

# Introduction

COMP 3200

Winter 2024

*“Computer science is no more about computers than astronomy is about telescopes.” – Edsger Dijkstra.*

1

## Course Goals

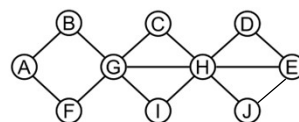
- Survey a number of mathematical tools that are useful when analyzing, modeling, and solving a wide variety of computational problems
- Gain experience with:
  - Formal reasoning and proof techniques
  - Careful use of language  $\Rightarrow$  pay attention to the exact meaning of words!  
*Example.* Each of  $n$  cards has a number on one side and a letter on the other. Given **B 2 5 J**, which cards do you need to turn to test the rule that if there is a **J** on one side, there must be a **5** on the other side?
  - Thinking with symbols and abstract generic objects
  - Modeling practical computing scenarios using standard math abstractions (sets, relations, functions, posets, graphs, trees)
  - Computing the resources required to store, process, and create various computational structures that meet specific requirements

2

2

## Course Contents

- This class is about the use of **discrete structures** in computation, including:
  - Combinatorics and counting (including some review)
    - *Enumerative combinatorics* (count the # of structures of a given kind)
    - *Combinatorial designs* (find a structure meeting certain criteria)
    - *Extremal combinatorics* (how big/small must it be to satisfy criteria?)
    - *Combinatorial optimization* (find the “best” structure among all that satisfy given criteria)
  - Advanced counting techniques
  - Discrete probability theory and probabilistic reasoning
  - Relations: Binary, equivalence, total and partial orders
  - Graph theory



*Example.* How many links must a network of size  $n$  have to guarantee that the network is connected? or to guarantee failure of a link or node does not disconnect the system?

3

3


## Required Background

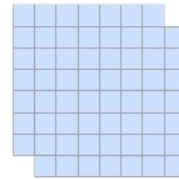
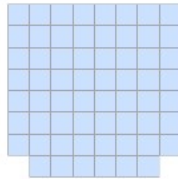
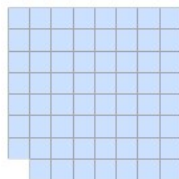
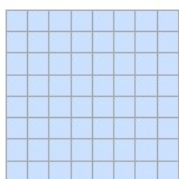
- Main prerequisite is sufficient *mathematical maturity*, i.e., the ability to follow and write an argument consisting of a sequence of statements, each of which follows from previous statements according to the laws of logic
- Elementary math functions: polynomials, logarithms, exponentials
- Sets and functions
- Propositional and predicate logic
- Proof techniques: induction, direct proof, proof by contradiction, proof by cases
  - Why some arguments are convincing while others are not?
  - What do you need to do to leave no room for doubt?
- Basic counting: permutations and combinations

4

4

## Warmup 1

- Which of the following “chessboards” can be tiled with  $2 \times 1$  domino pieces ? Prove your claim



- Can you state a *general rule* that distinguishes between tileable and non-tileable chessboards missing two arbitrary cells?
- Can you generalize your findings to  $n \times n$  boards missing two cells? Can you handle some special cases, e.g., when  $n$  is a power of two?

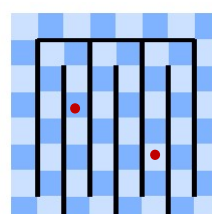
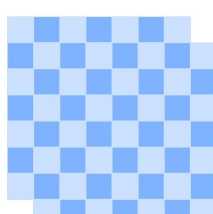
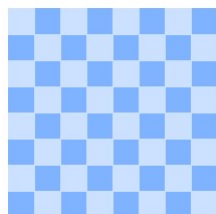
5

5

## Warmup...

*Claim.* Let  $B$  be a chessboard with 2 missing cells.  $B$  can be tiled **iff** the 2 missing cells have opposite colors

- If the cells have opposite colors, **then**  $B$  can be tiled ( $\Leftarrow$ )
- If  $B$  can be tiled, **then** the 2 cells have opposite colors ( $\Rightarrow$ )



6

6

## Warmup 2

- The following fragment sorts a list  $A$  of items from a *totally ordered set*

```

1  for  $i \leftarrow 1$  to  $n - 1$ 
2      do for  $j \leftarrow i + 1$  to  $n$ 
3          do if  $A[i] > A[j]$ 
4              then swap  $A[i]$  with  $A[j]$ 

```

- How many times is the comparison in line 3 executed?
- The answer is not as important as the *pattern of reasoning*

The set  $S$  of comparisons can be partitioned into  $n - 1$  disjoint subsets

$S_1, \dots, S_{n-1}$ , where  $S_k$  is the set of comparisons when  $i = k$

Since  $|S_i| = n - i$ , we want  $(n - 1) + (n - 2) + \dots + 2 + 1$

**Addition Rule.** The size of a union of mutually disjoint finite sets is the sum of the sizes of the sets.

7

7

## Exercise

- What is the value of the following sum?

$$\begin{array}{rccccccc}
 & & \leftarrow 13 \rightarrow & & & & \\
 F \rightarrow & 89+ & 102+ & 115+ & 128 & +141+ & \\
 & 154+ & & \dots & & +206+ & \\
 & 219+ & & \dots & & +271+ & \\
 & 284+ & & \dots & & +336+ & \\
 & 349+ & & \dots & & +401+ & \\
 & 414+ & & \dots & & +466 \leftarrow L & 
 \end{array}$$

- Can you derive a formula for a general pattern?

*Hint.* The answer depends on the number of terms  $n$ , the first term  $F$  and the last term  $L$

8

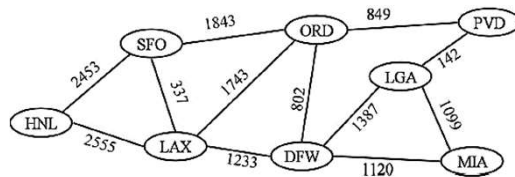
8

## Warmup 3

- Given a list of airports serviced by an airline (e.g., HNL, SFO, LAX, ORD, DFW, LGA, PVD, MIA)
  - How many different nonstop routes\* can the airline offer?
  - What is the smallest number of non-stop routes the airline must offer so that there is a way (possibly with connections) to get to any airport from any other airport in the list
  - Can you decide if it is possible to offer a set of nonstop routes, each no longer than  $m$  miles, that allows you to get from any airport to any other airport?
  - How do you visit all airports while minimizing flying time?
  - How to you test all routes while minimizing flying time?
  - Can you get from  $A$  to  $B$  even if an arbitrary airport closes

\* If  $(A, B)$  is a route, the airline offers flights from  $A$  to  $B$  as well as flights from  $B$  to  $A$ .

