MATH 113 COURSE LOG

This document contains a running log of problems, solutions, and topics discussed in class. If you find typos or find something confusing, please contact me at `ormsbyk@reed.edu`.

Contents

1. Week 1

1.1. **Monday.**

Question 1.1.1 (Non-attacking rooks). Rooks are chess pieces which move vertically and horizontally. We say that two rooks are attacking each other if they are in the same rank (*i.e.* row) or file (*i.e.* column). Is it possible to place 8 rooks on a standard 8×8 chessboard so that no two rooks are attacking each other? In how many different ways can non-attacking rooks be placed on the board? What if the chessboard is $n \times n$ and you have n rooks?

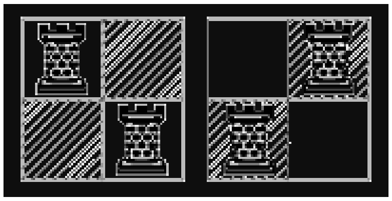


FIGURE 1. Pacifist rooks on a 2×2 chessboard.

Solution. Placing n rooks along the diagonal of an $n \times n$ chessboard exhibits a non-attacking configuration. We can enumerate all examples by placing rook 1 in any of the n positions in the first column, placing rook 2 in any of the $n-1$ positions in the second column not attackable by the first rook, placing rook 3 in any of the $n-2$ positions in the third column not attackable by the first two rooks, *etc.* For rook k, there are $n-k+1$ possibilities in the k-th column, and for the final rook there are $n - n + 1 = 1$ possible placements in the n-th column. In total, there are $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ non-attacking configurations of n rooks on an $n \times n$ chessboard. □

1.2. **Wednesday.** We began this course meeting with a discussion of the syllabus, and then moved on to the following problems.

Question 1.2.1. In how many distinct ways can the letters in the word MISSISSIPPI be arranged?

Solution. Begin by artificially labeling the letters $M_1, I_1, S_1, S_2, I_2, S_3, S_4, I_3, P_1, P_2, I_4$ and noting that there are 11 letters total. There are $11!$ ways to arrange the labeled letters (11 choices for the first letter, 10 for the second, *etc*). But this overcounts: given a particular word of labeled letters, we can rearrange the I's in $4!$ ways, rearrange the S's in $4!$ ways, and rearrange the P's in $2!$ ways and still get the same word of unlabled letters. Thus there are

$$\frac{11!}{4!4!2!} = 34,560$$

ways to rearrange the letters in MISSISSIPPI. □

Question 1.2.2 (Monotonic paths). A path on a square grid is called *monotonic* if it proceeds only by single steps right or up. On a 4×4 (or $n \times k$) grid, how many distinct monotonic paths go from the bottom left corner to the top right corner? What does this have to do with Figure 2?

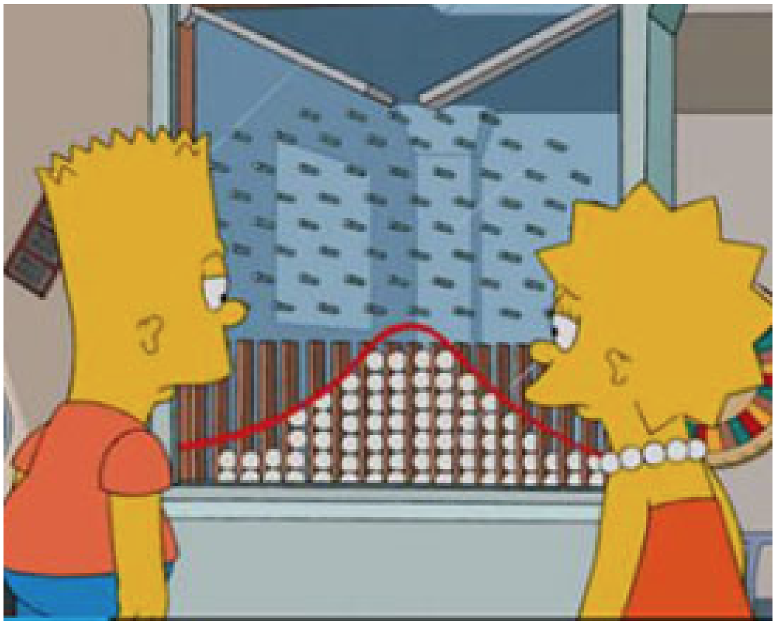


FIGURE 2. Bert and Lisa experience the Galton board

Solution. By an $n \times k$ grid, let's assume we mean ordered pairs of integers (a, b) where $0 \leq a \leq n$ and $0 \leq b \leq k$. Our aim is to go from $(0,0)$ to (n,k) without leaving the $n \times k$ grid and while only taking unit steps right or up.

First note that we have to take $n + k$ total steps to achieve our goal. Furthermore, exactly n of those steps can go right, and exactly k of those steps can go up (otherwise we don't get far enough or we leave the grid). Thus we can count the number of monotonic paths by counting the number of "words" with n R's (for right) and k U's (for up).

As a first approximation, we can label the R's $R_1, R_2, \ldots, R_n$ and the U's $U_1, U_2, \ldots, U_k$. There are $(n+k)!$ ways to order these distinguishable letters. But this is an overcount! The words $R_1R_2U_1R_3U_2$ and $R_3R_2U_2R_1U_1$ both correspond to $RRURU$; any re-ordering of the R's and any reordering of the U's gives the same word. Thus there are

$$\frac{(n+k)!}{n!k!}$$

monotonic paths. □

Remark 1.2.3. What does this have to do with the "Galton board" of Figure 2? Label the top center peg $(0,0)$. As the ball bounces down, it bounces either right or left (corresponding to R or U in a monotonic path). We have counted the total number of ways the ball can bounce so as to land in the trough labeled (n,k). We'll have more to say about this and the so-called binomial distribution later.

Remark 1.2.4. Later, we will identify the number $(n+k)!/(n!k!)$ as the *binomial coefficient* $\binom{n+k}{n} = \binom{n+k}{k}$, a quantity some of you may know something about already. For now, just keep this fact in mind.

1.3. **Friday.**

Problem 1.3.1. Is it always the case that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$? Draw a picture to support your assertion and then prove it.

Solution. Yes! See Figure 3 for a graphical representation of this fact.

For a more formal proof, let $X = A \cup (B \cap C)$ and let $Y = (A \cup B) \cap (A \cup C)$. As is typical, we prove that $X = Y$ by showing that $X \subseteq Y$ and $Y \subseteq X$.

$X \subseteq Y$: Suppose $x \in X$, which means that $x \in A$ or $x \in B \cap C$, *i.e.*, $x \in A$ or ($x \in B$ and $x \in C$). If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$, so $x \in Y$; if $x \in B$ and $x \in C$, then $x \in A \cup B$ and $x \in A \cup C$, so $x \in Y$. We have thus seen that $x \in X$ implies $x \in Y$, so $X \subseteq Y$.

$Y \subseteq X$: Suppose $y \in Y$, so $y \in A \cup B$ and $y \in A \cup C$. For the first condition to hold, $y \in A$ or $y \in B$. Equivalently, $y \in A$ or $y \in B \smallsetminus A$. (Do you see why?) If $y \in A$, then $y \in X = A \cup (B \cap C)$; if $y \in B \smallsetminus A$, then since $y \in A \cup C$, it must be in C (since it's not in A). Thus when $y \in B \smallsetminus A$, $y \in B$ and $y \in C$, *i.e.*, $y \in B \cap C$, whence $y \in X$. No matter what, whenever $y \in Y$, y is also in X, so $Y \subseteq X$.

We have just seen that $X \subseteq Y$ and $Y \subseteq X$, so $X = Y$. □

Cartesian product. There is another operation on sets called the *Cartesian product*. For sets A and B, their Cartesian product is the set

$$A \times B = \{(a,b) \mid a \in A, b \in B\},$$

the collection of ordered pairs where the first element is in A and the second is in B.

Question 1.3.2. Big Brothers Big Sisters of Portland has a collection A of 30 adult volunteers and group C of 50 children in need of an adult partner. What is a set which describes the possible adult-child pairings? How many adult-child pairings exist?

Answer. The set $A \times C$ consists of pairings (a,c) where $a \in A$ and $c \in C$, so $A \times C$ consists of all possible adult-child pairings. There are 30 adults, each of which can be paired with any of the 50 children, so there are $30 \cdot 50 = 1,500$ possible pairings. □

Problem 1.3.3. Find a general formula for $|A \times B|$ in terms of $|A|$ and $|B|$.

Solution. We claim that $|A \times B| = |A||B|$. Indeed, there are $|A|$ ways to fill the first entry, and $|B|$ ways to fill the second. □

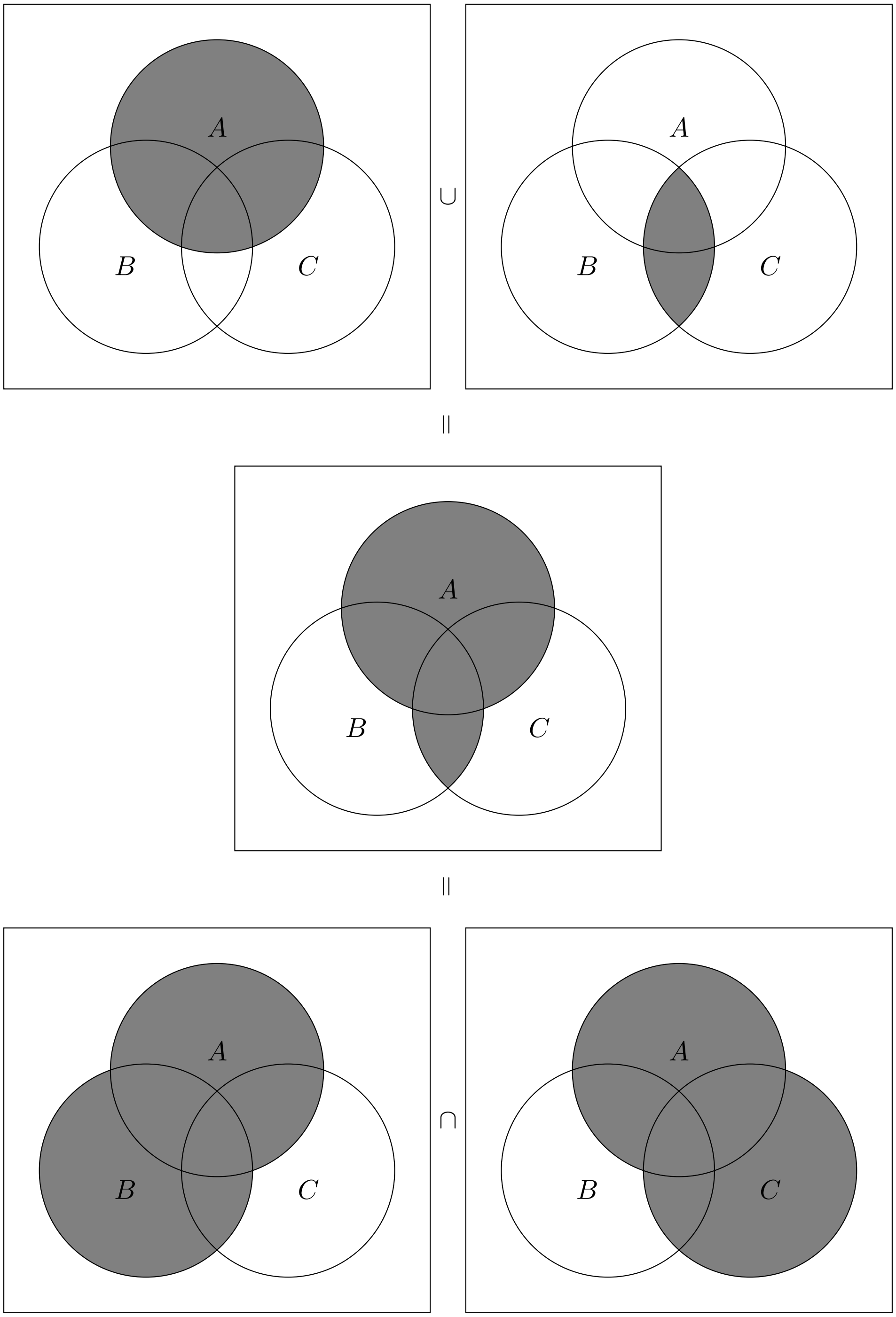


FIGURE 3. A graphical representation of $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Functions. Functions are ways of relating one set to another. Thus to each element a of a set A, a function assigns exactly one element $b \in B$. If the function's name is f, then we write $b = f(a)$.

The set A is called the *domain* of f and B is its *codomain* (aka *range*). This can all be compactly expressed via the notation $f : A \to B$.

Each function $f : A \to B$ has an associated *graph* $G_f = \{(a, f(a)) \mid a \in A\} \subseteq A \times B$. A generic subset $G \subseteq A \times B$ is the graph of a function if and only if for each $a \in A$ there is a unique $b \in B$ such that $(a, b) \in G$. In set theory (which aims to express every mathematical concept in terms of sets), a function is actually defined to be such a special subset of $A \times B$. It's good to be aware of this formalism, but more useful in everyday mathematical practice to think of functions as assignments.

Problem 1.3.4. Which of the following subsets of $\{1, 2, 3\} \times \{a, b, c, d\}$ are functions?

(a) $\{(1, a), (2, b), (3, d)\}$
(b) $\{(2, d), (3, c)\}$
(c) $\{(1, b), (2, c), (3, a), (2, d)\}$
(d) $\{(1, a), (2, a), (3, a)\}$

Solution. (a) This is a function: each element of $\{1, 2, 3\}$ appears in the first coordinate precisely once, and the second entries are all elements of $\{a, b, c, d\}$.

(b) This is not a function since no term of the form $(1, y)$ appears in the set.

(c) This is not a function since 2 appears twice in the first coordinate.

(d) This is a function. (It's fine for elements of the codomain to be repeated. This particular function is called the *constant function with value* a.)

□

Problem 1.3.5. Suppose $|A| = m$, $|B| = n$. How many functions $A \to B$ are there?

