansion of $n = 2^m + \ell$

Denote

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

where $b_i \in \{0,1\}$ and $b_m = 1$.

This notation stands for:

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

For example:

$$20 = (10100)_2 \quad \text{and} \quad 83 = (1010011)_2$$

Binary expansion of $n = 2^m + \ell$, where $0 \leqslant \ell < 2^m$

Observations:

1. $\ell = (0\, b_{m-1} \dots b_1\, b_0)_2$.
2. $2\ell = (b_{m-1} \dots b_1\, b_0 0)_2$.
3. $2^m = (10\dots00)_2$ and $1 = (00\dots01)_2$.
4. $n = 2^m + \ell = (1\, b_{m-1} \dots b_1\, b_0)_2$.
5. $2\ell + 1 = (b_{m-1} \dots b_1\, b_0 1)_2$

Corollary

$$J((\boxed{1}\; b_{m-1} \dots b_1\, b_0)_2 = (b_{m-1} \dots b_1\, b_0\; \boxed{1})_2$$

shift

Binary expansion of $n = 2^m + \ell$, where $0 \leqslant \ell < 2^m$

Observations:

1. $\ell = (0\, b_{m-1} \dots b_1\, b_0)_2$.
2. $2\ell = (b_{m-1} \dots b_1\, b_0 0)_2$.
3. $2^m = (10\dots00)_2$ and $1 = (00\dots01)_2$.
4. $n = 2^m + \ell = (1\, b_{m-1} \dots b_1\, b_0)_2$.
5. $2\ell + 1 = (b_{m-1} \dots b_1\, b_0 1)_2$

Corollary

$$J((\boxed{1}\ b_{m-1} \dots b_1\, b_0)_2 = (b_{m-1} \dots b_1\, b_0\ \boxed{1})_2$$

Binary expansion of $n = 2^m + \ell$, where $0 \leqslant \ell < 2^m$

Example

$$\begin{aligned} 100 &= 64 + 32 + 4 \\ J(100) &= J((1100100)_2) = (1001001)_2 \\ J(100) &= 64 + 8 + 1 = 73 \end{aligned}$$

TAL TECH

Iterating the Josephus function

Consider a sequence $x_0, x_1, \ldots, x_k, \ldots$ where:

- $x_0 = n$ is an arbitrary positive integer; and
- $x_k = J(x_{k-1})$ for every $k \geq 1$.

Questions:

1. Will the sequence reach a fixed point?
   That is: will $x_{k+1} = x_k$ for every k large enough?
2. If so: what are the possible fixed points?

Iterating the Josephus function: the answer

Proposition A

For every positive integer n, the sequence defined by:

$$\begin{aligned} x_0 &= n\,, \\ x_k &= J(x_{k-1}) \ \forall k \geqslant 1 \end{aligned}$$

reaches the fixed point $2^{\nu(n)} - 1$, where $\nu(n)$ is the number of bits equal to 1 in the binary representation of n.

Iterating the Josephus function: the answer

Proposition A

For every positive integer n, the sequence defined by:

$$\begin{aligned} x_0 &= n, \\ x_k &= J(x_{k-1}) \ \forall k \geqslant 1 \end{aligned}$$

reaches the fixed point $2^{\nu(n)} - 1$, where $\nu(n)$ is the number of bits equal to 1 in the binary representation of n.

Proof that x_k reaches a fixed point:

- For every $n = 2^m + \ell$ we have $J(n) = 2\ell + 1 \leqslant n$.
- Then the sequence x_k is *nonincreasing* in k:
  If $k \leqslant m$, then $x_k \geqslant x_m$.
- But a nonincreasing sequence of positive integers is ultimately constant.

Iterating the Josephus function: the answer

Proposition A

For every positive integer n, the sequence defined by:

$$\begin{aligned} x_0 &= n\,, \\ x_k &= J(x_{k-1}) \ \forall k \geqslant 1 \end{aligned}$$

reaches the fixed point $2^{\nu(n)} - 1$, where $\nu(n)$ is the number of bits equal to 1 in the binary representation of n.

Proof that the fixed point is $2^{\nu(n)} - 1$:

- The binary representation of $J(n)$ is obtained from that of n by a circular permutation.
- But after such a permutation, a leading 0 disappears, while a leading 1 is preserved.
- Then the binary writing of any fixed point must be made entirely of 1s.

Next section

Generalization

A first example of "simplifying by complicating"

The Josephus function $J : \mathbb{N} \to \mathbb{N}$ was defined using the recurrence:

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

Introducing integer constants α, β and γ, generalize it as follows:

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

The Josephus function $f(n) = J(n)$ corresponds to $\alpha = 1$, $\beta = -1$, $\gamma = 1$.

The repertoire method

To find closed form of a function f:

Step 1 Find few initial values for f.

Step 2 Find (or guess) closed formula from the values found by Step 1: *examine a repertoire of cases and combine them to find general closed formula*.

Step 3 Verify the closed formula constructed as the result of Step 2.

The idea is to examine a repertoire of cases and use it to find a general closed formula for the recurrently defined function.