HNL	SFO	2453	ORD	DFW	802
HNL	LAX	2555	ORD	PVD	849
SFO	ORD	1843	DFW	LGA	1387
SFO	LAX	337	DFW	MIA	1120
LAX	ORD	1743	LGA	PVD	142
LAX	DFW	1233	LGA	MIA	1099

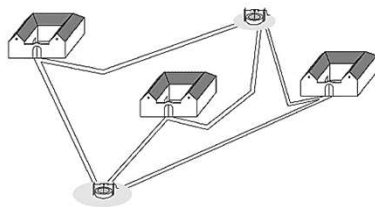


9

9

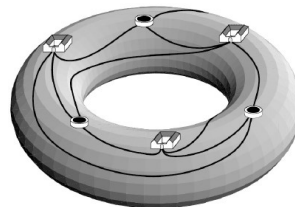
## Warmup 4

- When can you lay out  $n$  houses and  $m$  wells with paths from each house to each well that do not cross?



$n = 3, m = 2$

- Can you do  $n = 3, m = 3$ ?



*Always understand the unstated assumptions!*

10

10

## Notation

- Common sets of numbers

$\mathbb{Z}$  denotes the set of *integers*  $0, \pm 1, \pm 2, \pm 3, \dots$

$\mathbb{N}$  denotes the set of *natural* numbers or counting integers  $0, 1, 2, 3, \dots$

$\mathbb{Z}_n$  is the finite set  $\{0, 1, \dots, n-1\}$ , i.e., the set of integers modulo  $n$  (for  $n > 0$ )

$\mathbb{Q}$  is the set of *rational* numbers, i.e., ratios of integers

$\mathbb{R}$  is the set of *real* numbers

The set  $\mathbb{R} - \mathbb{Q}$  are the *irrational* numbers, e.g.,  $\pi, \sqrt{2}$

- If  $x \in \mathbb{R}$ ,

$\lfloor x \rfloor$  is the largest integer  $z \leq x$ , e.g.,  $\lfloor \sqrt{2} \rfloor = 1$

$\lceil x \rceil$  is the smallest integer  $z \geq x$ , e.g.,  $\lceil \sqrt{2} \rceil = 2$

- If  $a_1, a_2, \dots, a_n$  are numbers

$$\sum_{i=1}^n a_i = a_1 + a_2 + \dots + a_n \quad \text{and} \quad \prod_{i=1}^n a_i = a_1 \cdot a_2 \cdots a_n$$

11

11

## Exercise

- For which values of  $x$  is  $\sqrt{x}$  irrational?  
(an irrational number cannot be stored using floats)
- Can you find irrational numbers  $x$  and  $y$  such that  $x^y$  is rational?  
*Hint.* What can you say about  $x^y$  when  $x = y = \sqrt{2}$ ? Why?

12

12

## Exercise

- What is the value of the following expressions?

$$\lfloor -3.2 \rfloor \quad \sum_{i=1}^3 \frac{1}{2i} \quad \sum_{i=1}^n \sum_{j=1}^n (i+j) \quad \prod_{i=1}^{99} \frac{i+1}{i}$$

- Can you give a good approximation for the following sum when  $n$  is large?

$$\sum_{i=1}^n \frac{1}{2i}$$

13

13

## Exercise

- Recall that if  $A$  and  $B$  are  $n \times n$  matrices, the product  $C = A \times B$  is also an  $n \times n$  matrix defined as:

$$c_{ij} = \sum_{k=1}^n a_{ik} \cdot b_{kj}$$

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \begin{bmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ b_7 & b_8 & b_9 \end{bmatrix} = \begin{bmatrix} c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 \\ c_7 & c_8 & c_9 \end{bmatrix}$$

- How many scalar multiplications and scalar additions are performed when multiplying  $A \times B$ ?
- How many when computing  $A^n$ ?

14

14

## Logarithms

- Given reals  $a > 1$  and  $b > 0$ , the logarithm of  $b$  in base  $a$  is defined as

$$\log_a b = c \text{ iff } a^c = b$$

- Convention:  $\log b = \log_2 b$  and  $\ln b = \log_e b$

- Properties

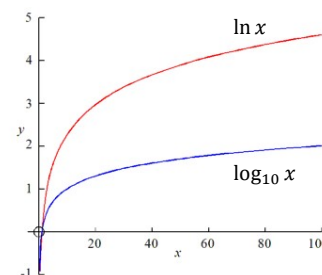
$$b^{\log_b a} = a$$

$$\log_c(ab) = \log_c a + \log_c b$$

$$\log_b a^n = n \log_b a$$

$$\log_b 1/a = -\log_b a$$

$$\log_b a = \log_c a / \log_c b$$



15

15

## Exercise

- Without using a calculator:
  - Explain why  $1 < \log_2 3 < 2$
  - Find  $\lfloor \log_3 24 \rfloor$
  - Find  $\lfloor \log_4 100 \rfloor$
- Exactly, how many *decimal* digits does integer  $x > 0$  require?
  - For example, 8 requires 1 digit while 256 requires 3
- How many bits are needed to store  $8^{100} - 3$ ?
- How many bits are needed to store  $4^{4^4} - 1$ ?
- Given a sorted list  $A$  of natural numbers and  $x \in \mathbb{N}$ , how many comparisons do you need to perform in order to determine if  $x \in A$ ?

16

16



## Functions

- Let  $X$  and  $Y$  be sets. Informally, a *function* is a rule that assigns to each element of  $X$  exactly one element of  $Y$

Example:  $f(x) := \frac{1}{1+x}, x \in \mathbb{R}_{\geq 0}, g(x) = 0x1x, x \in \{0,1\}^*$

- Definition.** A *function*  $f$  from a set  $X$  into a set  $Y$  is a set of ordered pairs  $(x, y)$  with  $x \in X$  and  $y \in Y$  such that for any  $x \in X$ , there is exactly one pair whose first component is  $x$
- We say that  $f$  *maps*  $X$  to  $Y$  or that  $f$  is a *mapping* from  $X$  to  $Y$
- We refer to  $X$  and  $Y$  as the *domain* and *codomain* of  $f$

*Question.* What computational artifacts (data structures, algorithms) can we use to represent  $f$ ?