Solution. We claim that there are n^m such functions. Indeed, for each element of the domain, we can assign any of n different potential values. Since there are m elements of A, the count amounts to taking the m-fold iterated product of n with itself, *i.e.*, n^m. □

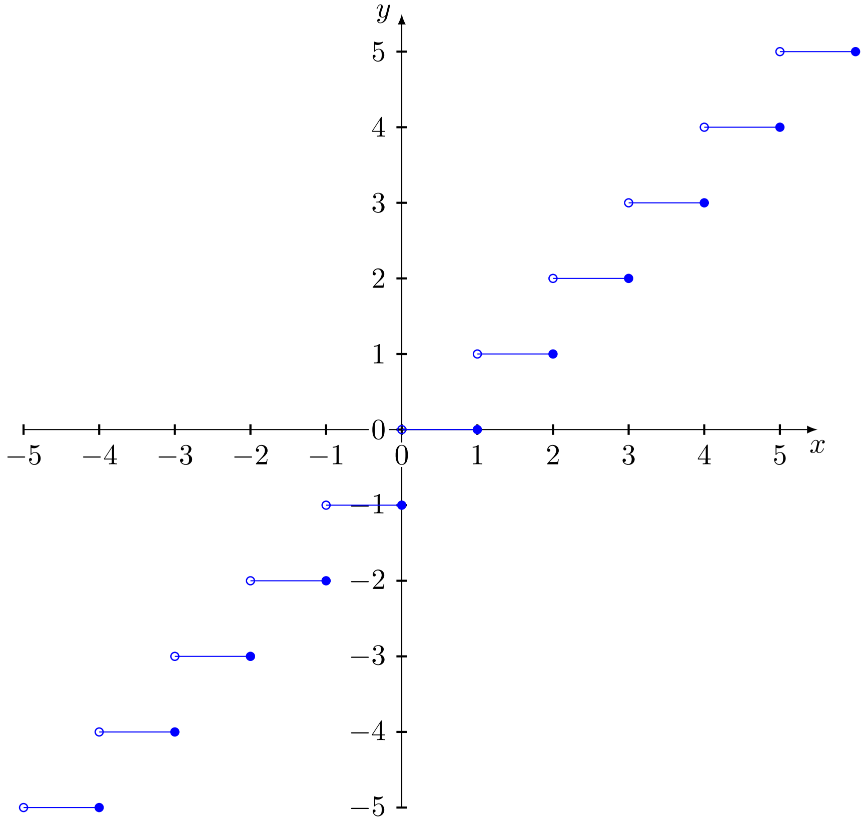
Remark 1.3.6. The set of functions with domain A and codomain B is often denoted B^A. With this notation, we have just shown that

$$\left|B^A\right| = |B|^{|A|}.$$

2.1. **Monday.** The *floor* function $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{R}$ sends $x \in \mathbb{R}$ to the greatest integer less than or equal to x. For instance, $\lfloor 4.5 \rfloor = 4$, $\lfloor 17 \rfloor = 17$, and $\lfloor -\pi \rfloor = -4$.

Problem 2.1.1. Draw a graph of $\lfloor\ \rfloor$ and check that it is a function. What is the image of the floor function? Is it injective or surjective?

Solution. A graph of $\lfloor\ \rfloor$ looks like this:



The image of $\lfloor\ \rfloor$ is exactly the set of integers, $\mathbb{Z}$. Indeed, for $n \in \mathbb{Z}$, $\lfloor n \rfloor = n$, so $\mathbb{Z} \subseteq \operatorname{im}\lfloor\ \rfloor$. By its definition, $\lfloor x \rfloor \in \mathbb{Z}$ for all $x \in \mathbb{R}$, so $\operatorname{im}\lfloor\ \rfloor \subseteq \mathbb{Z}$ as well, hence $\operatorname{im}\lfloor\ \rfloor = \mathbb{Z}$.

Since the image of the floor function is not its entire codomain, $\mathbb{R}$, it is not surjective; furthermore, the floor function is not injective since, for instance, $\lfloor 0 \rfloor = 0 = \lfloor 1/2 \rfloor$. □

Problem 2.1.2. Define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even,} \\ \frac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Show that f is a bijection.

Solution. We first show that f is injective. Suppose that $f(n) = f(m)$. If n and m are both even, then we know $n/2 = m/2$, and multiplying by 2 we conclude that $n = m$. If n and m are both odd, then we know $(1 - n)/2 = (1 - m)/2$; multiplying by 2, subtracting 1, and then multiplying by -1, we get $n = m$. If n is even and m is odd, then by definition $f(n) = n/2 \geq 0$ and $f(m) = (1 - m)/2 < 0$, a contradiction. If n is odd and m is even, we similarly get $f(n) < 0$ and $f(m) \geq 0$, a contradiction. We conclude that whenever $f(n) = f(m)$, in fact $n = m$, so f is injective.

We now show that f is surjective, concluding our proof of bijectivity. If a is a nonnegative integer, then $2a$ is an even natural number and $f(2a) = (2a)/2 = a$. If a is a negative integer, then $1 - 2a$ is an odd natural number, and $f(1-2a) = (1-(1-2a))/2 = a$. We conclude that $\operatorname{im} f = \mathbb{Z}$, so f is surjective. □

Problem 2.1.3. Suppose A and B are finite sets and $f : A \to B$ is injective. What can we say about $|A|$ and $|B|$? What if f is surjective?

Solution. If $f : A \to B$ is injective, then $|A| \leq |B|$. If $f : A \to B$ is surjective, then $|A| \geq |B|$. □

Suppose A and B are sets and $f : A \to B$ is a function. If $A' \subseteq A$, then the *image* of A' in B is defined as

$$f(A') := \{f(a) \mid a \in A'\}.$$

Note that $f(A) = \operatorname{im}(f)$. If $B' \subseteq B$, then the *preimage* of B' in A is defined as

$$f^{-1}(B') := \{a \in A \mid f(a) \in B'\}.$$

In other words, $f^{-1}(C)$ consists of everything in A pushed into C by f.

Problem 2.1.4. Determine $f(\varnothing)$ and $f^{-1}(\varnothing)$. More generally, when is $f^{-1}(B') = \varnothing$?

Solution. By definition, $f(\varnothing) = \{f(a) \mid a \in \varnothing\}$. Since there are no a in the empty set, we conclude that $f(\varnothing) = \varnothing$.

By definition, $f^{-1}(\varnothing) = \{a \in A \mid f(a) \in \varnothing\}$. Since there are no $f(a)$ in the empty set, we conclude that $f^{-1}(\varnothing) = \varnothing$.

If $f^{-1}(B') = \varnothing$, then $f(a) \notin B'$ for all $a \in A$, *i.e.*, the function f completely misses the set B'. This is equivalent to $\operatorname{im} f \cap B' = \varnothing$. □

Problem 2.1.5. For $A_1, A_2 \subseteq A$, $B_1, B_2 \subseteq B$, and $f : A \to B$, prove that

$$\begin{aligned} f(A_1 \cup A_2) &= f(A_1) \cup f(A_2), \\ f(A_1 \cap A_2) &\subseteq f(A_1) \cap f(A_2), \\ f^{-1}(B_1 \cup B_2) &= f^{-1}(B_1) \cup f^{-1}(B_2), \text{ and} \\ f^{-1}(B_1 \cap B_2) &= f^{-1}(B_1) \cap f^{-1}(B_2). \end{aligned}$$

Find an example to show that equality does not necessarily hold in the second line.

Solution. For each equality $X = Y$, we need to demonstrate the two inclusions $X \subseteq Y$ and $Y \subseteq X$.

$f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$: If $y \in f(A_1 \cup A_2)$, then $y = f(x)$ for some $x \in A_1 \cup A_2$. If $x \in A_1$, then $y \in f(A_1)$, and if $x \in A_2$, then $y \in f(A_2)$. In either case, $y \in f(A_1) \cup f(A_2)$, proving that $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$.

$f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$: Suppose $y \in f(A_1) \cup f(A_2)$. If $y \in f(A_1)$, then $y = f(x)$ for some $x \in A_1$; such an x is also in $A_1 \cup A_2$, so $y \in f(A_1 \cup A_2)$. If $y \in f(A_2)$, then $y = f(x)$ for some $x \in A_2$; such an x is also in $A_1 \cup A_2$, so $y \in f(A_1 \cup A_2)$. It follows that $f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$.

$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$: If $y \in f(A_1 \cap A_2)$, then $y = f(x)$ for some $x \in A_1 \cap A_2$. Such an x is in A_1 and A_2, and thus $y = f(x)$ is in $f(A_1)$ and $f(A_2)$, whence $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

$f^{-1}(B_1 \cup B_2) \subseteq f^{-1}(B_1) \cup f^{-1}(B_2)$: If $x \in f^{-1}(B_1 \cup B_2)$, then $f(x) in B_1 \cup B_2$, and thus $f(x) \in B_1$ or $f(x) \in B_2$. In the first case, $x \in f^{-1}(B_1)$; in the second case, $x \in f^{-1}(B_2)$. Thus $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$, and we conclude that $f^{-1}(B_1 \cup B_2) \subseteq f^{-1}(B_1) \cup f^{-1}(B_2)$.

$f^{-1}(B_1) \cup f^{-1}(B_2) \subseteq f^{-1}(B_1 \cup B_2)$: If $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$, then $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$. In the first case, $f(x) \in B_1 \subseteq B_1 \cup B_2$, so $f(x) \in B_1 \cup B_2$; similarly, in the second case $f(x) \in B_1 \cup B_2$. Thus always $x \in f^{-1}(B_1 \cup B_2)$ and we conclude that $f^{-1}(B_1) \cup f^{-1}(B_2) \subseteq f^{-1}(B_1 \cup B_2)$.

The final equality follows a similar line of argument. Make sure you can write out the proof on your own! □

2.2. **Wednesday.**

Problem 2.2.1. If $a_1, a_2, \dots, a_k \in \{0,1\}$, we write $(a_1a_2\dots a_k)_2$ for the integer represented by this string in base 2; in other words,

$$(a_1a_2\dots a_k)_2 = a_1 2^{k-1} + a_2 2^{k-2} + \cdots + a_{k-1}2^1 + a_k 2^0.$$

(a) How do you express $2 \cdot (a_1a_2\dots a_k)_2$ in binary?
(b) Find a closed formula for the n-th term in the sequence 1_2, 11_2, 111_2, 1111_2, $\dots$.

Solution. (a) We compute

$$\begin{aligned}2\cdot(a_1a_2\dots a_k)_2 &= 2\cdot(a_1 2^{k-1} + a_2 2^{k-2} + \cdots + a_{k-1}2^1 + a_k 2^0)\\ &= a_1 2^k + a_2 2^{k-1} + \cdots + a_{k-1}2^2 + a_k 2^1 + 0\cdot 2^0\\ &= (a_1a_2\dots a_k0)_2.\end{aligned}$$

(b) Let B_n denote the binary number with n 1's. Thus $B_1 = 1_2 = 1$, $B_2 = 11_2 = 3$, $B_3 = 111_2 = 7$, *etc.*, and we conjecture that $B_n = 2^n - 1$. Indeed, if we add 1 to B_n (and use the usual addition algorithm with carrying) we get $B_n + 1 = 100\dots0_2$, where there are n 0's. Thus $B_n + 1 = 2^n$ and $B_n = 2^n - 1$.

□

Problem 2.2.2. Suppose A is a nonempty finite set containing n elements and that a is a particular element of A. How many subsets of A contain a? (Try to solve this problem both with a direct count, and also by producing a bijection between $\{B \subseteq A \ : \ a \in B\}$ and a set which you've already counted.)

Solution (first method). Label the elements of A as $a_1 = a$, a_2, …, a_n. Then we can encode subsets of A with n bit binary numbers where having first bit equal to 1 indicates $a \in A$. Thus we are seeking the number of n bit binary numbers with first bit equal to 1. We have two choices for each of the remaining $n-1$ bits, and thus there are 2^{n-1} subsets of A containing a. □

Solution (second method). Let $X = \{B \subseteq A \mid a \in B\}$ and let Y be the set of subsets of $A \setminus \{a\}$. Define a function $f : X \to Y$ by $f(B) = B \setminus \{a\}$. (Note that $B \setminus \{a\}$ is necessarily a subset of $A \setminus \{a\}$, so the function is well-defined.) It suffices to prove now that f is a bijection.

To show injectivity, suppose $f(B) = f(C)$ for some $B, C \in X$. This means that $B \setminus \{a\} = C \setminus \{a\}$. Taking the union with $\{a\}$ on both sides gives $B = C$, so f is injective.

It remains to show that f is surjective. Given $C \subseteq A \setminus \{a\}$, it is easy to check that $C \cup \{a\} \in X$ and $f(C \cup \{a\}) = C$, so f is surjective.

We conclude that f is a bijection, whence $|X| = |Y|$. Since Y is the set of subsets of a set of cardinality $n-1$, both Y and X have cardinality 2^{n-1}. □

Remark 2.2.3. The second solution method for Problem is an important one in combinatorics. Underlying it is the fact that two sets X and Y have the same cardinality if and only if there is a bijection $X \to Y$. If we know how to count the elements of Y and we can produce a bijection $X \to Y$, then we know X has the same number of elements!

Problem 2.2.4. Determine the number of ordered pairs (A, B) where

$$A \subseteq B \subseteq \{1, 2, \dots, n\}.$$

Solution. There are 3^n such pairs. Indeed, for each of the n elements of $\{1, \dots, n\}$, that element may be in neither A nor B, just in B, or in both A and B. Since there are three such choices for each element, there are 3^n pairs. □

Problem 2.2.5. In what number system can you easily enumerate the pairs in Problem 2.2.4? Use this number system to enumerate such pairs when $n = 3$.

Solution. We can use ternary (*i.e.* base 3) numbers to easily enumerate the pairs. Ternary numbers consist of "trits" (trinary digits) taking the value 0, 1, or 2. We put a 0 for the k-th trit if k is in neither A nor B; a 1 for the k-th trit if k is in B but not in A; and a 2 for the k-th trit if k is in both B and A.