The repertoire method for generalized f: STEP 1

n	$f(n)$	Calculation
1	α	$f(1) = \alpha$
2	$2\alpha + \beta$	$f(2) = 2f(1) + \beta$
3	$2\alpha + \gamma$	$f(3) = 2f(1) + \gamma$
4	$4\alpha + 3\beta$	$f(4) = 2f(2) + \beta$
5	$4\alpha + 2\beta + \gamma$	$f(5) = 2f(2) + \gamma$
6	$4\alpha + \beta + 2\gamma$	$f(6) = 2f(3) + \beta$
7	$4\alpha + 3\gamma$	$f(7) = 2f(3) + \gamma$
8	$8\alpha + 7\beta$	$f(8) = 2f(4) + \beta$
9	$8\alpha + 6\beta + \gamma$	$f(9) = 2f(4) + \gamma$

The repertoire method for generalized f: STEP 2

Observations:

For $n = 1, 2, \ldots, 9$, taking $n = 2^m + \ell$:

- The coefficient of α is 2^m;
- The coefficient of β is $2^m - 1 - \ell$;
- The coefficient of γ is ℓ.

The repertoire method for generalized f: STEP 3

Proposition

If the function f is defined by the recurrence formula:

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

then letting $n = 2^m + \ell$ with $0 \leq \ell < 2^m$,

$$f(n) = \alpha A(n) + \beta B(n) + \gamma C(n) ,$$

where:

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

Proof of the Proposition: Part 1

Lemma 1.

Let $n = 2^m + \ell$ with $0 \leqslant \ell < 2^k$ Then:

$$A(n) = 2^m \text{ for every } n \in \mathbb{N}$$

Proof: Let $\alpha = 1$ and $\beta = \gamma = 0$. Then $f(n) = A(n)$ and:

$$A(1) = 1\,; \quad A(2n) = 2A(n) \text{ for } n > 0\,; A(2n+1) = 2A(n) \text{ for } n > 0\,.$$

By induction over m:

Base: If $m = 0$, then $n = 2^0 + \ell$ and $0 \leqslant \ell < 1$. Thus $n = 1$ and

$$A(1) = 2^0 = 1\,.$$

Step: Assume that $A(2^{m-1} + t) = 2^{m-1}$, where $0 \leqslant t < 2^{m-1}$ Two cases:

- If n is even, then ℓ is even and $\ell/2 < 2^m/2 = 2^{m-1}$, thus

$$A(n) = A(2^m + \ell) = 2A(2^{m-1} + \ell/2) = 2 \cdot 2^{m-1} = 2^k$$

- If n is odd, then $\ell - 1$ is even and $(\ell - 1)/2 < 2^{m-1}$ as above, thus:

$$A(n) = A(2^m + \ell) = 2A(2^{m-1} + (\ell - 1)/2) = 2 \cdot 2^{m-1} = 2^m$$

□

Proof of the Proposition: Part 2

Lemma 2.

Let $n = 2^m + \ell$ with $0 \leqslant \ell < 2^m$ Then:

$$A(n) - B(n) - C(n) = 1 \text{ for every } n \in \mathbb{N}$$

Proof: Let f be the constant function $f(n) = 1$. Then:

$$f(1) = \alpha ; \quad f(2n) = 2f(n) + \beta ; \quad f(2n+1) = 2f(n) + \gamma$$

or equivalently,

$$1 = \alpha ; \quad 1 = 2 + \beta ; \quad 1 = 2 + \gamma .$$

As this must hold for every $n \geq 1$, it must be $\alpha = 1$ and $\beta = \gamma = -1$. □

TAL TECH

Proof of the Proposition: Part 3

Lemma 3.

Let $n = 2^m + \ell$ with $0 \leqslant \ell < 2^m$ Then:

$$A(n) + C(n) = 1 \text{ for every } n \in \mathbb{N}$$

Proof: Let $f(n) = n$. Then:

$$f(1) = \alpha\,; \quad f(2n) = 2f(n) + \beta\,; \quad f(2n+1) = 2f(n) + \gamma$$

or equivalently,

$$1 = \alpha\,; \quad 2n = 2n + \beta\,; \quad 2n+1 = 2n + \gamma.$$

As this must hold for every $n \geq 1$, it must be $\alpha = 1$, $\beta = 0$ and $\gamma = 1$. □

Proof of the Proposition: Part 4

We have obtained a repertoire of three triples, each one associated to a function of n:

$$(1,0,0) \longleftrightarrow 2^m ; \ (1,-1,-1) \longleftrightarrow 1 ; \ (1,0,1) \longleftrightarrow n .$$

From Lemma 3 and Lemma 1 we can conclude:

$$2^m + C(n) = A(n) + C(n) = n = 2^m + \ell ,$$

which gives:

$$C(n) = \ell .$$

From Lemma 2 follows:

$$B(n) = A(n) - 1 - C(n) = 2^m - 1 - \ell .$$

□

Incidentally, we observe that $\det \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & -1 \\ 1 & 0 & 1 \end{pmatrix} \neq 0$. Um. . .