17

17

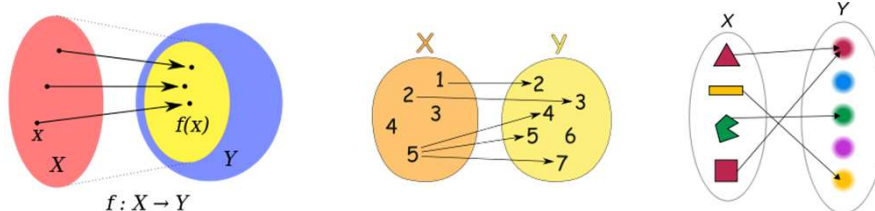
## Notation

- $f: X \rightarrow Y, x \mapsto y$
- $\text{Domain}(f) = X$  and  $\text{Codomain}(f) = Y$
- Given  $S \subseteq X$ , the *image* of  $S$  under  $f$  is defined as:

$$f(S) = \{f(x) : x \in S\}$$

- The *range* of  $f$  is defined as:

$$\text{Range}(f) = f(X) = \{f(x) : x \in X\}$$



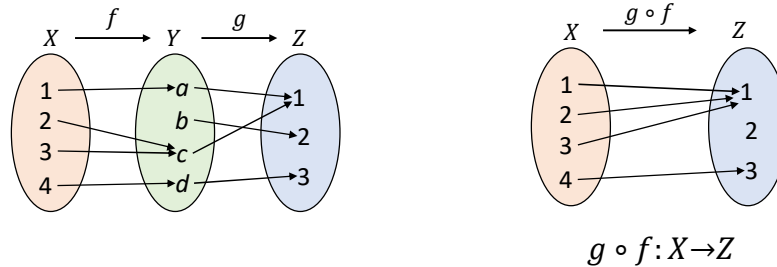
18

18

## Function Composition

- It is often useful to apply several functions in sequence, so that the output of one is the input to the next one

$$(g \circ f)(x) = g(f(x))$$

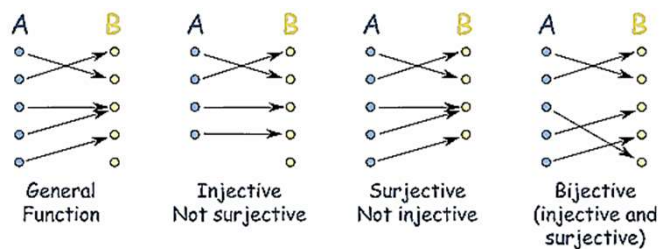


19

19

## Special Types of Functions

- A function  $f: X \rightarrow Y$  is called **One-to-one** or **injective** if  $x \neq y \Rightarrow f(x) \neq f(y)$ . We write  $f: X \hookrightarrow Y$   
**Onto** or **surjective** if for every  $y \in Y$  there is  $x \in X$  such that  $f(x) = y$ , i.e., the range of  $f$  is the same as its codomain  
**Bijective** if it is both one-to-one and onto

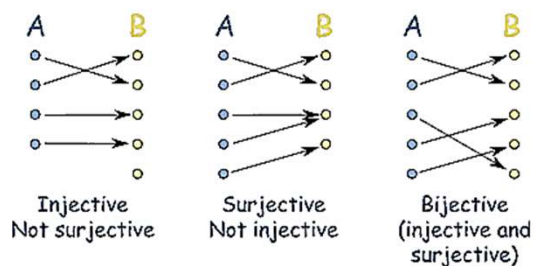


20

20

## Consider a function $f: X \rightarrow Y$

- For a one-to-one (injective) function, each element of  $Y$  has *at most* one incoming arrow
- For an onto (surjective) function each element of  $Y$  has *at least* one incoming arrow
- For a bijective (both one-to-one and onto) function, each element of  $Y$  has *exactly* one incoming arrow



21

21

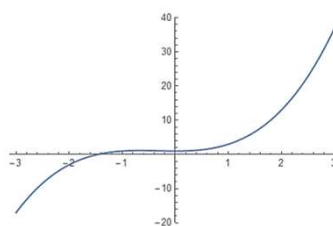
## Exercise

Which of the following functions  $\mathbb{Z} \rightarrow \mathbb{Z}$  are injective?

Which ones are surjective?

Which ones are bijective?

- $x \mapsto x + 2$
- $x \mapsto x^2 + 2$
- $x \mapsto x^3 + x^2 + 1$



*Exercise.* Is your answer the same if we change the domain and codomain to  $\mathbb{N}$ ? if we change it to  $\mathbb{R}$ ?

22

22

## Properties of function composition

**Claim.** Let  $f: X \rightarrow Y$  and  $g: Y \rightarrow Z$  be functions. Then

1. If  $f$  and  $g$  are injective, then  $g \circ f$  is also injective
2. If  $f$  and  $g$  are surjective, then  $g \circ f$  is also surjective
3. If  $f$  and  $g$  are bijective, then  $g \circ f$  is also bijective
4. For any function  $f: X \rightarrow Y$  there exists a set  $Z$ , a bijection  $h: Z \hookrightarrow Y$ , and a surjection  $g: X \rightarrow Z$ , such that  $f = h \circ g$ .

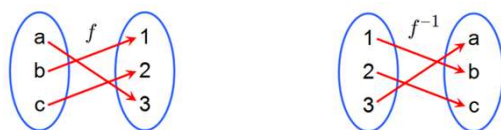
*Exercise.* Statement (4) says that *any* function can be written as a composition of an injective function and a surjective function. Prove this claim.

23

23

## Inverse Functions

- If  $f: X \hookrightarrow Y$  is a bijection, then the inverse function  $f^{-1}: Y \hookrightarrow X$  is also a bijection defined as  $f^{-1}(y) = x$  iff  $y = f(x)$



*Exercise.* Given a bijection  $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  describe an efficient algorithm to compute  $f^{-1}$

*Hint.* Since the domain of  $f$  is finite, we can represent  $f$  using an array

24

24

## Partial Functions

- Sometimes, we may want to allow a function to be undefined for some domain elements.
- A function defined on all domain elements is called a **total function**; otherwise, it is a **partial function**
- From now on, the term *function* includes *both* partial and total functions

*Example.* On domain  $\mathbb{R}$ ,  $f(x) = 1/(x^2 - 1)$  is partial while  $g(x) = 1/(x^2 + 1)$  is total

*Remark.* Algorithms, in general, can be viewed as definitions of functions from  $\mathbb{N} \rightarrow \mathbb{N}$ . Why?

Are these functions partial or total?

25

25

## Pigeonhole Principle



[Wikipedia:](https://en.wikipedia.org/wiki/Pigeonhole_principle)

[https://en.wikipedia.org/wiki/Pigeonhole\\_principle](https://en.wikipedia.org/wiki/Pigeonhole_principle)

26

26

## Warmup

- If you own three colors of socks, how many socks do you need to take in the dark to guarantee that you have a matching pair?
- Are there two different subsets of the list below that add up to the same value?