For $n = 3$, we get the dictionary

$$\begin{aligned}
&000_3 \longleftrightarrow \varnothing \subseteq \varnothing \subseteq \{1,2,3\}\\
&001_3 \longleftrightarrow \varnothing \subseteq \{3\} \subseteq \{1,2,3\}\\
&002_3 \longleftrightarrow \{3\} \subseteq \{3\} \subseteq \{1,2,3\}\\
&010_3 \longleftrightarrow \varnothing \subseteq \{2\} \subseteq \{1,2,3\}\\
&011_3 \longleftrightarrow \varnothing \subseteq \{2,3\} \subseteq \{1,2,3\}\\
&012_3 \longleftrightarrow \{3\} \subseteq \{2,3\} \subseteq \{1,2,3\}\\
&020_3 \longleftrightarrow \{2\} \subseteq \{2\} \subseteq \{1,2,3\}\\
&021_3 \longleftrightarrow \{2\} \subseteq \{2,3\} \subseteq \{1,2,3\}\\
&022_3 \longleftrightarrow \{2,3\} \subseteq \{2,3\} \subseteq \{1,2,3\}\\
&100_3 \longleftrightarrow \varnothing \subseteq \{1\} \subseteq \{1,2,3\}\\
&101_3 \longleftrightarrow \varnothing \subseteq \{1,3\} \subseteq \{1,2,3\}\\
&102_3 \longleftrightarrow \{3\} \subseteq \{1,3\} \subseteq \{1,2,3\}\\
&110_3 \longleftrightarrow \varnothing \subseteq \{1,2\} \subseteq \{1,2,3\}\\
&111_3 \longleftrightarrow \varnothing \subseteq \{1,2,3\} \subseteq \{1,2,3\}\\
&112_3 \longleftrightarrow \{3\} \subseteq \{1,2,3\} \subseteq \{1,2,3\}\\
&120_3 \longleftrightarrow \{2\} \subseteq \{1,2\} \subseteq \{1,2,3\}\\
&121_3 \longleftrightarrow \{2\} \subseteq \{1,2,3\} \subseteq \{1,2,3\}\\
&122_3 \longleftrightarrow \{2,3\} \subseteq \{1,2,3\} \subseteq \{1,2,3\}\\
&200_3 \longleftrightarrow \{1\} \subseteq \{1\} \subseteq \{1,2,3\}\\
&201_3 \longleftrightarrow \{1\} \subseteq \{1,3\} \subseteq \{1,2,3\}\\
&202_3 \longleftrightarrow \{1,3\} \subseteq \{1,3\} \subseteq \{1,2,3\}\\
&210_3 \longleftrightarrow \{1\} \subseteq \{1,2\} \subseteq \{1,2,3\}\\
&211_3 \longleftrightarrow \{1\} \subseteq \{1,2,3\} \subseteq \{1,2,3\}\\
&212_3 \longleftrightarrow \{1,3\} \subseteq \{1,2,3\} \subseteq \{1,2,3\}\\
&220_3 \longleftrightarrow \{1,2\} \subseteq \{1,2\} \subseteq \{1,2,3\}\\
&221_3 \longleftrightarrow \{1,2\} \subseteq \{1,2,3\} \subseteq \{1,2,3\}\\
&222_3 \longleftrightarrow \{1,2,3\} \subseteq \{1,2,3\} \subseteq \{1,2,3\}.
\end{aligned}$$

□

Problem 2.2.6. Generalize the above two problem to finite "chains of subsets" $(A_1, A_2, \ldots, A_m)$ where

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_m \subseteq \{1, 2, \ldots, n\}.$$

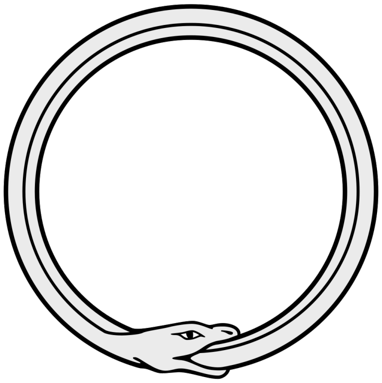


FIGURE 4. The ouroboros. (IMAGE: Wikipedia.)

Solution. We can use the base $m+1$ number system to enumerate such chains. The $(m+1)$-ary digit ℓ in the k-th position indicates that k is in the sets $A_{m-\ell+1}, A_{m-\ell+2}, \ldots, A_m$, and that k is not in $A_1, \ldots, A_{m-\ell}$.

Since there are $m+1$ choices for each of the n $(m+1)$-ary digits, we see that there are $(m+1)^n$ such chains of subsets. □

2.3. **Friday.** For $n \in \mathbb{N}$, let $\underline{n} = \{1, 2, \ldots, n\}$. In particular $\underline{1} = \{1\}$, $\underline{2} = \{1, 2\}$, $\underline{3} = \{1, 2, 3\}$, etc. Note that $\underline{0} = \varnothing$ by convention.

Problem 2.3.1. There are k^n length n strings where each entry in the string comes from a set with k elements. Earlier, you proved that there are k^n functions with domain $\underline{n}$ and codomain $\underline{k}$. Is this a coincidence? Explain.

Solution. There is a natural bijection explaining the co-incidence of the number k^n. Let X denote the set of length n strings with each entry coming from $\underline{k}$. For $s = s_1 s_2 \ldots s_n \in X$, let F_s denote the function $F_s : \underline{n} \to \underline{k}$ given by $F_s(a) = s_a$. Then the assignment $F : X \to \underline{k}^{\underline{n}}$ taking $s \mapsto F_s$ is a bijection, as we currently show.

Since X and $\underline{k}^{\underline{n}}$ have the same cardinality, it suffices to show that F is surjective. Given a function $f : \underline{k} \to \underline{n}$, define the string s by $s_a = f(a)$. Then $F_s(a) = s_a = f(a)$ for all $a \in \underline{n}$, so $F_s = f$, proving that F is surjective. □

Remark 2.3.2. It can feel disorienting when you first work with functions between sets of functions. That's OK! Like an ouroboros, mathematics gains strength from devouring itself.

We take the viewpoint that a permutation is a bijection from a set to itself. This can also be though of as a reordering of the set. If $\pi : \underline{n} \to \underline{n}$ is a bijection, it reorders $\underline{n}$ from $1, 2, \ldots, n$ to $\pi(1), \pi(2), \ldots, \pi(n)$. This also gives us the SAT-style analogy

string : function :: reordering : permutation.

In particular, we may view permutations of $\underline{n}$ as length n strings with entries in $\underline{n}$ in which no 'letters' are repeated.

Problem 2.3.3. Why does this prove that $n! \leq n^n$? What do you think $n!/n^n$ approaches as n goes to ∞?

Solution. There are n^n strings of length n with entries in $\underline{n}$. Since permutations are special types of such strings (those with no repetition) and there are $n!$ permutations of $\underline{n}$, we conclude that $n! \leq n^n$.

We can rewrite $n!/n^n$ as

$$\frac{n!}{n^n} = \frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \cdots \frac{2}{n} \cdot \frac{1}{n}.$$

As $n \to \infty$, each factor has a finite limit, and $\lim 1/n = 0$, so $\lim n!/n^n = 0$. We can interpret this as saying that there are vanishingly few permutations amongst all length n strings as n gets big. □

Define the *sign* of a permutation $\pi : \underline{n} \to \underline{n}$ by the formula

$$\operatorname{sgn}(\pi) = \prod_{1 \le i < j \le n} \frac{\pi(j) - \pi(i)}{j - i}.$$

Here $\prod$ stands for product, and we are taking the product of the factors $\frac{\pi(j)-\pi(i)}{j-i}$ as i and j range over all pairs of integers (i, j) with $1 \le i < j \le n$.

Problem 2.3.4. Write out the formula for $\operatorname{sgn}(\pi)$ when $n = 3$. Why is it the case that $\operatorname{sgn}(\pi) = \pm 1$ in this case? Show that $\operatorname{sgn}(\pi) \in \{\pm 1\}$ for all n.

Solution. For $n = 3$, the relevant pairs (i, j) are $(1, 2), (1, 3), (2, 3)$ and thus for a permutation $\pi : \underline{3} \to \underline{3}$, we have

$$\operatorname{sgn}(\pi) = \frac{\pi(2) - \pi(1)}{2 - 1} \cdot \frac{\pi(3) - \pi(1)}{3 - 1} \cdot \frac{\pi(3) - \pi(2)}{3 - 2}.$$

Let $S = \{(i, j) \mid i, j \in \mathbb{Z},\ 1 \le i < j \le n\}$ be the index set for the product, and let $\pi(S) = \{(\pi(i), \pi(j) \mid i, j \in \mathbb{Z},\ 1 \le i < j \le n\}$. The crucial observation is that for each $(i, j) \in S$, there is exactly one $(k, \ell) \in S$ such that either $(\pi(k), \pi(\ell))$ or $(\pi(\ell), \pi(k))$ is equal to (i, j). Reordering the numerators and denominators in the product expansion of $\operatorname{sgn}(\pi)$, we see that each $\frac{\pi(\ell)-\pi(k)}{j-i}$ is either 1 or -1, depending on whether the order of i and j was swapped by π. Thus the product as a whole is $(-1)^m$ where m is the number of pairs (i, j) with order swapped by π; in particular, $\operatorname{sgn}(\pi) = (-1)^m \in \{\pm 1\}$.

We now justify the crucial observation. For a given $(i, j) \in S$, we know there exist unique $k, \ell \in \underline{n}$ such that $\pi(k) = i$ and $\pi(\ell) = j$. If $k < \ell$, then $(k, \ell) \in S$ is the desired pair; if $k > \ell$, then $(\ell, k) \in S$ is the desired pair. □

3. WEEK 3

3.1. **Monday.**

Problem 3.1.1. For the following relations (with their standard meanings), determine what (if any) of the three properties of an equivalence relation they have: $\neq$, $>$, $\leq$.

Solution. The relation $\neq$ is not reflexive ($a \neq a$ is false), is symmetric (if $a \neq b$ then $b \neq a$), and is not transitive ($0 \neq 1$ and $1 \neq 0$, but $0 \neq 0$ is false).

The relation $>$ is not reflexive ($a > a$ is false), is not symmetric ($1 > 0$ but it is not the case that $0 > 1$), and is transitive.

The relation $\leq$ is reflexive, is not symmetric, and is transitive. □

Problem 3.1.2. Consider the relation $\sim$ on $\mathbb{R}$ such that $x \sim y$ if and only if $x - y \in \mathbb{Z}$. Prove that $\sim$ is an equivalence relation.

Solution. We check the properties one by one, beginning with reflexivity: if $x \in \mathbb{R}$, then $x - x = 0 \in \mathbb{Z}$, so $x \sim x$. For symmetry, suppose $x \sim y$, meaning that $x - y \in \mathbb{Z}$. Then $y - x = -(x - y)$ is an integer as well, so $y \sim x$. Finally, we check transitivty: if $x \sim y$ and $y \sim z$, then $x - y, y - z \in \mathbb{Z}$. Thus $(x - y) + (y - z) = x - z \in \mathbb{Z}$, so $x \sim z$. □

Problem 3.1.3. How many ways can we string n distinct beads on a necklace? We say that two lists of the n beads are equivalent if each bead is adjacent to the same two beads on each list. (The first and last beads on the list are considered adjacent.)

(a) Prove that the above relation on bead lists is an equivalence relation.
(b) How many lists are in an equivalence class?
(c) How many equivalence classes are there?

Solution. Write $\sim$ for the relation defined in the problem. Without loss of generality, call the beads $1, 2, \ldots, n$, and write $a = a_1 a_2 \cdots a_n$ for a list of these beads. To say that $a \sim b$ is to say that for each $i \in \{1, \ldots, n\}$ there exists some $j \in \{1, \ldots, n\}$ such that $a_{i-1} = b_{j-1}$ and $a_{i+1} = b_{j+1}$ (where we interpret a_0 as a_n and interpret a_{n+1} as a_1), or $a_{i-1} = b_{j+1}$ and $a_{i+1} = b_{j-1}$.

Lemma 3.1.4. *For lists a, b, we have $a \sim b$ if and only if b is obtained from a either by rotating the indices of a cyclically, or by reversing the order of the indices and then rotating them cyclically.*

(a) Reflexivity is obvious (right?). To check symmetry, suppose $a \sim b$. By the lemma, we can reverse the cycling/order-reversion that takes a to b to get $b \sim a$. To check transitivity, just note that composing two cycling/order-reversions gives a new cycling/order-reversion.
(b) There are n ways to cycle the indices of a given list (including the "do nothing" cycling). Each such cycling can be composed or not composed with order-reversion. Thus there are $2n$ lists in each equivalence class.
(c) Since each equivalence class has size $2n$ and there are $n!$ distinct lists, we have
$$\frac{n!}{2n}$$
total equivalence classes.

□

Problem 3.1.5. Use an equivalence class count to interpret and answer the following question: n Americans and n Russians attend a meeting and sit around a round table. If Americans and Russians alternate seats, in how many ways may they be seated?

Solution. Label the seats $1, \ldots, 2n$. Put Russians in seats $1, 3, \ldots, 2n-1$ and put Americans in seats $2, 4, \ldots, 2n$. There are $n! \cdot n! = (n!)^2$ ways to do so. Declare two such seatings equivalent if one can be rotated to obtain the other. (We take it as obvious that this forms an equivalence relation, but it's good practice to check the conditions.) There are $2n$ such rotations, so there are

$$\frac{(n!)^2}{2n}$$

seating arrangements. □

Problem 3.1.6. We place two red and two black checkers on the corners of a square. Say that two configurations are equivalent if one can be rotated to the other. Check that this is an equivalence relation, and write down its equivalence classes. Can the number of equivalence classes be found by dividing 6 (the number of words in RRBB) by some natural number?

Solution. Again, it's fairly "obvious" that this is an equivalence relation. (But check!) In order to enumerate the equivalence classes, we will consider a word using RRBB to have first letter corresponding to the color in the northwest corner, second letter corresponing to northeast corner, third corresponding to southeast, and fourth corresponding to southwest. Each word has up to four potentially distinct rotations:

$$RRBB \to RBBR \to BBRR \to BRRB$$
$$RBRB \to BRBR \to RBRB \to BRBR$$

We stop here because we've enumerated all the words in RRBB, but note that words are repeated in the second set of rotations. The equivalence classes are in fact

$$\{RRBB, RBRB, BBRR, BRRB\} \text{ and } \{RBRB, BRBR\}.$$

While it is the case that $2 = 6/3$, it is not the case that each equivalence class has size 3, so it would be inaccurate to say that we "found" the number of equivalence classes in this way. □

3.2. **Wednesday.** Recall that for natural numbers n, k, the number

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!},$$

read "n choose k," is the number size k subsets of an n-element set. If $n \geq k$, this can also be written as $\frac{n!}{k!(n-k)!}$.

Problem 3.2.1. Compute the sums

$$\binom{1}{0}$$
$$\binom{2}{0} + \binom{2}{2}$$
$$\binom{3}{0} + \binom{3}{2}$$
$$\binom{4}{0} + \binom{4}{2} + \binom{4}{4}$$
$$\binom{5}{0} + \binom{5}{2} + \binom{5}{4}$$
$$\binom{6}{0} + \binom{6}{2} + \binom{6}{4} + \binom{6}{6}$$
$$\binom{7}{0} + \binom{7}{2} + \binom{7}{4} + \binom{7}{6}$$

and develop a conjecture regarding the value of

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots$$

where the sum's final term is $\binom{n}{n-1}$ or $\binom{n}{n}$ depending on whether n is odd or even, respectively. Give a combinatorial argument proving that your conjecture is true.

Solution. We first compute

$$\begin{aligned}
\binom{1}{0} &= 1 \\
\binom{2}{0} + \binom{2}{2} &= 2 \\
\binom{3}{0} + \binom{3}{2} &= 4 \\
\binom{4}{0} + \binom{4}{2} + \binom{4}{4} &= 8 \\
\binom{5}{0} + \binom{5}{2} + \binom{5}{4} &= 16 \\
\binom{6}{0} + \binom{6}{2} + \binom{6}{4} + \binom{6}{6} &= 32 \\
\binom{7}{0} + \binom{7}{2} + \binom{7}{4} + \binom{7}{6} &= 64.
\end{aligned}$$

Based on this evidence, we conjecture that $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = 2^{n-1}$. We can interpret this conjecture as saying that the number of even-sized subsets of a size n set is 2^{n-1}. Since the total number of subsets of such a set is 2^n, we could also say that precisely half of all subsets of a finite nonempty set have even size.