4815379351865384279613427	5332822657075235431620317	5173920083651862307925394	9270880194077636406984249
5692168374637019617423712	8247331000042995311646021	1843971862675102037201420	4837052948212922604442190
0489445991866915676240992	3208234421597368647019265	7215654874211755676220587	9324301480722103490379204
5800949123548989122628663	8496243997123475922766310	2396951193722134526177237	5106389423855018550671530
1082662032430379651370981	3437254656355157864869113	7256932847164391040233050	9436090832146695147140581
6042900801199280218026001	8518399140676002660747477	2781394568268599801096354	5142368192004769218069910
1178480894769706178994993	3574883393058653923711365	3171004832173501394113017	9475308159734538249013238
6116171789137737896701405	8543691283470191452333763	2796605196713610405408019	5181234096130144084041856
1253127351683239693851327	3644909946040480189969149	7426441829541573444964139	9492376623917486974923202
6144868973001582369723512	8675309258374137092461352	2931016394761975263190347	5198267398125617994391348
1301505129234077811069011	3790044132737084094417246	7632198126531809327186321	9511972558779880288252979
6247314593851169234746152	8694321112363996867296665	2933458058294405155197296	5317592940316231219758372
131156711143866433882194	3870332127437971355322815	7712154432211912882310511	9602413424619187112552264
6814428944266874963488274	8772321203608477245851154	3075514410490975920315348	5384358126771794128356947
1470029452721203587686214	4080505804577801451363100	7858918664240262356610010	9631217114906129219461111
6870852945543886849147881	8791422161722582546341091	8149436716871371161932035	3157693105325111284321993
1578271047286257499433886	4167283461025702348124920	3111474985252793452860017	5439211712248901995423441
691495508120950093732397	9062628024592126283973285	7898156786763212963178679	9908189853102753335981319
1638243921852176243192354	423599683112377788211249	3145621587936120118438701	5610379826092838192760458
6949632451365987152423541	9137845566925526349897794	8147591017037573337848616	9913237476341764299813987
1763580219131985963102365	4670939445749439042111220	3148901255628881103198549	5632317555465228677676044
7128211143613619828415650	9153762966803189291934419	5763257331083479647409398	8176063831682536571306791
1826227795601842231029694	0020480135385502964448038		

27

27

## Exercise

- For an arbitrary integer  $n > 0$ , construct a set of  $n$  positive integers such that all its subsets have distinct sums

*Note:* your algorithm must work for *any*  $n$

*Example.* If  $n = 5$ , one solution is

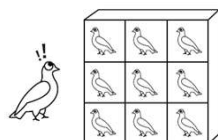
$\{6, 9, 11, 12, 13\}$

28

28

## Pigeonhole Principle

**Basic Pigeonhole Principle.** If  $n + 1$  objects are placed into  $n$  boxes, then at least one box contains two or more objects



*Proof.* By contradiction.

**Example.** Among 13 people there are at least two whose birthdays fall in the same month.

**Note.** Claim is tight and non-constructive

**Alternative phrasing.** Let  $X$  and  $Y$  be finite sets and  $f: X \rightarrow Y$  a function from  $X$  to  $Y$ . Then, if  $|X| > |Y|$  then  $f$  is not 1-1

29

29

## Example

Given a sequence  $m$  integers  $a_1, a_2, \dots, a_m$ , there is  $1 \leq k \leq h \leq m$  such that  $a_k + a_{k+1} + \dots + a_h$  is divisible by  $m$

*Proof.* Consider the  $m$  sums  $a_1, a_1 + a_2, \dots, a_1 + \dots + a_m$ . If any of these is divisible by  $m$  then the conclusion holds. Otherwise, each sum  $\neq 0 \pmod{m}$ , i.e.,  $a_1 + \dots + a_j \pmod{m} \in \{1, \dots, m-1\}$ .

Therefore, there are two sums that are equal (mod  $m$ ):  $a_1 + \dots + a_k = a_1 + \dots + a_h = r \pmod{m}$ , and  $a_{k+1} + \dots + a_h$  is divisible by  $m$  ■

**Exercise.** Describe and analyze an efficient algorithm to find a contiguous subsequence of  $a_1, a_2, \dots, a_m$  that is divisible by  $m$

30

30

## Exercise

Suppose you choose 101 integers from the set  $\{1, 2, \dots, 200\}$ . Show that among the integers chosen there are two such that one of them is divisible by the other.

*Hint.* Express each integer as an odd number multiplied by a power of two.

31

31

## Variants and Generalizations

**Generalized Pigeonhole Principle.** Let  $q_1, \dots, q_n$  be positive integers. If  $q_1 + \dots + q_n - n + 1$  objects are placed into  $n$  boxes, then for each  $1 \leq i \leq n$ , there is a box containing at least  $q_i$  objects

**Variant 1.** If  $n(r - 1) + 1$  objects are placed into  $n$  boxes, then one of the boxes contains  $r$  or more objects

Equivalently, if  $X$  and  $Y$  are finite sets with  $|X| > (r - 1)|Y|$  then every function  $f: X \rightarrow Y$  maps at least  $r$  elements of  $X$  to the same element of  $Y$

**Variant 2.** If  $n$  integers  $m_1, \dots, m_n$  have an average greater than  $r - 1$ , then at least one of the integers is greater than or equal to  $r$

32

32



## Example (Paul Erdős)

**Claim.** Let  $n$  be an arbitrary positive integer. If  $n^2 + 1$  people are lined up shoulder to shoulder in a straight line, then it is always possible to choose  $n + 1$  of the people to take one step forward so that, from left to right, they appear sorted by height (either increasingly, or decreasingly).

Equivalently, *every* sequence  $a_1, \dots, a_{n^2+1}$  of numbers contains an increasing or decreasing subsequence of length  $n + 1$

*Note.* The target sequence need not be contiguous.

*Example.* For  $\langle 8, 7, 5, 11, 9, 3, 6, 4, 12, 2 \rangle$ , with  $n = 3$ , the longest increasing subsequence has length 3, but there is a decreasing sequence, e.g.,  $\langle 8, 7, 4, 2 \rangle$ , of length 4.

*Proof.* Let  $a_1, \dots, a_{n^2+1}$  be an arbitrary sequence of numbers.

We consider two cases. If there is an increasing subsequence of length  $n + 1$  we are done! Therefore, for the rest of the argument we assume that there is *no* increasing subsequence of length  $n + 1$ . We show then that there must be a decreasing subsequence of length  $n + 1$ .

*Continued on next page...*

33

33

## Proof...

*Proof.* Let  $a_1, \dots, a_{n^2+1}$  be our sequence of numbers.

Suppose there is *no* increasing subsequence of length  $n + 1$  (else we are done!). We will show that this implies that there must be a decreasing subsequence of length  $n + 1$ .

For each  $k = 1, \dots, n^2 + 1$ , let  $m_k$  be the length of the longest increasing subsequence that starts with  $a_k$ . We must have  $m_k \leq n$  for each  $k$  (by our assumption above).

Since  $m_k \geq 1$ , the  $n^2 + 1$   $m_i$ 's are integers between 1 and  $n$ . By Variant 1 of Pigeonhole, with  $r = n + 1$ , we can distribute  $n(r - 1) + 1$  integers into  $n$  boxes by their value.

Therefore, one of the boxes contains at least  $r = n + 1$  integers, i.e.,  $n + 1$  of the  $m_i$ 's are equal, say  $m_{k_1} = m_{k_2} = \dots, m_{k_{n+1}}$ , with  $1 \leq k_1 < k_2 < \dots < k_{n+1} \leq n^2 + 1$ .

Suppose  $\exists i, a_{k_i} \leq a_{k_{i+1}}$ . Then, since  $k_i < k_{i+1}$  we can take a longest increasing sequence starting with  $a_{k_{i+1}}$  and make it longer by prefixing it with  $a_{k_i}$ . But then  $m_{k_i} > m_{k_{i+1}}$ , contradicting the fact that  $m_{k_i} = m_{k_{i+1}}$ . Thus,  $a_{k_i} > a_{k_{i+1}}$  for every  $i = 1, \dots, n$ .

Since  $a_{k_i} > a_{k_{i+1}}$ , for all  $i = 1, \dots, n$ , it follows  $a_{k_1} > a_{k_2} > \dots > a_{k_{n+1}}$ , a decreasing subsequence of length  $n + 1$  ■

34

34

## Related Principles

The following principles, related to Pigeonhole, are sometimes useful:

1. If  $n$  objects are put into  $n$  boxes and no box is empty, then each box contains exactly one object.
2. If  $n$  objects are put into  $n$  boxes and no box gets more than one object, then each box contains exactly one object.
3. If  $n$  objects are put into  $n + 1$  boxes, then at least one box is empty

35

35

## Exercise

Consider the following game. Two players receive a **sequence** of 0s and 1s. Starting with the given sequence of length  $n$ , they alternate their moves. In each move, a player appends 0 or 1 to the end of the current sequence. A player loses if his digit completes a block of  $n$  consecutive digits that has already appeared before (the two occurrences may overlap).

*Example.* For  $n = 4$  and sequence **0010**00**0110**11**1100**1 player 2 will lose

Is the game guaranteed to terminate? If so, provide an upper bound on the number of moves before termination; otherwise, describe a sequence that will force the game to go on indefinitely

36

36

## Ramsey's Theorem

Prove that given six or more people, either there are three, each pair of whom are acquainted, or there are three, each pair of whom are unacquainted.

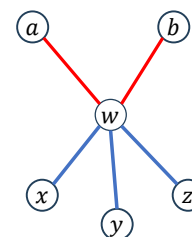
*Proof.* The first step is to find a suitable abstraction.

We model the problem by using a complete graph with six vertices.

For every pair of vertices  $u$  and  $v$ , the edge between  $u$  and  $v$  is colored blue if  $u$  and  $v$  know each other, and red, otherwise.

Consider any vertex  $w$  and its 5 incident edges. The *Generalized Pigeonhole Principle* guarantees that at least three of these edges have the same color (all blue **or** all red).

Assume three are blue meeting vertices  $x, y, z$ . If any of the edges joining  $x, y, z$ , say  $xy$  is blue we have a trio  $\{w, x, y\}$  of mutual acquaintances; otherwise, no pair from  $\{x, y, z\}$  know each other.



37

37

## Exercise

- Let  $X = \langle x_1, x_2, \dots, x_n \rangle$  be a list of  $n$  distinct numbers, in no particular order
- Elements  $x_i$  and  $x_j$  are *neighbors* if they would be adjacent had  $X$  been sorted, i.e., if  $x_i < x_j$  and there is no  $h \neq i, j$ , with  $x_i < x_h < x_j$   
*Example.* If  $X = \langle 2, 7, 5, 12, 11 \rangle$ ,  $(2, 5)$  and  $(11, 12)$  are pairs of neighbors
- We consider two related problems:
  1. In the *minimum-gap* problem, you want to find a *closest pair* of neighbors
  2. In the *maximum-gap* problem, you want to find a *farthest pair* of neighbors*Example.* If  $L = \langle 2, 7, 5, 12, 11 \rangle$ , the minimum-gap is  $12 - 11 = 1$  and the maximum-gap is  $11 - 7 = 4$
- How fast can you solve these problems?
  - Trivially solved in sub-quadratic time (how?)
- Can you find faster solutions by making use of the pigeonhole principle, or one of its variants? *Hint.* Partition the range of  $X$  into  $n - 1$  buckets

38

38

# Double Counting

$$A \begin{array}{|c|} \hline \\ \hline \\ \hline \\ \hline \\ \hline \\ \hline \end{array} = \begin{array}{|c|} \hline \\ \hline \\ \hline \\ \hline \\ \hline \\ \hline \end{array} \quad \sum_{i=1}^n \sum_{j=1}^m A_{ij} = \sum_{j=1}^m \sum_{i=1}^n A_{ij}$$

[Wikipedia:](https://en.wikipedia.org/wiki/Double_counting_(proof_technique))

[https://en.wikipedia.org/wiki/Double\\_counting\\_\(proof\\_technique\)](https://en.wikipedia.org/wiki/Double_counting_(proof_technique))

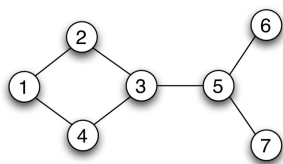
39

39

## Warmup

- At the end of a party, the host asks each of the guests how many times they shook hands. She gets the following counts (including her own):  
2, 5, 1, 3, 1, 0, 4, 2, 3
- Did everyone report an accurate count?

**Claim (Handshaking Lemma).** Every simple undirected graph contains an even number of vertices of odd degree.



40

40

## Double Counting

- A proof technique for demonstrating that two expressions are equal by showing that they are simply two ways of counting the size of the same set
  - *By counting the same set in two different ways we get interesting results*
- *Approach.* Describe a set from two perspectives. This results in two different expressions for its size which, consequently, must be equal to each other
- *Challenge.* Decide what needs to be double-counted

*Example.* Show that  $S_n = 1 + 9 + \dots + 9^n = (9^{n+1} - 1)/8$ .

Let  $S_i$  be the quantity to be double-counted.

On one hand,  $S_{n+1} = S_n + 9^{n+1}$ ; on the other,  $S_{n+1} = 1 + 9 \cdot S_n$

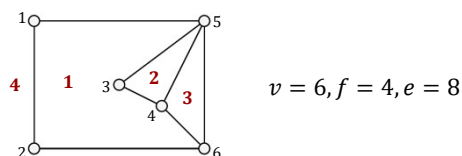
This implies the desired result.

41

41

## Example

- A *planar graph* is a graph  $G$  that can be drawn with no edge crossings
  - $G$  partitions the plane into  $v$  vertices,  $e$  edges and  $f$  faces



- If  $s_i$  is the size of the  $i^{\text{th}}$  face then 
$$e = \frac{1}{2} \sum_{i=1}^f s_i$$

$$\begin{aligned} s_1 &= 6 \\ s_2 &= 3 \\ s_3 &= 3 \\ s_4 &= 4 \end{aligned}$$

- If  $d_j$  is the degree of the  $j^{\text{th}}$  vertex then 
$$e = \frac{1}{2} \sum_{j=1}^v d_j$$

$$\begin{aligned} d_1 &= 2 \\ d_2 &= 2 \\ d_3 &= 2 \\ d_4 &= 3 \\ d_5 &= 4 \\ d_6 &= 3 \end{aligned}$$

42

42

## Example

- In a class of 10 students everyone solved three problems from the homework, and each problem was solved by two students. What is the number  $k$  of problems in the homework?
- Imagine a table recording who solved what

	1	2	3	4	5	...	$k$
Alice	✓	✓			✓		
Bob		✓	✓	✓			
Charlie	✓		✓		✓		
⋮	⋮						

- How many problems were solved in total?
- $\sum \text{ of columns} = 2k = \sum \text{ of rows} = 3 \cdot 10 \Rightarrow k = 15$

43

43

## Exercise

- In the next assignment (for the same group of 10 students), every student solved more than half of the problems. Is it possible that no problem was solved by more than half of the students?
- Now, suppose that in the same class (again, 10 students) every girl knows 3 boys and every boy knows 2 girls. How many students are boys?
  - What should you double count?