One nice argument for this fact relies on the decision tree model of creating a subset: Recall that the leaves of this binary tree correspond to the subsets. For each pair of leaves emanating from the final layer of nodes, exactly one has even and one has odd size. Thus half of all subsets have even size. □

Problem 3.2.2. Compute the sums

$$\begin{aligned}
&\binom{0}{0}^2 \\
\binom{1}{0}^2 + &\binom{1}{1}^2 \\
\binom{2}{0}^2 + \binom{2}{1}^2 + &\binom{2}{2}^2 \\
\binom{3}{0}^2 + \binom{3}{1}^2 + \binom{3}{2}^2 + &\binom{3}{3}^2 \\
\binom{4}{0}^2 + \binom{4}{1}^2 + \binom{4}{2}^2 + \binom{4}{3}^2 + &\binom{4}{4}^2 \\
\binom{5}{0}^2 + \binom{5}{1}^2 + \binom{5}{2}^2 + \binom{5}{3}^2 + \binom{5}{4}^2 + &\binom{5}{5}^2
\end{aligned}$$

by hand and develop a conjecture regarding the value of

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2.$$

Give a combinatorial argument proving that your conjecture is true.

Solution. First we compute

$$\begin{aligned}
\binom{0}{0}^2 &= 1 \\
\binom{1}{0}^2 + \binom{1}{1}^2 &= 2 \\
\binom{2}{0}^2 + \binom{2}{1}^2 + \binom{2}{2}^2 &= 6 \\
\binom{3}{0}^2 + \binom{3}{1}^2 + \binom{3}{2}^2 + \binom{3}{3}^2 &= 20 \\
\binom{4}{0}^2 + \binom{4}{1}^2 + \binom{4}{2}^2 + \binom{4}{3}^2 + \binom{4}{4}^2 &= 70 \\
\binom{5}{0}^2 + \binom{5}{1}^2 + \binom{5}{2}^2 + \binom{5}{3}^2 + \binom{5}{4}^2 + \binom{5}{5}^2 &= 252
\end{aligned}$$

Suspciously and amazingly, these appear in the center column of Pascal's triangle as the numbers of the form $\binom{2n}{n}$. We conjecture that

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}$$

and note that this matches the cases computed above.

This puts us on the hunt for subsets of a size $2n$ set of size n. Suppose $|A| = 2n$ and then color half its elements blue and half its elements red. (We can do that!) To get a size n subset of A, we can choose a blue elements and b red elements where $a + b = n$. For fixed a, there are $\binom{n}{a}\binom{n}{b}$ ways to do this. Since $b = n - a$, we have $\binom{n}{b} = \binom{n}{n-a} = \binom{n}{a}$, and so $\binom{n}{a}\binom{n}{b} = \binom{n}{a}^2$. Letting a vary from 0 to n, we see that in sum we have

$$\begin{aligned}
\binom{2n}{n} &= \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n}\binom{n}{0} \\
&= \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2,
\end{aligned}$$

as desired. □

Problem 3.2.3. How many ways are there to write a nonnegative integer m as a sum of r positive integer summands? (We decree that the order of the addends matters, so $3 + 1$ and $1 + 3$ are two different representations of 4 as a sum of 2 nonnegative integers.) Develop a conjecture and prove it.

Solution. After playing around for a while (OK, maybe a long while...), one comes to the conclusion that $\binom{m-1}{r-1}$ gives the desired count. For instance, we can represent 5 as the sum of 3 positive integers as $3 + 1 + 1$, $1 + 3 + 1$, $1 + 1 + 3$, $2 + 2 + 1$, $2 + 1 + 2$, or $1 + 2 + 2$, and $6 = \binom{4}{2}$.

A nice argument for this is given by the Balls and Walls method.[1] Imagine that we have m balls in a row. In order to represent m as a sum of r positive integers, we can place $r-1$ walls in the spaces between the balls, taking care to not place two or more walls in a single gap. For example, the sum $7 = 1+3+2+1$ is represented by

$$\bullet|\bullet\bullet\bullet|\bullet\bullet|\bullet\,.$$

There is clearly a bijection between such ball-wall configurations and the sums we are counting, and each ball-wall configuration is specified by choosing $r-1$ spots to places walls amongst the $m-1$ gaps between balls; this number is, of course, $\binom{m-1}{r-1}$. □

3.3. **Friday.**

Problem 3.3.1. Use algebra and the binomial theorem to prove that

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

Proof. Let x be a variable. By the binomial theorem

$$(1+x)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} x^i.$$

In particular, the coefficient of x^n in this polynomial is $\binom{2n}{n}$.

We also have $(1+x)^{2n} = (1+x)^n(x+1)^n$, and applying the binomial theorem to each factor results in

$$(1+x)^{2n} = \left(\sum_{i=0}^{n} \binom{n}{i} x^i\right)\left(\sum_{j=0}^{n} \binom{n}{j} x^{n-j}\right).$$

When we expand this product, we get a term contributing to x^n when $i+n-j=n$, *i.e.* when $i=j$. Thus the coefficient of x^n is $\sum_{i=0}^{n}\binom{n}{i}^2$, and this must equal our alternate computation of the coefficient, $\binom{2n}{n}$. □

Problem 3.3.2. Use a combinatorial argument and an algebraic argument to produce two proofs of the identity

$$\sum_{k=0}^{n} \binom{n}{k}\binom{k}{m} = \binom{n}{m} 2^{n-m}.$$

[*Hint for the algebraic case*: First prove that $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$.]

Combinatorial solution. The summands on the left-hand side are suggestive of first choosing k elements from a size n set, and then choosing m elements from the k elements. This could be modeled by choosing a size k committee from n members, and then choosing a size m subcommittee of the committee. Since we are summing these over $k = 0, 1, \ldots, n$ while m is fixed, this counts the number of committees formed from $\{1, \ldots, n\}$ with a size m subcommittee. We can also count this by first choosing the size m subcommittee (in $\binom{n}{m}$ possible ways) and then choosing a subset of the remaining elements to form the remainder of the committee. Since there are $n-m$ remaining members, there are 2^{n-m} such subsets, and we conclude that there are $\binom{n}{m}2^{n-m}$ committe-with-size-m-subcommittee pairs from n members. Since both sides count the same thing, they are equal. □

[1] *Née* Stars and Bars, but that's a little too militaristic for Reed in my opinion.

Algebraic solution. As the hint suggests, first note that

$$\binom{n}{k}\binom{k}{m} = \frac{n!}{k!(n-k)!} \cdot \frac{k!}{m!(k-m)!} = \frac{n!}{(n-k)!m!(k-m)!}$$

while

$$\binom{n}{m}\binom{n-m}{k-m} = \frac{n!}{m!(n-m)!} \cdot \frac{(n-m)!}{(k-m)!(n-k)!} = \frac{n!}{m!(k-m)!(n-k)!}.$$

These quantities are obviously equal, so $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$.[2]

We now leverage the identity $2^{n-m} = \sum_{i=0}^{n-m}\binom{n-m}{i}$ to manipulate the right-hand side, first noting that $\sum_{i=0}^{n-m}\binom{n-m}{i} = \sum_{k=m}^{n}\binom{n-m}{k-m}$ via the change of variables $i = k - m$. (Check that the summands are in fact identical.) Thus we have

$$\binom{n}{m}2^{n-m} = \sum_{k=m}^{n}\binom{n}{m}\binom{n-m}{k-m} = \sum_{k=m}^{n}\binom{n}{k}\binom{k}{m}$$

where the second equality uses the hint's identity. When $k < m$, $\binom{k}{m} = 0$, so the final sum can also be indexed with k ranging from 0 to n, producing the desired identity. □

[2] It is also possible to give a combinatorial argument for this equality: The left-hand side counts k-subsets of an n-set paired with an m-subset of the k-subset. The right-hand side counts the m-subset first and then chooses the remaining $k - m$ members of the k-subset from the remaining $n - m$ elements of the n-set.

4. Week 4

4.1. **Monday.** In-class exam!

4.2. **Wednesday.**

Problem 4.2.1. The 0-th diagonal in Pascal's triangle is the constant sequence of 1's. The first diagonal is the sequence of positive integers $1, 2, 3, \ldots$. What is the second diagonal? The third? The n-th?

Solution. By the n-th diagonal, we mean $\binom{n}{0}, \binom{n+1}{1}, \binom{n+2}{2}, \binom{n+3}{3}, \ldots$. By iterated application of Pascal's identity, we know that $\binom{n+k}{k}$ is the sum of the preceding elements on the $(k-1)$-th diagonal, *i.e.*,

$$\binom{n+k}{k} = \binom{n-1}{0} + \binom{n}{1} + \binom{n+1}{2} + \cdots + \binom{n+k-1}{k}.$$

In particular, the second diagonal consists of the sums of consecutive positive integers,

$$\binom{2+k}{k} = \binom{1}{0} + \binom{2}{1} + \binom{3}{2} + \cdots + \binom{1+k}{k} = 1 + 2 + 3 + \cdots + (k+1).$$

These numbers are sometimes called the *triangular numbers*. (Note that $\binom{2+k}{k} = \binom{2+k}{2}$, so we can also write $\binom{n}{2} = 1 + 2 + \cdots + (n-1)$.) □

Problem 4.2.2. You proved in your homework that $n^2 = \binom{n}{2} + \binom{n+1}{2}$. Where do these terms appear in Pascal's triangle? Use your "second diagonal" interpretation from Problem 1 to produce a new proof of this identity.

Solution. We have

$$\begin{aligned}\binom{n}{2} &= 1 + 2 + 3 + \cdots + (n-3) + (n-2) + (n-1)\\ \binom{n+1}{2} &= n + (n-1) + (n-2) + \cdots + 3 + 2 + 1.\end{aligned}$$

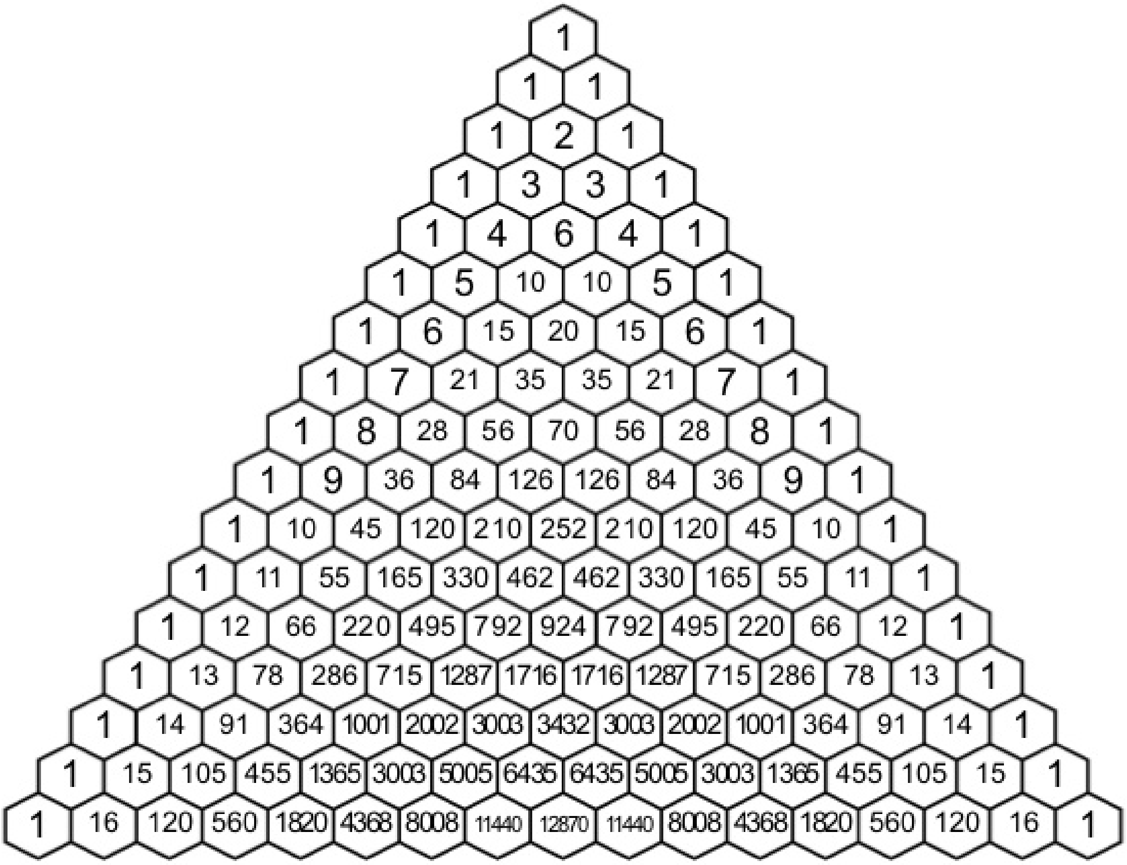
Since $0 + n = 1 + (n-1) = 2 + (n-2) = 3 + (n-3) = \cdots = n$ (note the vertical alignment above), and there are n such terms, we have that $\binom{n}{2} + \binom{n+1}{2} = n \cdot n = n^2$. □

Problem 4.2.3. How many odd numbers are there in the 2019-th row of Pascal's triangle? (To answer this, you may as well find a general formula for the number of odd numbers in the n-th row of Pascal's triangle. [*Hint*: How many odd numbers in the 2^k-th row?])

Solution. Let $\alpha(n)$ denote the number of 1's in the binary expansion of n. Let $O(n)$ denote the number of odd numbers in the n-th row of Pascal's triangle. We claim that $O(n) = 2^{\alpha(n)}$.[3]

To present a good proof of this fact, we'll need modular arithmetic, specifically mod 2 arithmetic. We defer the proof until we've developed that technology. □

[3] How would you ever guess such a result?! Patience and experimentation, for starters. You might first get some hunches by seeing that (a) the first several values of $O(n)$ are $1, 2, 2, 4, 2, 4, 4, 8, 2, 4, \ldots$, and these are all powers of 2, (b) $O(2^k)$ seems to always be $2 = 2^1$, and (c) $O(2^k - 1)$ seems to always be 2^k.



1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1
1 11 55 165 330 462 462 330 165 55 11 1
1 12 66 220 495 792 924 792 495 220 66 12 1
1 13 78 286 715 1287 1716 1716 1287 715 286 78 13 1
1 14 91 364 1001 2002 3003 3432 3003 2002 1001 364 91 14 1
1 15 105 455 1365 3003 5005 6435 6435 5005 3003 1365 455 105 15 1
1 16 120 560 1820 4368 8008 11440 12870 11440 8008 4368 1820 560 120 16 1

FIGURE 5. Pascal's triangle, 0-th through 16-th rows.

4.3. **Friday.**

Problem 4.3.1. Use induction to show that

$$2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$$

for $n \geq 1$.