44

44

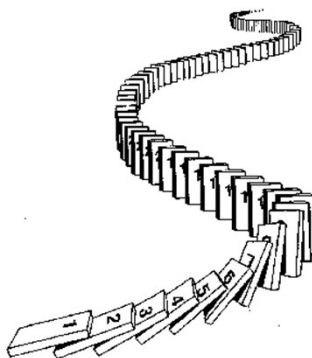
## Exercise

- Using double-counting compute the number of triples  $(a, b, c)$  which satisfy  $a, b, c \in \{1, 2, \dots, n\}$ ,  $a < c$ , and  $b < c$
- How many triples  $(a, b, c)$  of numbers satisfy  $a, b, c \in \{1, 2, \dots, n\}$  and  $a < b < c$ ?

45

45

## Mathematical Induction



### Section 1.3

46

46

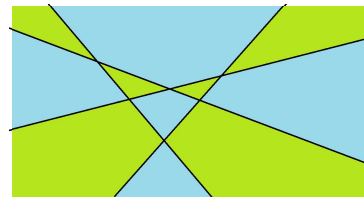
## Warmup

- The **four-color map theorem** states that no more than four colors are needed to color the regions of any map so that no two adjacent regions<sup>†</sup> have the same color



<sup>†</sup>Adjacent means that two regions share a common boundary *segment*, not merely a corner where three or more regions meet.

- A number of lines are drawn in the plane, dividing it into regions. Can the regions be 2-colored in such a way that no two adjacent regions have the same color?

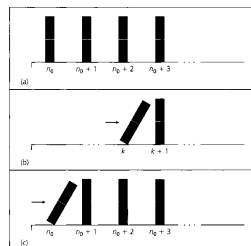


47

47

## Induction

- A powerful technique to prove properties of arbitrarily large sets of natural numbers, including all of  $\mathbb{N}$
- In practice, induction can be used to prove properties about other mathematical structures, such as sets, graphs, trees, algorithms, etc.
- Main idea captured by a simple metaphor



- 1-1 correspondence between natural numbers and dominos
- If one domino falls, the next falls
- If the first domino falls, all dominos fall

48

48



## Principle of Mathematical Induction

Let  $X$  be a set of natural numbers with the following properties:

1. The number 0 belongs to  $X$  (*base case*)
2. If a natural number  $k$  belongs to  $X$ , then  $k + 1$  also belongs to  $X$  (*inductive step*)

Then  $X = \mathbb{N}$

- Use when you want to prove that every natural number  $n$  satisfies a certain property  $P(n)$
- We can use induction to prove properties about other mathematical structures (sets, graphs, trees, algorithms)
  - The key is to express the goal in terms of a property  $P$  of natural numbers

49

49

## Template for Induction Proofs

1. **State that the proof uses induction.** This immediately conveys to the reader the overall structure of the proof, making it easier to follow the argument.
2. **Define an appropriate predicate  $P(k)$ .** The eventual conclusion of your argument will be that  $P(k)$  holds for all natural numbers  $k$ . This predicate, when assumed true, is referred to as the *inductive hypothesis*.
3. **Prove that  $P(0)$  is true.** This step, called the *base case* is usually easy to prove by direct verification. More than one base case may be required
4. **Prove that  $P(k)$  implies  $P(k + 1)$ , for all  $k \in \mathbb{N}$ .** This is the *inductive step*. We are not claiming that either  $P(k)$  or  $P(k + 1)$  are true. Even though the statements  $P(k)$  and  $P(k + 1)$  look similar, bridging the gap may be tricky.
5. **Invoke induction.** Given 1-4 the induction principle allows you to conclude that  $P(k)$  holds for all natural numbers.

50

50

## Example

- Prove that  $\sum_{i=0}^n 2^i = 2^{n+1} - 1$  for all  $n \in \mathbb{N}$
- What is the predicate  $P(k)$ ?  
 $P(k)$  is the property of  $k$  that  $1 + 2 + \dots + 2^k = 2^{k+1} - 1$
- *Base case*: Is  $P(0)$  true? or  $P(k-1) \Rightarrow P(k)$
- *Inductive step*: show  $P(k) \Rightarrow P(k+1)$   
 We assume  $P(k)$ , i.e., assume that  $\sum_{i=0}^k 2^i = 2^{k+1} - 1$   
 Need to show that, under this assumption,  $P(k+1)$  also holds

$$\sum_{i=0}^{k+1} 2^i = 2^{k+1} + \sum_{i=0}^k 2^i = 2^{k+1} + 2^{k+1} - 1 = 2^{k+2} - 1$$

51

51

## Exercise

Prove each of the following by induction

a)  $1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$

b)  $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \dots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$

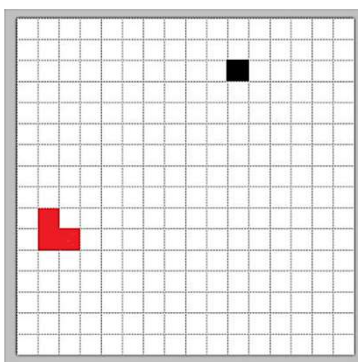
c)  $\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$

52

52

## Exercise

- Consider a  $2^n \times 2^n$  grid with an arbitrary cell removed (shown in black)
- Prove that such board can be tiled with L-shapes consisting of 3 cells each (shown in red)

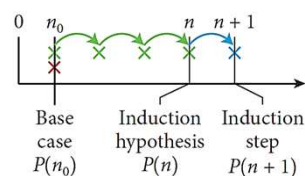


53

53

## Variants

- Use induction to prove properties of a subset of  $\mathbb{Z}$  of the form  $\{x \in \mathbb{Z}, x \geq n_0\}$



- Can strengthen the inductive hypothesis by assuming it holds for *all* natural numbers  $\leq k$  (**strong induction**). Then, the inductive step becomes:

$$\{P(0), P(1), \dots, P(k)\} \Rightarrow P(k+1)$$

*Exercise.* Prove that every integer greater than 1 can be expressed uniquely as a product of prime numbers listed in ascending order

54

54

## Exercise

- Following the induction template, prove that 3 and 5 cent coins can be used to produce *any* amount of change greater than 7 cents
- What are the base cases
- What is the inductive hypothesis?

55

55

## Exercise

- What is wrong with the following proof that all horses have the same color?