Solution. For $n = 1$, we have $2^0 = 1 = 2^1 - 1$, so the base case checks. Now fix some $n \geq 1$ and suppose that $2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1$. (This is our inductive hypothesis.) Then

$$2^0 + 2^1 + \cdots + 2^{n-1} + 2^n = 2^n - 1 + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1$$

so the result holds for $n+1$ as well. By mathematical induction, the identity holds for all $n \geq 1$. □

Problem 4.3.2. Use induction to prove that the number of permutations of $\underline{n} = \{1, 2, \ldots, n\}$ is $n!$.

Solution. If $n = 0$, then $\underline{n} = \underline{0} = \varnothing$ and there is only one permutation of $\varnothing$. Since $0! = 1$, this confirms the base case $n = 0$. Now fix $n \geq 0$ and suppose for induction that there are $n!$ permutations of $\underline{n}$. Now think of a permutation π of $\underline{n+1}$ as its list of outputs, $\pi(1)\pi(2)\cdots\pi(n)\pi(n+1)$. All such lists arise by first permuting $\underline{n}$ (in any of the $n!$ ways) and then placing $n+1$ at the start of the list, in between two numbers, or at the end of the list. There are $n+1$ such positions and hence $n!(n+1) = (n+1)!$ permutations of $\underline{n+1}$. □

Problem 4.3.3. Use induction to prove that

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$$

for $n \geq 1$.

Solution. If $n = 1$, then $\frac{1}{1\cdot 2} = \frac{1}{2} = \frac{1}{1+1}$, so the base case holds. Now fix $n \geq 1$ and suppose for induction that $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$. Then

$$\begin{aligned}\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)} &= \frac{n}{n+1}+\frac{1}{(n+1)(n+2)}\\ &= \frac{n(n+2)+1}{(n+1)(n+2)}\\ &= \frac{n^2+2n+1}{(n+1)(n+2)}\\ &= \frac{(n+1)^2}{(n+1)(n+2)}\\ &= \frac{n+1}{n+2},\end{aligned}$$

as desired. □

Problem 4.3.4. Use induction to prove that a convex n-gon has $n(n-3)/2$ diagonals.

Solution. Our base case is $n = 3$, the triangle, which has no diagonals, and indeed $3(3-3)/2 = 0$. Fix $n \geq 3$ and suppose for induction that that a convex n gon has $n(n-3)/2$ diagonals. Now consider a convex $(n+1)$-gon with vertices labeled $1, 2, \ldots, n+1$ in order. By the inductive hypothesis, the n-gon with vertices $1, \ldots, n$ has $n(n-3)/2$ diagonals, and each of these is a diagonal of our $(n+1)$-gon. Additionally, the $(n+1)$-gon has diagonals joining $n+1$ to $2, 3, \ldots, n-1$, and it also has the diagonal from 1 to n. That amounts to $n-1$ additional diagonals, so the $(n+1)$-gon has

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

diagonals, as desired. □

Problem 4.3.5. Use induction to prove that

$$\binom{2n}{n} < 2^{2n-2}$$

for $n \geq 5$.

Solution. When $n = 5$, we have $\binom{10}{5} = 252$ and $2^8 = 256$, so the inequality holds in the base case. Fix $n \geq 5$ and assume for induction that $\binom{2n}{n} < 2^{2n-2}$. Since $2^{2(n+1)-2} = 2^{2n} = 4\cdot 2^{2n-2}$, it suffices to prove that $\binom{2(n+1)}{n+1} < 4\binom{2n}{n}$. By algebra,

$$\binom{2(n+1)}{n+1}=\frac{(2n+2)!}{(n+1)!^2}=\frac{(2n+2)(2n+1)}{(n+1)^2}\cdot\frac{(2n)!}{n!^2}=\frac{(2n+2)(2n+1)}{(n+1)^2}\binom{2n}{n},$$

so it suffices to prove that $\frac{(2n+2)(2n+1)}{(n+1)^2} < 4$. This is the case if and only if $(2n+2)(2n+1) < 4(n+1)^2$, *i.e.*, $4n^2+6n+2 < 4n^2+8n+4$, *i.e.*, $0 < 2n+2$, which is in fact true for all natural numbers n. □

Remark 4.3.6. The reason the theorem does not extend to all natural numbers is because the base case does not hold until $n = 5$.

5. Week 5

5.1. **Monday.** The inclusion-exclusion principle tells us how to count the size of a union of sets. Its first two cases are

$$|A\cup B| = |A|+|B|-|A\cap B| \qquad \text{and} \qquad |A\cup B\cup C| = |A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|.$$

The general formula is messier, but is underpinned by the same idea of counting, removing duplicate count, adding back in things removed too many times, *etc*.

Theorem 5.1.1 (Inclusion-Exclusion Principle)**.** *Suppose $A_1, A_2, \ldots, A_n$ are finite sets. Then*

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots A_n| = &\sum_{1\le i_1\le n} |A_{i_1}| - \sum_{1\le i_1<i_2\le n} |A_{i_1}\cap A_{i_2}| + \cdots \\ &+ (-1)^{k-1} \sum_{1\le i_1<i_2<\cdots<i_k\le n} |A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}| + \cdots \\ &+ (-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|. \end{aligned}$$

This can be equivalently phrased as

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\varnothing\neq J\subseteq \underline{n}} (-1)^{|J|-1} \left|\bigcap_{i\in j} A_i\right|.$$

Problem 5.1.2. At a large university, 1232 students have taken a course in Spanish, 879 have taken a course in French, and 114 have taken a course in Russian. Further, 103 have taken a course in both Spanish and French, 23 have taken a course in both Spanish and Russian, and 14 have taken courses in both French and Russian. If 2092 students have taken at least one of Spanish, French, and Russian, how many students have taken a course in all three languages?

Solution. Let S, F, and R denote the sets of Spanish, French, and Russian students, respectively. We are given that

$$|S| = 1232, \qquad |F| = 879, \qquad |R| = 114,$$

and

$$|S\cap F| = 103, \qquad |S\cap R| = 23, \qquad |F\cap R| = 14.$$

Furthermore, $|S\cup F\cup R| = 2092$. By the inclusion-exclusion principle,

$$|S\cup F\cup R| = |S|+|F|+|R|-|S\cap F|-|S\cap R|-|F\cap R|+|S\cap F\cap R|$$

so

$$\begin{aligned} |S\cap F\cap R| &= |S\cup F\cup R|-|S|-|F|-|R|+|S\cap F|+|S\cap R|+|F\cap R| \\ &= 2092-1232-879-114+103+23+14 \\ &= 7, \end{aligned}$$

and this is the number of students taking a course in all three languages. □

Problem 5.1.3. How many poker hands (5 cards) from a regular deck (52 cards) have at least one card from each of the four standard suits? *Hint*: Let $N_\spadesuit$ be the collection of hands containing no spades, and similarly define $N_\clubsuit$, $N_\heartsuit$, and $N_\diamondsuit$. What is the relationship between the answer to this question and $|N_\spadesuit\cup N_\clubsuit\cup N_\heartsuit\cup N_\diamondsuit|$?

Solution. Let S denote the set of hands with at least one card from each suit, and let H denote the set of all hands. Then $S = H\smallsetminus(N_\spadesuit\cup N_\clubsuit\cup N_\heartsuit\cup N_\diamondsuit)$ and $|S| = |H|-|N_\spadesuit\cup N_\clubsuit\cup N_\heartsuit\cup N_\diamondsuit|$. Since each hand contains 5 of the 52 cards, $|H| = \binom{52}{5}$, and it remains to count $|N_\spadesuit\cup N_\clubsuit\cup N_\heartsuit\cup N_\diamondsuit|$.

We proceed via inclusion-exclusion. Since only the excluded suit changes, we have $|N_\spadesuit| = |N_\clubsuit| = |N_\heartsuit| = |N_\diamondsuit|$, and for each of these counts we select 5 cards from the $52-13 = 39$ cards which aren't of the selected suit. Thus the cardinality of each of these is $\binom{39}{5}$. Each pairwise intersection excludes 26 cards and thus has cardinality $\binom{26}{5}$, and each triple intersection excludes 39 cards and thus has cardinality $\binom{13}{5}$. The quadruple intersection is empty, since each card has some suit. Note that there are $\binom{4}{2} = 6$ pairwise intersections and there are $\binom{4}{3} = 4$ triple intersections. We conclude that

$$|N_\spadesuit \cup N_\clubsuit \cup N_\heartsuit \cup N_\diamondsuit| = 4 \cdot \binom{39}{5} - 6 \cdot \binom{26}{5} + 4 \cdot \binom{13}{5}$$

and

$$|S| = \binom{52}{5} - 4 \cdot \binom{39}{5} + 6 \cdot \binom{26}{5} - 4 \cdot \binom{13}{5} = 685,464.$$

□

Alternate solution. We can also proceed without using the inclusion-exclusion principle. Every such hand can be constructed by choosing a spade, then a club, then a heart, then a diamond, and then one of the remaining 48 cards. This results in $13^4 \cdot 48$ choices, but overcounts in that the final card may be swapped with the other card of its suit, resulting in the same hand. (Hands don't have an order.) Thus there are

$$\frac{13^4 \cdot 48}{2} = 685,464$$

such hands. □

Second alternate solution. And here's the other method we covered in class. In order to construct such a hand, we first choose any of the 52 cards and note its suit. We then choose any of the remaining 39 cards of a different suit, then any of the remaining 26 cards not of the first two suits, then any of the remaining 13 cards not of the first 3 suits. Finally, we choose any of the remaining 48 cards. All such hands can be produced in this way, but there are still 4! to permute the first four cards and 2 ways to swap (or not swap) the final card with the one matching its suit. Thus there are

$$\frac{52 \cdot 39 \cdot 26 \cdot 13 \cdot 48}{4! \cdot 2} = 685,464$$

such hands. □

5.2. **Wednesday.** The *pigeonhole principle* tells us that if we have n pigeonholes and $k > n$ pigeons, then if we put all the pigeons in pigeonholes, one of the pigeonholes must contain at least two pigeons. In the language of functions, this says that if $f : A \to B$ is a function with $|A| > |B|$, then f is *not* injective. (Careful! It does not say that f is surjective — make sure you appreciate the difference.)

The *generalized pigeonhole principle* says that if there are n pigeonholes and $k > rn$ pigeons where r is a positive integer, then if we put all the pigeons in pigeonholes, one of the pigeonholes must contain at least $r + 1$ pigeons. This is equivalent to the statement that if N objects are put in b boxes, then some box contains at least $\lceil N/b \rceil$ objects.

Problem 5.2.1. In a round robin chess tournament with n participants, every player plays every other player exactly once. Prove that at any given time during the tournament, two players have finished the same number of games.

Solution. At any given moment, each player has played between 0 and $n - 1$ games, a range of n possibilities, so the pigeonhole principle does not directly apply. Note, though, that if one player has played $n - 1$ games, then everyone has played between 1 and $n - 1$ games, a range of $n - 1$ possibilities. If no players have played $n-1$ games, then everyone has played between 0 and $n-2$

games, again $n-1$ possibilities. Thus the pigeonhole principle applies in both cases to guarantee that (at least) two players have played the same number of games. □

Problem 5.2.2. What is the least number of area codes needed to guarantee that the 25 million phones in a state can be given distinct 10-digit telephone numbers of the form NXX-NXX-$XXXX$ where each X is any digit from 0 to 9 and each N represents a digit from 2 to 9? (The area code is the first three digits.)

Solution. There are $8 \cdot 10^6$ seven-digit phone numbers (excluding area code) according to these rules. With 3 or fewer area codes, there are at most 24 million distinct phone numbers, whence the pigeonhole principle would guarantee phone number repetition in the state. With 4 area codes, there are 32 million distinct phone numbers, a sufficient number to prevent repetition. □

Problem 5.2.3. Show that in the sequence 7, 77, 777, 7777, . . . there is an integer divisible by 2003. (*Hint*: First use "obvious" facts about integer divisibility to prove that if there are terms in the sequence $a_i > a_j$ such that $a_i - a_j$ is divisible by 2003, then there is a term of the sequence divisible by 2003. In order to show that such a_i, a_j exist, note that $a_i - a_j$ is divisible by 2003 if and only if a_i and a_j have the same remainder upon division by 2003; then use the pigeonhole principle.)

Solution. Following the hint, suppose $a_i > a_j$ are terms of the sequence such that $a_i - a_j$ is divisible by 2003. The number $a_i - a_j$ is of the form $a_k \cdot 10^r$ for some positive integer r. Since 2003 does not share any prime factors with 10 (in fact, 2003 is prime), we have that 2003 divides a_k.

Now note that when we divide a term a_i by 2003, we get a remainder between 0 and 2002. If the remainders of terms a_i and a_j are equal, then $a_i - a_j = 2003q_i + r - (2003q_j + r) = 2003(q_i - q_j)$ for some integers q_i, q_j, r. Thus 2003 divides $a_i - a_j$. Finally, note that there are finitely many remainders and infinitely many terms $a_i > a_j$, so such a pair with common remainder must exist. □

5.3. **Friday.** Recall that a *derangement* is a fixed point-free permutation (meaning $\pi(i) \neq i$ for all i) and that the number of derangements of an n-element set is

$$n¡ = n!(1 - 1/1! + 1/2! - 1/3! + \cdots + (-1)^n/n!).$$

Problem 5.3.1. How many derangements π of $\underline{n}$ have $\pi(1) = 2$ and $\pi(2) = 1$? Fix some k, $2 \leq k \leq n$; how many derangements π of $\underline{n}$ have $\pi(1) = k$ and $\pi(k) = 1$?

Solution. If $\pi(1) = 2$ and $\pi(2) = 1$, then the restriction of π to $\{3, 4, \ldots, n\}$ is a derangment of an $(n-2)$-element set, and all such derangments arise in this way. Thus there are $(n-2)¡$ derangments of this form. The same argument applies to derangements with $\pi(1) = k$ and $\pi(k) = 1$, with $\{i \mid i \in \mathbb{N},\ 2 \leq i \leq n,\ i \neq k\}$ playing the role of $\{3, 4, \ldots, n\}$. □

Problem 5.3.2. How many derangements π of $\underline{n}$ have $\pi(1) = 2$ and $\pi(2) \neq 1$? Fix some k, $2 \leq k \leq n$; how many derangements π of $\underline{n}$ have $\pi(1) = k$ and $\pi(k) \neq 1$?

Solution. If $\pi(1) = 2$, and $\pi(2) \neq 1$, then "the rest" of π (meaning the restriction of π to $\{2, 3, \ldots, n\}$) constitutes a bijection $\pi' : \{2, 3, 4, \ldots, n\} \to \{1, 3, 4, \ldots, n\}$. This bijection satisfies $\pi'(2) \neq 1$, $\pi'(3) \neq 3$, $\pi'(4) \neq 4$, . . . , $\pi'(n) \neq n$, *i.e.*, each element of the domain has one excluded outcome. This is the same as counting the number of derangements of an $(n-1)$-element set, $(n-1)¡$. The same argument applies to any other fixed k, $2 \leq k \leq n$ and π such that $\pi(1) = k$, $\pi(k) \neq 1$. □

Problem 5.3.3. Let $n¡$ be the number of derangements of $\underline{n}$. Use your answers to Problems 1 and 2 to find a formula for $n¡$ in terms of $(n-2)¡$ and $(n-1)¡$. Determine 1¡ and 2¡ by hand and then use your formula to determine $n¡$ for $n = 3$, 4, 5, and 6; check that your answers match with the closed formula given by the inclusion-exclusion principle.

Solution. Given a derangment π of $\underline{n}$, we have $\pi(1)$ equal to some k, $2 \leq k \leq n$, and there are $n-1$ such k. Either $\pi(k) = 1$, and there are $(n-2)¡$ such derangments for each k, or $\pi(k) \neq 1$, and there are $(n-1)¡$ such derangements for each k. We conclude that $n¡ = (n-1) \cdot (n-2)¡ + (n-1) \cdot (n-1)¡$, or, more compactly,

$$n¡ = (n-1)((n-2)¡ + (n-1)¡).$$

By direct inspection, we have $1¡ = 0$ and $2¡ = 1$. Thus

$$\begin{aligned}
3¡ &= 2(0+1) = 2, \\
4¡ &= 3(1+2) = 9, \\
5¡ &= 4(2+9) = 44, \\
6¡ &= 5(9+44) = 265.
\end{aligned}$$

We also have

$$\begin{aligned}
3!(1 - 1/1! + 1/2! - 1/3!) &= 3 - 1 = 2, \\
4!(1 - 1/1! + 1/2! - 1/3! + 1/4!) &= 12 - 4 + 1 = 9, \\
5!(1 - 1/1! + 1/2! - 1/3! + 1/4! - 1/5!) &= 60 - 20 + 5 - 1 = 44, \\
6!(1 - 1/1! + 1/2! - 1/3! + 1/4! - 1/5! + 1/6!) &= 360 - 120 + 30 - 6 + 1 = 265,
\end{aligned}$$

as expected. □

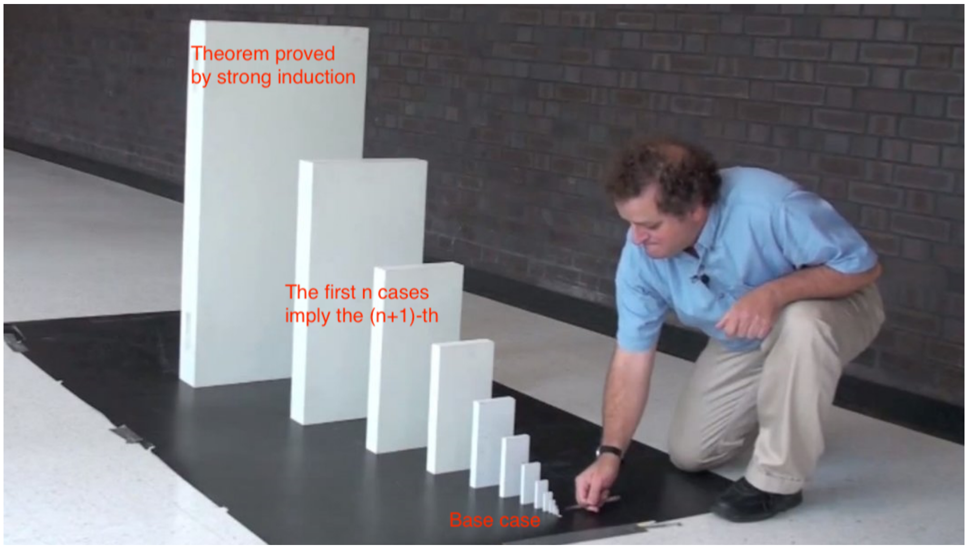


FIGURE 6. A set of dominoes for which the strong induction hypothesis is necessary?

6. Week 6

6.1. **Monday.**

Problem 6.1.1. In how many ways can you fill a $2 \times n$ chessboard with 2×1 dominoes? (Each domino must cover exactly two squares, but may be placed horizontally or vertically.) Work out the answer directly for several small values of n, make a conjecture about the overall pattern, then prove your conjecture.

Solution. Let D_n be the number of ways to fill a $2 \times n$ chessboard with 2×1 dominoes. By inspection, we see that $D_1 = 1$, $D_2 = 2$, $D_3 = 3$, $D_4 = 5$, and $D_5 = 8$. We thus suspect that $D_n = F_{n+1}$ for $n \geq 1$.

We proceed by strong induction,[4] having already verified the first several base cases. Now fix $n \geq 2$ and suppose that $D_n = F_{n+1}$ ad $D_{n-1} = F_n$. In a $2 \times (n+1)$ chessboard, the top right square must be covered by a horizontal or a vertical domino. In the first case, another horizontal domino must be directly below the top right one, and thus it remains to fill a $2 \times (n-1)$ board with $n-1$ dominoes. By the strong induction hypothesis, we can do this in $D_{n-1} = F_n$ many ways. In the vertical case, it remains to fill a $2 \times n$ board with n dominoes, which we can do in $D_n = F_{n+1}$ many ways. Since the cases are mutually exclusive, we conclude that the board may be filled in

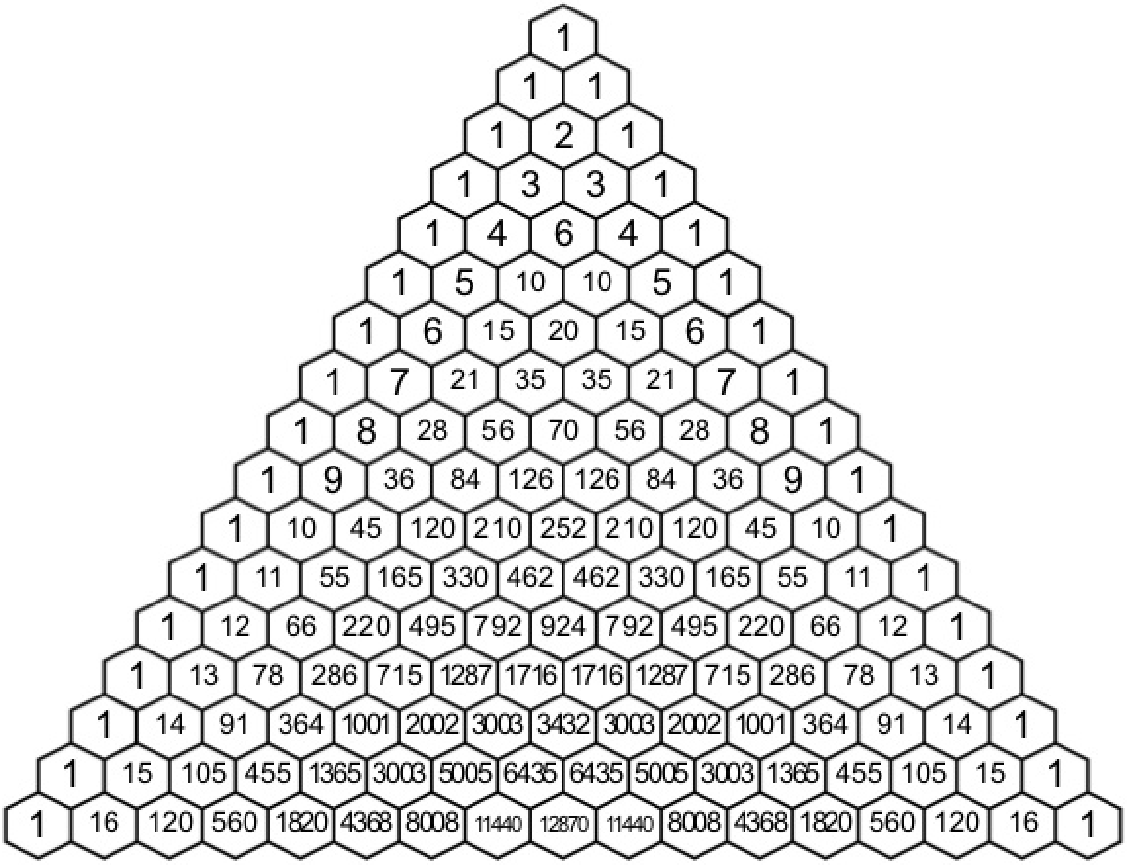
$$D_{n+1} = F_n + F_{n+1} = F_{n+2}$$

many ways, finishing our proof. □

Problem 6.1.2. Mark the first entry in some row of Pascal's triangle (this is a 1). Move one step east and one step northeast, and mark the entry there. Repeat this until you exit the triangle. Compute the sum of the entries you marked.

(a) Repeat this process for several other rows of Pascal's triangle. Guess what pattern is emerging.
(b) Express your guess in terms of a sum of binomial coefficients and prove that it is true.

[4] In strong induction, your induction hypothesis is that for some n, the claim holds for that n and all previous n; you then show that this hypothesis implies the claim for $n+1$. See Figure 6.



Solution. Let S_n denote the sum in question when we begin with $\binom{n}{0}$. Then $S_0 = 1$, $S_1 = 1$, $S_2 = 2$, $S_3 = 3$, $S_4 = 5$, $S_5 = 8$, and $S_6 = 13$. We suspect that $S_n = F_{n+1}$. To prove this, we need to check that $S_0 = F_1$, $S_1 = F_2$, and $S_{n-1} + S_n = S_{n+1}$ for $n \geq 1$. We have already seen the first two facts.

Fix $n \geq 1$. By definition, $S_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{0}{n} = \sum_{k=0}^{n} \binom{n-k}{k}$. (We have extended the sum into the "0-range" of Pascal's triangle in order to make the indexing easier.) Then

$$S_{n-1} + S_n = \sum_{k=0}^{n-1} \binom{n-1-k}{k} + \sum_{k=0}^{n} \binom{n-k}{k}$$

In the first sum, we can allow the indices to range from 0 to n by replacing k with $k-1$. (The first term becomes $\binom{n}{-1} = 0$, which is fine. Also note that the upper term of the binomial coefficient becomes $n - 1 - (k-1) = n - k$.) Thus

$$\begin{aligned} S_{n-1} + S_n &= \sum_{k=0}^{n} \binom{n-k}{k-1} + \sum_{k=0}^{n} \binom{n-k}{k} \\ &= \sum_{k=0}^{n} \binom{n-k}{k-1} + \binom{n-k}{k} \\ &= \sum_{k=0}^{n} \binom{(n+1)-k}{k} \end{aligned}$$

where the third equality follows from Pascal's identity. This final quantity is missing the $\binom{0}{n+1}$ term from our definition of S_{n+1}, but this is 0 so the two quantities are equal. We have shown that $S_{n-1} + S_n = S_{n+1}$, so our proof is complete. □

Problem 6.1.3. Extend the Fibonacci sequence backwards (with negative indices) via the relation $F_n = F_{n+2} - F_{n+1}$. Write out the terms $F_{-5}, F_{-4}, F_{-3}, \dots, F_3, F_4, F_5$ (and maybe a few more in either direction). Come up with a conjecture about the relation between Fibonacci numbers with negative indices and positive indices. Prove your conjecture.

Solution. We have $F_{-1} = F_1 - F_0 = 1$, $F_{-2} = F_0 - F_{-1} = -1$, $F_{-3} = F_{-1} - F_{-2} = 2$, $F_{-4} = F_{-2} - F_{-3} = -3$, and $F_{-5} = F_{-3} - F_{-4} = 5$. It appears that $F_{-n} = (-1)^{n-1}F_n$ for $n \geq 1$. The base case has been checked and, for a proof by strong induction, we fix $n \geq 2$ and assume $F_{-n} = (-1)^{n-1}F_n$ and $F_{-(n-1)} = (-1)^{n-2}F_{n-1}$. By definition, $F_{-(n+1)} = F_{-(n-1)} - F_{-n} = (-1)^{n-2}F_{n-1} - (-1)^{n-1}F_n = (-1)^{n-2}(F_{n-1} + F_n) = (-1)^n F_{n+1}$, where the last equality uses the recursive definition of the Fibonacci sequence and the fact that $(-1)^n = (-1)^{n-2}$ for all n. This concludes our proof by strong induction. □

6.2. **Wednesday.**

Problem 6.2.1. Compute the following sums:

$$F_1$$
$$F_1 + F_3$$
$$F_1 + F_3 + F_5$$
$$F_1 + F_3 + F_5 + F_7$$
$$F_1 + F_3 + F_5 + F_7 + F_9$$

Develop and prove a conjecture about the value of $G_n = \sum_{k=1}^{n} F_{2k-1}$.

Solution. We have $G_1 = 1$, $G_2 = 3$, $G_3 = 8$, $G_4 = 21$, $G_5 = 55$. These are all Fibonacci numbers, and after fiddling with indices for long enough, it appears that $G_n = F_{2n}$. We have checked the first several cases and, for a proof by induction, we fix $n \geq 1$ and assume that $G_n = F_{2n}$. Then $G_{n+1} = G_n + F_{2n+1} = F_{2n} + F_{2n+1} = F_{2n+2} = F_{2(n+1)}$, concluding our proof. □

Problem 6.2.2. Develop and prove a conjecture about the value of $F_{n-1}F_{n+1} - F_n^2$.

Proof. For $n \geq 1$, let $H_n = F_{n-1}F_{n+1} - F_n^2$. Then

$$H_1 = 0 \cdot 1 - 1^2 = -1$$
$$H_2 = 1 \cdot 2 - 1^2 = 1$$
$$H_3 = 1 \cdot 3 - 2^2 = -1$$
$$H_4 = 2 \cdot 5 - 3^2 = 1$$
$$H_5 = 3 \cdot 8 - 5^2 = -1.$$

It appears that $H_n = (-1)^n$. We have verified $H_1 = -1$. For induction, fix $n \geq 1$ and assume $H_n = (-1)^n$. Then

$$\begin{aligned} H_{n+1} &= F_{n+2}F_n - F_{n+1}^2 \\ &= (F_n + F_{n+1})F_n - F_{n+1}^2 \\ &= F_n^2 + (F_n - F_{n+1})F_{n+1} \\ &= F_n^2 - F_{n-1}F_{n+1} \\ &= -H_n = -(-1)^n = (-1)^{n+1}, \end{aligned}$$

as desired. □

6.3. **Friday.**

Problem 6.3.1. In this problem we will determine the number of regions in the plane created by a system of n mutually overlapping circles in general position. By *mutually overlapping*, we mean that each pair of circles intersects in two distinct points. By *general position*, we mean that there are no three circles through a common point. Let a_n be the number of regions created by such a system.

(a) Draw some pictures to determine a_0, a_1, a_2, and a_3.

(b) Do you have a conjecture regarding the value of a_n? Check it by drawing a picture to determine a_4.