**Theorem.** In every set of  $n > 0$  horses, all the horses are of the same color

*Proof.* We proceed by induction on  $n$ .

*Base case.* If there is only one horse, the claim is true.

*Inductive step.* Assume that any set of  $n$  horses is monochromatic

Let  $H = \{h_1, h_2, \dots, h_n, h_{n+1}\}$  be an *arbitrary* set of  $n + 1$  horses. Consider the sets  $H_1 = \{h_1, \dots, h_n\}$  and  $H_2 = \{h_2, \dots, h_{n+1}\}$

Since  $|H_1| = |H_2| = n$ , each  $H_i$  is monochromatic

Thus,  $h_2, \dots, h_n$  have the same color

Since  $h_1$  has the same color as  $h_2$  and  $h_n$  has the same color as  $h_{n+1}$  we conclude that all horses of  $H$  have the same color.

By induction, all horses have the same color

56

56

## Well-Ordering Principle (WOP)

*Any non-empty subset of natural numbers contains a smallest element.*

- The well-ordering principle, (regular) induction, and strong induction are all equivalent!
  - Each one of the principles implies the other two
- While all equivalent, some arguments are best expressed using the well-ordering principle
- As obvious as the principle may sound, it *does not* hold for real or even rational numbers!

*Exercise.* Show that if the WOP is correct, then the principle of induction is correct.

57

57

## Example

*Claim.* Every integer  $n > 1$  can be factored as a product of primes.

*Proof* (by WOP).

Let  $C$  be the set of integers  $> 1$  that *cannot* be factored into primes.

For the sake of contradiction, assume that  $C$  is not empty.

The WOP implies that  $C$  has a smallest element  $s$  which cannot be prime (why?)

But then,  $s = a \cdot b$ , where  $1 < a, b < s$ . Since  $p \notin C, q \notin C$  (else,  $s$  would not be smallest) they have prime factorizations  $p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_m}$  and  $p_{j_1} \cdot p_{j_2} \cdot \dots \cdot p_{j_n}$ , respectively

Writing  $s = p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_m} \cdot p_{j_1} \cdot p_{j_2} \cdot \dots \cdot p_{j_n}$  contradicts  $s \in C$  so  $C$  is empty. ■

*Question.* Does the proof above imply that the factorization of  $n$  into primes is unique (up to ordering of the prime factors)?

58

58

## Template for WOP proofs

- To prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  using the WOP:
  1. **State that the proof uses the WOP.** This announces the overall structure of the proof.
  2. **Define  $P(n)$ .** May need to be clever in defining  $n$  in terms of the variables involved.
  3. **Define the set  $C$  of counter examples to  $P$ .** Specifically,  $C := \{n \in \mathbb{N} : P(n) \text{ is false}\}$ .
  4. **Assume claim is false.** To prove by contradiction, assume that  $C$  is non-empty.
  5. **Invoke WOP.** The non-empty set  $C$  must contain a smallest element  $s \in C$ .
  6. **Reach a contradiction.** This might involve showing that  $P(s)$  is true or that there is a member of  $C$  smaller than  $s$  (this is the open-ended part of the proof).
  7. **Conclusion.** The contradiction implies that  $C$  is empty, i.e., there are no false cases.

59

59

## Exercise

- Using the Well Ordering Principle prove that the following equation admits no solution where  $x, y, z \in \mathbb{N}$

$$4x^3 + 2y^3 = z^3$$

*Hint.* There are different valid ways in which you could formulate  $P(n)$ . One of them is in terms of  $n = xyz$

60

60

## Invariants

- Invariants are important tools for proving properties of a system (a game, program, device, etc.) such as impossibility of certain events, termination, and various types of bounds
- The goal is to prove that a process preserves a certain property (the *invariant*) at *all* times
- An invariant may take many forms, including:
  - *Sign* (e.g., a variable never becomes negative)
  - *Parity* (e.g., a quantity of interest is always odd)
  - *Value* (e.g., a quantity does not change)
  - *Order*, e.g., (a section of an array is sorted)
  - *Logical proposition* (e.g., the altitude of a plane never drops below 1,000 feet without the landing gear being deployed)

61

61

## Invariants...

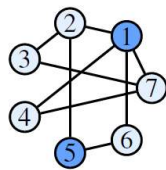
- Tools to reason about invariants include double counting, the well-ordering principle, and induction
- Double counting uses a sum invariant
- The well-ordering principle is based on showing that a relevant quantity never goes below a certain threshold
- To prove a property by induction, show that the property holds at the beginning (base case) and, if it holds after  $t$  steps, then it also holds after  $t + 1$  steps
  - To prove termination or to compute a bound, identify a non-negative quantity that decreases at every step
  - To prove impossibility, find a quantity that never changes

62

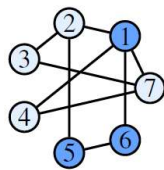
62

## A Toy Example

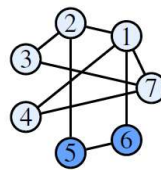
- Each citizen of a town supports one of two candidates for an election
- If among the friends of a citizen  $z$  there are more fans of the other candidate than the candidate preferred by  $z$ , then  $z$  changes their support to the other candidate
- In each time period (say, a day), one such citizen switches
- Is it possible that this switching process goes on forever?
- What is a good mathematical abstraction to model the problem?



day 0



day 1



day 2

day 3?

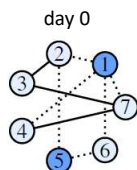
63

63

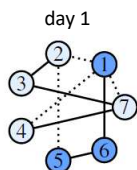
## Termination

- Is it possible for a large enough population and pattern of friendships that the process does not terminate?
- To show termination, find a non-negative quantity that decreases at every step
- A friendship between two friends is *shaky* if they favor opposite candidates
- How does the number of shaky friendships change with time?

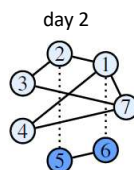
**Claim.** For any friendship network, the number of shaky connections decreases with every switch. Therefore, the network stabilizes in finite time.



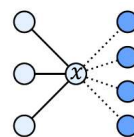
# shaky = 6



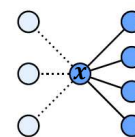
# shaky = 4



# shaky = 2



switch



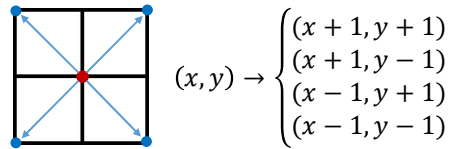
64

64



## Exercise

- You are programming a robot that moves along the cells of a regular grid.
- The robot starts at  $(0,0)$  and at each step it moves up or down one vertical unit and left or right one horizontal unit.



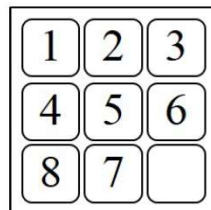
- How many steps does the robot need to reach cells  $(13,12)$  and  $(5,19)$ ?
- Can you design an algorithm that allows the robot to reach an arbitrary cell  $(s, t)$  using a minimum number of steps, or determine that the cell cannot be reached?

65

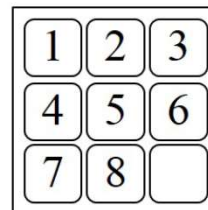
65

## Exercise

- The 8-puzzle consists of a  $3 \times 3$  board containing 8 tiles labeled 1 through 8 plus one empty space. You are given an initial and a final state
- Starting with the initial state, the goal is to repeatedly move tiles into the adjacent hole until the final configuration is reached.
- Show a solution to the instance below or explain why it cannot be solved



Initial State



Final State

66

66

## Exercise

- Prove that the following function correctly sorts an array  $A$  of  $n > 0$  integers

**Loop Invariant  $P(j)$ :** after completing iteration  $j$ ,  
 $A[1..j]$  is sorted, for all  $j \geq 1$

```

ISORT( $A, n$ )
1  for  $j \leftarrow 2$  to  $n$ 
2      do  $key \leftarrow A[j]$ 
3          ▷ Insert  $A[j]$  into the sorted sequence  $A[1..j-1]$ 
4           $i \leftarrow j - 1$ 
5          while  $i > 0$  and  $A[i] > key$ 
6              do  $A[i+1] \leftarrow A[i]$ 
7                   $i \leftarrow i - 1$ 
8           $A[i+1] \leftarrow key$ 
  
```

67

67

## The Unstacking Game

- On a stack of  $n$  boxes, you make a sequence of moves.
- In each move, you divide one stack of boxes into two nonempty stacks. The game ends when you have  $n$  stacks of one box each. You earn points for each move according to the following rule:  
*if you divide a stack of size  $s = a + b$  into stacks of sizes  $a$  and  $b$ , respectively, then you score  $a \cdot b$  points.*
- Your total score is the sum of the points that you earn for each move.
- What strategy maximizes your total score?

68

68

## Exercise

- Argue that the call  $\text{MSORT}(A, 1, n)$  correctly sorts an array  $A(1:n)$  of arbitrary integers, assuming  $\text{MERGE}$  is correct

```

MSORT( $A, p, r$ )
1  if  $p < r$ 
2    then  $q \leftarrow \lfloor (p + r)/2 \rfloor$ 
3         MSORT( $A, p, q$ )
4         MSORT( $A, q + 1, r$ )
5         MERGE( $A, p, q, r$ )

```

- Let  $T(n)$  be the running time of  $\text{MSort}(A, 1, n)$ . Prove that for any  $n \geq 2$ , there is a constant  $c$  such that  $T(n) \leq cn \log n$

69

69

## Recursion

- Computational counterpart to induction
  - Constructive induction argument can be turned into code
- Solves a problem by using the solution to smaller subproblems of the same type
- Include base case(s) that can be solved directly
- Each recursive call should make progress, i.e., get you closer to a base case
  - Usually, arguments of the recursive call are getting smaller

*Example.* You are standing in a long line waiting for the opening of a museum. How can you find the number of people ahead of you if you are not allowed to get out of the line and count?

70

70

## Example: The Euclidean Algorithm

- Find the largest integer  $g$  that evenly divides natural numbers  $a$  and  $b$ , where  $a > b$

*Claim.* If  $a, b \in \mathbb{Z}^+$ , there exist unique  $q, r \in \mathbb{N}$  such that  $a = q \cdot b + r$  and  $0 \leq r < b$ .

*Claim.* If  $d|a$  and  $d|b$  then  $d|(a \bmod b)$ . (why?)

```
GCD( $a, b$ )
// Precondition:  $a, b \in \mathbb{N}, a > b$ .
1  if  $b = 0$ 
2      return  $a$ 
3  return GCD( $b, a \bmod b$ )
```

gcd(3978, 1590)

$a$	$b$	$r$
3978	1590	798
1590	798	792
798	792	6
792	6	0

71

71

## Exercise

- Show that the number of recursive calls is at most  $\log_2 a$  (under the assumption that  $a > b$ )
- What happens if  $b > a$ ?

```
GCD( $a, b$ )
// Precondition:  $a, b \in \mathbb{N}, a > b$ .
1  if  $b = 0$ 
2      return  $a$ 
3  return GCD( $b, a \bmod b$ )
```

72

72

## Exercise

- Let  $a, b \in \mathbb{N}$  and  $c = \text{GCD}(a, b)$ . Explain how to find integers  $x$  and  $y$  such that  $a \cdot x + b \cdot y = c$  (think of a modification of the GCD algorithm)
- One of the computational tasks of RSA cryptography requires finding the inverse of a number modulo another. Given  $a, n \in \mathbb{Z}^+$  explain how to solve  $a \cdot x = 1 \pmod{n}$  or determine that no solution exists.

73

73

## Exercise

- Let  $a, b \in \mathbb{N}$ . Suppose you want to tile a rectangle of size  $a \times b$  using a minimum number of squares. How many such tiles are needed? What is the size of the smallest tile?

*Example.  $a = 175, b = 65$*



74

74

## Recurse with Care!

- Beware of infinite loops (never reaching a base case)

Example.  $n! = \frac{(n+1)!}{(n+1)}$

```
def fact(n):
    if n < 2: return 1
    return fact(n+1) // (n+1)
```

- Beware of exponential running time

Example.  $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

```
def fib(n):
    if n < 2: return n
    return fib(n-1) + fib(n-2)
```

- Avoid unnecessary use of extra memory

Exercise. What is  $f(10001)$ ?  
Does  $f$  always terminate?

```
def f(n):
    if n < 2: return 1
    if n % 2 == 0: return f(n//2)
    else: return f(3*n+1)
```

75

## Structural Induction

- While our use of induction has focused on the natural numbers, the idea is far more general, and it is often applied to sets other than  $\mathbb{N}$
- Recursive data types play a central role in programming.
- Not surprisingly, the definition of a recursive data type mimics the steps of an inductive proof and includes
  - Base cases that stand alone
  - Constructor cases that build new instances using base cases and other instances known to be valid

76

76

## Exercise

- What set  $S$  is defined by each of the following rules:
  1. *Base case:* the empty string  $\varepsilon \in S$   
*Constructor:* if  $s \in S$  then  $s0 \in S$  and  $s1 \in S$
  2. *Base case:* the empty string  $\varepsilon \in S$   
*Constructor:* if  $s, t \in S$  then  $(s)t \in S$

77

77

## Functions of Recursive Data Types

- Functions of recursive data structures can be conveniently defined recursively.
- Given  $\varepsilon \in S$  and  $r, t \in S \Rightarrow (r)t \in S$  we can define

$$\text{depth}(s) = \begin{cases} 0 & \text{if } s = \varepsilon \\ \max\{1 + \text{depth}(r), \text{depth}(t)\} & \text{if } s = (r)t \end{cases}$$

*Exercise.* Define rooted binary trees recursively and provide a function to compute their height.

78

78