(c) Take a system of $n-1$ circles (creating a_{n-1} regions) then add an n-th circle which is mutually overlapping and in general position. How many times does this circle intersect circles in the system of $n-1$ circles? How many arcs on the new circle are created by these intersections?

(d) Use your above analysis to determine a recurrence relation which a_n satisfies. (For which n does the recurrence relation hold?)

(e) Use your recurrence relation to find a closed formula (only in terms of n) for a_n (at least for n sufficiently large).

(bonus) Can you find a direct (as opposed to recurrence-based) argument for your formula in (e)?

Solution. (a) We see that $a_0 = 1$, $a_1 = 4$, and $a_3 = 8$.

(b) It is tempting to conjecture that $a_n = 2^n$, but from our picture we see that $a_4 = 14$.

(c) The new circle intersects each of the $n-1$ circles in two points, so there are a total of $2(n-1)$ intersections. This produces $2(n-1)$ arcs on the new circle.

(d) Each arc splits an old region into two regions, *i.e.*, creates one new region. Thus a_n satisfies the recurrence $a_n = a_{n-1} + 2(n-1)$ for $n \geq 2$. (Our analysis in (c) depended on there being at least one circle in the $(n-1)$-th case.) Thus a_n is given by the initial conditions $a_0 = 1$, $a_1 = 2$, and the above recurrence.

(e) Iteratively applying the recurrence relation to a_n when $n \geq 2$ results in

$$\begin{aligned}
a_n &= a_{n-1} + 2(n-1) \\
&= a_{n-2} + 2(n-2) + 2(n-1) \\
&= a_{n-3} + 2(n-3) + 2(n-2) + 2(n-1) \\
&\vdots \\
&= a_1 + 2(1) + 2(2) + 2(3) + \cdots + 2(n-2) + 2(n-1) \\
&= 2 + 2(1 + 2 + \cdots + (n-1)) \\
&= 2 + n(n-1) \\
&= n^2 - n + 2.
\end{aligned}$$

Here we employed the identity $1 + 2 + \cdots + (n-1) = n(n-1)/2$ to get the second-to-last equality. This proves that $a_n = n^2 - n + 2$ for $n \geq 2$. By coincidence, the identity holds for $n = 1$ as well, but does not hold for $n = 0$.

□

Problem 6.3.2. An anxious ant wanders through a 3×3 grid of the form

1	2	3
4	5	6
7	8	9

and only passes between cells via edges (as opposed to corners). We would like to count the number p_n of length n paths the ant can take where there is no constraint on where the ant starts or ends the path. (A "step" in the path is when the ant changes cells, despite the fact that this takes the ant many many steps. We do not permit the "stay put" step.) A direct recurrence relation on p_n is difficult to come by. (If the $(n-1)$-th step is to cell 1, then the ant can only travel to 2 or 4, but if the $(n-1)$-th step is to cell 5, the ant can travel to 2, 4, 6, or 8.) Instead, we seek multiple recurrence relations (and some good luck).

(a) Let a_n denote the number of length n paths ending in 1, let b_n denote the number of length n paths ending in 2, and let c_n denote the number of length n paths ending in 5. What is the relationship between p_n and these three sequences. (Use symmetry!)

(b) Determine a *system of recurrence relations* for the sequences a_n, b_n, c_n. (This is like a recurrence relation, but each sequence may depend on previous terms of the other sequences.)

(c) Use algebra to find a recurrence relation for b_n (only in terms of previous terms from the same sequence).

(d) Put everything together to get a recurrence relation for p_n.

(e) Compute p_0, p_1, p_2, p_3, p_4, and p_5. Why is the ant anxious?

Proof. (a) Each path ends in some cell, and by symmetry the same number of paths, a_n end in cells 1, 3, 7, and 9; similarly, the same number of paths, b_n, end in 2, 4, 6, and 8; the remaining case is the c_n paths ending in cell 5. Thus $p_n = 4a_n + 4b_n + c_n$.

(b) In order to end in cell 1 in n steps, the ant may either be in cell 2 or 4 at step $n-1$. Thus $a_n = 2b_{n-1}$. To end in cell 2 in n steps, the ant may either be in cell 1, 3, or 5 at step $n-1$. Thus $b_n = 2a_{n-1} + c_{n-1}$. Finally, $c_n = 4b_{n-1}$ since to end in cell 5 in n steps, the ant must be in cell 2, 4, 6, or 8 at step $n-1$. Our system of recurrences is

$$\begin{aligned} a_n &= 2b_{n-1} \\ b_n &= 2a_{n-1} + c_{n-1} \\ c_n &= 4b_{n-1}. \end{aligned}$$

(c) Since $a_{n-1} = 2b_{n-2}$ and $c_{n-1} = 4b_{n-2}$, we get

$$b_n = 2 \cdot 2b_{n-2} + 4b_{n-2} = 8b_{n-2}.$$

Since $b_1 = 3$ and $b_2 = 8$, we can solve for b_n explicitly as $b_n = 8^{n/2} \cdot 8 = 8^{n/2+1}$ if n is even and $b_n = 8^{(n-1)/2} \cdot 3$ if n is odd.

(d) We know that $p_n = 4a_n + 4b_n + c_n$ for $n \geq 1$, which becomes $p_n = 4 \cdot 2b_{n-1} + 8b_{n-2} + 4b_{n-1} = 12b_{n-1} + 8b_{n-2}$ for $n \geq 2$. Thus if n is even and ≥ 2, $p_n = 12 \cdot 8^{(n-2)/2} \cdot 3 + 8 \cdot 8^{(n-2)/2+1} = 36 \cdot 8^{(n/2-1} + 8^{n/2+1}$. If n is odd and ≥ 2, $p_n = 12 \cdot 8^{(n-1)/2+1} + 8 \cdot 8^{(n-3)/2} \cdot 3 = 12 \cdot 8^{(n-1)/2+1} + 3 \cdot 8^{(n-3)/2+1}$.

(e) The explicit computations are not horribly illuminating, but the asymptotic growth is proportional to $8^{n/2}$, which is exponential. In reality, ant is paralyzed by the overwhelming number of choices and simply stays put.

□

7. WEEK 7

7.1. **Monday.**

Problem 7.1.1. A *complete graph* on n vertices, denoted K_n, has every possible edge. Draw pictures of K_3, K_4, and K_5. How many edges are there in a complete graph on n vertices? For a general graph $G = (V, E)$, make an inequality relating $|V|$ and $|E|$.

Solution. There are $\binom{n}{2}$ edges in K_n, since there are as many edges as there are choices of 2 vertices. Since $K_{|V|}$ has the maximal number of edges amongst graphs with $|V|$ vertices, we know that $|E| \leq \binom{|V|}{2}$ for a general graph $G = (V, E)$. □

Problem 7.1.2. A graph $G = (V, E)$ is called *bipartite* if $V = A \cup B$ with $A \cap B = \varnothing$ and there are no edges between vertices in A and similarly for B (so only edges between a vertex in A and a vertex in B are allowed). The *complete bipartite graph on $p + q$ vertices*, denoted $K_{p,q}$, has $|A| = p$, $|B| = q$, and all possible edges between A and B.

(a) Draw pictures of $K_{2,3}$ and $K_{3,5}$.
(b) How many edges are in $K_{p,q}$?
(c) If $|A| = p$ and $|B| = q$ with $A \cap B = \varnothing$, how many (not necessarily complete) bipartite graphs have vertex set $A \cup B$?

Solution. (a)
(b) Each of the p vertices in A is connected to all q vertices in B, so $K_{p,q}$ has pq edges.
(c) Each of the pq potential edges joining A to B is either in or not in the graph. Thus there are 2^{pq} such bipartite graphs.

□

Problem 7.1.3. Suppose $G = (V, E)$ and $G' = (V', E')$ are graphs.

(a) When should a function $f : V \to V'$ be considered a "map" $G \to G'$?
(b) When should we consider G and G' to be "the same" graph?

Proof. (a) The function must take edges to edges, so we require that if $\{v, w\} \in E$, then $\{f(v), f(w)\} \in E'$.
(b) We demand that there exist maps of graphs $f : G \to G'$ and $g : G' \to G$ such that $f \circ g = \mathrm{id}_{V'}$ and $g \circ f = \mathrm{id}_V$. Thus f is a bijection on the set of vertices, it preserves edges, and its inverse function also preserves edges. This is equivalent to f being a bijection on vertex sets which induces a bijection on edge sets $\{v, w\} \mapsto \{f(v), f(w)\}$.

□

7.2. **Wednesday.**

Problem 7.2.1. Let $G = (V, E)$ be a graph with connected subgraphs $H_1 = (V_1, E_1)$ and $H_2 = (V_2, E_2)$ such that $V_1 \cap V_2 \neq \varnothing$. Prove that G is connected.

Solution. We must show that there is a walk in G between any two vertices in G. Given $v, w \in V$, such a walk exists if both vertices are in V_1 or both are in V_2 since H_1 and H_2 are connected. Now suppose that $v \in H_1$ and $w \in H_2$. Choose $u \in V_1 \cap V_2$. By connectivity of H_1, there is a walk in G from v to u. By connectivity of H_2, there is a walk in G from u to w. Concatenating those paths, we get a walk from v to w, as desired. □

Call a graph *acyclic* if it does not contain any subgraphs which are cycles. A *tree* is a connected acyclic graph. A disconnected acyclic graph is called a *forest*.

Problem 7.2.2. How many edges are there in a tree with n vertices? Prove your assertion (by induction?).

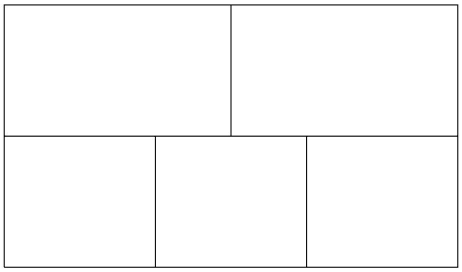
Solution. We prove that there are $n - 1$ edges in a tree with n vertices by induction on $n \geq 1$. Clearly, if $n = 1$ then there are $0 = 1 - 1$ edges in a single vertex tree. For induction, fix $n \geq 1$ and suppose that every tree with n vertices has $n - 1$ edges. Given a tree with $n + 1$ vertices, there exists a vertex of degree 1 (why?). Prune this vertex and its edge from the tree to get a tree with n vertices and hence $n - 1$ edges. The $(n + 1)$-vertex tree has one more edge, hence $n = (n + 1) - 1$ edges, as desired. □

Problem 7.2.3. Prove that a graph G is a tree if and only if there is a *unique* path between any two vertices of G.

Solution. First suppose that G is a tree. Since G is connected, there is at least one path between any two vertices. Suppose for contradiction that there are two paths $P_1 \neq P_2$ joining $u \neq v \in G$. Suppose P_1 goes from $u = u_1$ to u_2 to u_3 to . . . to $u_k = v$ and P_2 goes from $u = v_1$ to v_2 to v_3 to . . . to $v_\ell = v$. Let i be the first index such that $u_i \neq v_i$ and let $j \geq i$ be the next index so that $u_j = v_m$ for some $i \leq m \leq \ell$. Then we have paths from u_{i-1} to u_j and (reversing part of P_2) from $u_j = v_m$ to $u_{i-1} = v_{i-1}$. This creates a circuit, contradicting the hypothesis that G is a tree.

Now suppose that G is not a tree. Then either G is not connected (in which case there are vertices joined by no path) or G contains a cycle $u_0u_1u_2 \cdots u_mu_0$. Then u_0u_1 and $u_0u_mu_{m-1} \cdots u_2u_1$ are two distinct paths from u_0 to u_1. □

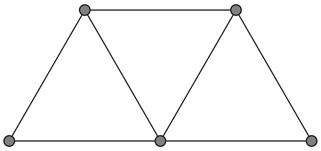
7.3. **Friday.** Consider the following floor plan for a building:



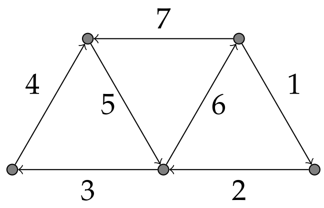
We would like to know if it is possible to cross each interior wall in the building exactly once (without teleporting).

Problem 7.3.1. (a) Turn this into a graph theory problem about a particular kind of walk.
(b) Either find such a walk, or prove that no such walk exists.
(c) What if we want to pass through the exterior walls as well?

Solution. (a) We may think of each room as a vertex, and then connect rooms with edges if they share an interior wall. This results in the graph



for which we would like to know if there is an Eulerian walk.
(b) The vertices have degrees 2, 4, 2, 3, and 3 starting from the lower left and moving counterclockwise. Thus an Eulerian walk exists and it must start at one of the upper two vertices and end at the other. Here is an example of such a walk:



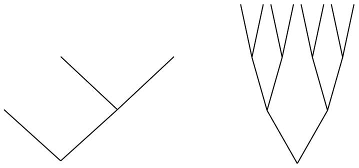
(c) Considering the exterior walls introduces an extra vertex in the graph corresponding to the exterior of the building joined to the bottom vertex by a single edge and joined to every other edge by **two** edges. Thus the new vertex has degree 9 and the top two vertices each have degree 5. We conclude that this graph has no Eulerian walks since more than two vertices have odd degree.

□

8. Week 8

8.1. **Monday.** A *full binary tree* is a rooted tree in which each vertex has either two children or no children; furthermore, when there are two children, one is designated *left* and the other *right*. Vertices with no children are called *leaves*.

Here are some examples:



Problem 8.1.1. Let C_n denote the number of unlabelled full binary trees with $n+1$ leaves. Prove that $C_0 = 1$ and

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$$

for $n \geq 0$. Compute the first several values of C_n and draw the corresponding full binary trees.

Solution. The only full binary tree with 1 leaf is the singleton tree, of which there is 1, so $C_0 = 1$.

Given a full binary tree T with $n+1$ leaves, $n \geq 0$, let $L(T)$ denote its left sub-tree (with root the left child of the root of T and all its children in T) and let $R(T)$ denote its right sub-tree (similarly defined). Then $L(T)$ has $1 \leq j \leq n+1$ leaves and $R(T)$ has $n+2-j$ leaves. The number of possibilities for $L(T)$ with j leaves is counted by C_{j-1}, and then there are C_{n+1-j} possibilities for $R(T)$. This proves that

$$C_{n+1} = \sum_{j=1}^{n+1} C_{j-1} C_{n+1-j}.$$

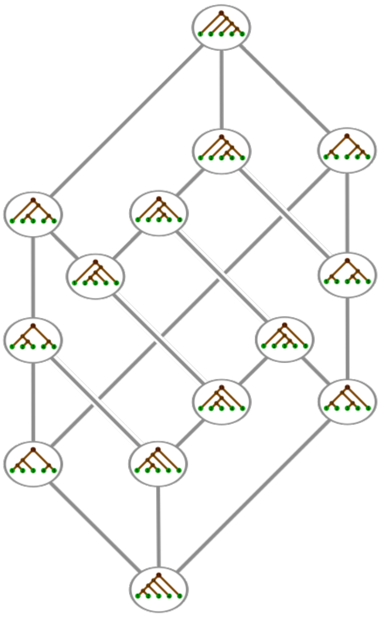
Changing indices with $i = j-1$ gives

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}.$$

By the recurrence,

$$\begin{aligned}
C_1 &= C_0C_0 = 1,\\
C_2 &= C_0C_1 + C_1C_0 = 2,\\
C_3 &= C_0C_2 + C_1C_1 + C_2C_0 = 5,\\
C_4 &= C_0C_3 + C_1C_2 + C_2C_1 + C_3C_0 = 14,\\
C_5 &= C_0C_4 + C_1C_3 + C_2C_2 + C_3C_1 + C_4C_0 = 42.
\end{aligned}$$

Here is an alluring picture of the 14 full binary trees with 5 leaves. Do you see what the edges represent?



□

The numbers C_n are called the *Catalan numbers* and can be expressed concisely as $C_n = \frac{1}{n+1}\binom{2n}{n}$. The standard proof of this fact uses *generating functions* and will not be presented here. A bijective proof for this formula appears after we establish that some additional combinatorial structures counted by Catalan numbers.

Problem 8.1.2. Find an explicit bijection between full binary trees with $n+1$ leaves and full parenthesizations of $n+1$ factors. (For instance, the full parenthesizations of abc are $(ab)c$ and $a(bc)$, while the full parenthesizations of $abcd$ are $((ab)c)d$, $(a(bc))d$, $(ab)(cd)$, $a((bc)d)$, and $a(b(cd))$.) This proves that C_n counts the number of full parenthesizations of $n+1$ factors.

Solution. Call the factors $a_1, \ldots, a_{n+1}$ and label the leaves with the factors from left to right. Call the *level* of a node k if it is k steps from the root. Begin with the largest level nodes, which are necessarily leaves. Each is in a two-leaf subtree labeled with a_i and a_{i+1}. Label such vertices' parent node $(a_i a_{i+1})$ and delete the largest level nodes (and the attached edges). Proceed inductively until one ends up with a parenthesization of $a_1 \cdots a_n$ at the root. □

It follows that C_n is also the number of ways of arranging n pairs of correctly matched parentheses. This perspective is very important in computer science, where trees are frequently stored via bracketing schemes.

8.2. **Wednesday.**

Problem 8.2.1. A *Dyck path* of length $2n$ is a monotonic lattice path in $[0,n]^2$ starting from $(0,0)$ and ending at (n,n) which never goes above the diagonal. Prove that there are C_n Dyck paths of length $2n$.

Solution. Label each step in the path (starting from $(0,0)$) either E for east or N for north, and create the associated word of length $2n$ in the alphabet $\{E, N\}$. Now replace each E with a left parenthesis, and each N with a right parenthesis. In total, there are n opening and n closing parentheses, and the fact that the path never goes above the diagonal guarantees that at any given position in the string, there are at least as many opening as closing parentheses. As such we get n pairs of parentheses which are completely matched.

We leave it to the reader to put such sets of parentheses in bijection with valid full parenthesizations of $n+1$ factors. □

Dyck paths also give a proof of the formula

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Proof. Recall that there are $\binom{2n}{n}$ monotonic lattice paths from $(0,0)$ to (n,n). We aim to partition the monotonic paths into $n+1$ subsets of equal size, where precisely one of the subsets is the collection of Dyck paths. This will prove that $C_n = \binom{2n}{n}/(n+1)$, as desired.

We define the *exceedance* of a monotonic lattice path to be its number of vertical steps above the diagonal. The exceedance of a monotonic lattice path from $(0,0)$ to (n,n) is between 0 and n (inclusive), and the Dyck paths are precisely those monotonic lattice paths with exceedance 0. Let P be the set of monotonic lattice paths from $(0,0)$ to (n,n) and let E_i be the set of paths with exceednace i; then $P = E_0 \cup E_1 \cup \cdots \cup E_n$ is clearly a partition of P. If we can show that $|E_0| = |E_1| = |E_2| = \cdots = |E_n|$, then we will be done.

Given a path $p \in E_i$, write $p = BrAuC$ where r is the first right step below the diagonal and u is the first up step touching the diagonal after r. Then B is a path above the diagonal with exceedance $j \leq i$, A is a path below the diagonal, and C is the reamining path with exceedance $i-j$. Switch Br and Au to produce $f(p) = AuBrC$. The exceedances of A, uBr, and C are 0, $j+1$, and $i-j$, respectively. (Draw some pictures and check this!) Thus $f(p) \in E_{i+1}$.

Given a path $q \in E_{i+1}$, write $q = AuBrC$ where u is the first up step above the diagonal and r is the first right step touching the diagonal after u. Define $g(q) = BuAdC$ and check that $g(q) \in E_i$. Finally, check that $f : E_i \to E_{i+1}$ and $g : E_{i+1} \to E_i$ are inverse to each other. □

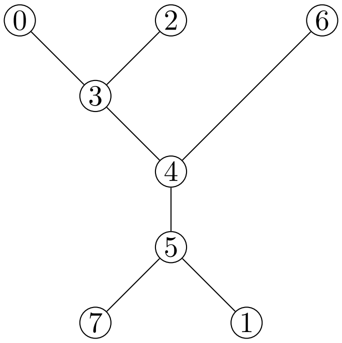
Problem 8.2.2. Prove that we can also express C_n as

$$C_n = \frac{(2n)!}{n!(n+1)!} = \binom{2n}{n} - \binom{2n}{n+1}$$

Solution. Both identities follow from simple algebra. □

8.3. **Friday.** A *leaf* of a tree is a vertex of degree 1. Suppose T is a tree with vertex set $\{0,1,2,\ldots,n-1\}$. The *Prüfer code* of T is the sequence of length $n-2$ with entries in $\{0,1,\ldots,n-1\}$ generated by the following algorithm: At step i, remove the leaf with the smallest label not equal to 0 and set the i-th entry of the Prüfer code equal to the label of the leaf's neighbor. After step $n-2$, the end of the algorithm, one is left with a single edge joining some node to 0.

For instance, the Prüfer code of the following graph is 534543.



In your reading, you learned how to turn a Prüfer code into a tree by writing down its extended Prüfer code, a $2 \times n$ array with entries in $\{0,1,\ldots,n-1\}$ with columns corresponding to edges. To quote,

> Each entry in the first row of the extended Prüfer code is the smallest integer that does not occur in the first row before it, nor in the second row below or after it.

One applies this procedure with initial data the second row consisting of the Prüfer code with a 0 tacked on the end.

Problem 8.3.1. Draw a tree on vertex set $\{0, 1, \dots, n-1\}$ with $n = 6$, 7, 8, or 9. Determine its Prüfer code and write the Prüfer code on the whiteboard. Then trade Prüfer codes with another group and decode into a tree. Draw the tree next to its Prüfer code and check your work with the group that made the Prüfer code.

Problem 8.3.2. Which trees have Prüfer codes that contain only one value?

Solution. These are the stars. Indeed, a star with i as its root and $\{0, 1, \dots, n-1\} \smallsetminus \{i\}$ as its leaves has Prüfer code i^{n-2} (by which we mean i repeated $n-2$ times). The converse clearly holds as well. □

Problem 8.3.3. Which trees have Prüfer codes with distinct values in all positions?

Solution. These are the paths. Indeed, consider the path going from $\pi(0)$ to $\pi(1)$ to $\pi(2)$ to ... to $\pi(n-1)$ where π is some permutation of $\{0, 1, \dots, n-1\}$. At each step, the associated Prüfer code picks off one of the leaves, and these are all distinct values between 0 and $n-1$. It is easy to check the converse as well. □

9. WEEK 9

9.1. **Monday.** Let S be our sample space (really any set) and let $\mathscr{E} = 2^S$ denote the corresponding collection of events (just the set of subsets of S). Recall that a *probability distribution* on S is a function

$$P : \mathscr{E} \to [0,1]$$

such that (1) $P(S) = 1$, (2) $P(\varnothing) = 0$, and (3) if A, $B \in \mathscr{E}$ are mutually exclusive events (so $A \cap B = \varnothing$), then $P(A \cup B) = P(A) + P(B)$. If S is a finite set, then we can define the *uniform probability distribution* on S to be the function taking $A \subseteq S$ to $|A|/|S|$.

Problem 9.1.1. A lottery has participants choose 5 distinct numbers from the set $\{1, 2, \ldots, 36\}$. On a prescribed date, the lottery announces a collection of 5 winning numbers. Complete the following prompts in order to determine why the lottery does not offer a prize for having selected only 1 winning number.

(a) What sample space is pertinent in this question? Describe it both as a collection of certain types of objects, and in a more mathematical fashion.
(b) Is it reasonable to put the uniform probability distribution on this sample space? (Assume that the lottery is fair.)
(c) Let B denote the event of choosing a ticket with no winning numbers. What $P(B)$?
(d) Let A denote the event of choosing a ticket with at least one winning number. What is $A \cap B$? $A \cup B$?
(e) Use the axioms for a probability distribution and your answer to (c) to determine $P(A)$.
(f) [Follow up question] Might it be reasonable to offer prizes for anyone with 2 or more winning numbers?

Solution. (a) The sample space is the collection of valid lottery tickets. If we assume that the lottery does not care about the order of the numbers, then we may model this sample space as $\binom{\underline{36}}{5}$, the collection of 5-element subsets of $\underline{36} = \{1, 2, \ldots, 36\}$.
(b) Sure! If the lottery is fair, then each ticket has an equal chance of being drawn.
(c) Suppose the winning ticket is the set $\{a_1, a_2, a_3, a_4, a_5\}$ where the a_i are distinct elements of $\underline{36}$. Then $B = \{t \in \binom{\underline{36}}{5} \mid a_i \neq t\}$. In other words, B is the collection of 5-element subsets of $\underline{36} \smallsetminus \{a_1, \ldots, a_5\}$. As such $|B| = \binom{31}{5}$ and $P(B) = \binom{31}{5}/\binom{36}{5} \approx 0.45$.
(d) We have $A \cap B = \varnothing$ and $A \cup B = \binom{\underline{36}}{5}$.
(e) It follows that $P(A) = P(A \cup B) - P(B) = 1 - \binom{31}{5}/\binom{36}{5} \approx 0.55$. If the lottery pays out 55% of the time, then it's not a very lucrative lottery for those running it!

□

Problem 9.1.2. What is the probability that in a random ordering of a standard deck of cards, the ace of spades precedes the king of hearts?

(a) Rephrase this as a question about permutations of $\underline{52}$. What is the sample space under consideration? the event?
(b) Prove that the probability of this event (under the uniform distribution) is $1/2$ by producing a bijection between the event and its complement. (Why does that solve things?)

Solution. (a) We can number the cards 1 through 52, designating the ace of spades 1 and the king of hearts 2. An ordering of the cards corresponds to a permutation of $\underline{52}$, so the sample space is Σ_{52}, the set of permutations of $\underline{52}$. The event is

$$A = \{\pi \in \Sigma_{52} \mid \pi(1) < \pi(2)\}.$$

(b) We have $\Sigma_{52} \smallsetminus A = \{\pi \in \Sigma_{52} \mid \pi(2) < \pi(1)\}$. This is in bijection with A via the function that swaps the values of $\pi(1)$ and $\pi(2)$. Thus $|A| = |B|$, $A \cup B = \Sigma_{52}$, and $A \cap B = \varnothing$. As such,

$$1 = P(A \cup B) = P(A) + P(B) = 2P(A)$$

whence $P(A) = 1/2$.

□

Problem 9.1.3. Your partner invites you to play a game: they write ten distinct real numbers on ten blank cards. The cards are shuffled randomly and placed face down on the table. You start at the top of the deck and start revealing cards. At any point you may choose to stop turning over cards and select the most recently revealed card. You win if your selection is the largest of all ten numbers (both those previously revealed and those still unrevealed). Devise a strategy which guarantees you will win this game at least 25% of the time.

The start of a solution. This is a variant on the so-called *secretary problem*, née *fianceé problem*. We can use a *stopping rule* to increase our chance of winning: look at the first r cards and note the maximal value among them, M. For the subsequent $10 - r$ cards, select the first one larger than M. (If the tenth is not larger than M, select and it and bemoan your bad luck). With $r = 4$, you will select the largest number about 40% of the time, and this is the best r for 10 cards. A full analysis can be found in (Sardelis and Valahas, *Decision Making: A Golden Rule*, The American Mathematical Monthly Vol. 106, No. 3 (Mar., 1999), pp. 215-226). □

9.2. **Wednesday.**

Problem 9.2.1. Show that if A and B are independent, then so are their complements A^c and B^c.

Solution. Since A and B are indpendent, we know that $P(A)P(B) = P(A \cap B)$. Since $A^c \cap B^c = (A \cup B)^c$, we aim to show that $P(A^c)P(B^c) = P((A \cup B)^c)$. We now compute

$$\begin{aligned} P(A^c)P(B^c) &= (1 - P(A))(1 - P(B)) \\ &= 1 - P(A) - P(B) + P(A)P(B) \\ &= 1 - P(A) - P(B) + P(A \cap B). \end{aligned}$$

We have $P(A) + P(B) - P(A \cap B) = P(A \cup B)$ (a probabilistic version of inclusion-exclusion) and thus

$$P(A^c)P(B^c) = 1 - P(A \cup B) = P((A \cup B)^c),$$

as desired. □

Problem 9.2.2. We flip a fair coin n times. Let A be the event that the first coin flip was heads. Let B be the event that the number of heads was even. Let C be the event that the number of heads was more than the number of tails. Which pairs of these three events are independent?

Solution. First, we compute the probability of each event. Thinking of the coin flips as an n-bit binary sequence, we easily see that $P(A) = 2^{n-1}/2^n = 1/2$. Thinking of these sequences as subsets of an n-element set and recalling that there are the same number of even- and odd-sized subsets of $\underline{n}$, we get that $P(B) = 1/2$. Finally, $P(C) = \left(\sum_{k>n/2} \binom{n}{k}\right)/2^n$. When $n = 3$, we may compute this value to be $1/2$, and when $n = 4$ it is $5/16$.

The event $A \cap B$ consists of flip sequences with first flip a head and total heads even. This is the same as the first flip being heads and, amongst the subsequent $n - 1$ flips having an odd number of heads. There are 2^{n-2} such flip sequences, so $P(A \cap B) = 2^{n-2}/2^n = 1/4$ and A and B are independent as $P(A)P(B) = 1/2 \cdot 1/2 = 1/4$ as well.

The event $A \cap C$ consists of flip sequences with first flip a head and more heads than tails, total. When $n = 3$, $P(A \cap C) = 3/8 \neq 1/4$ so A and C are not independent in general.

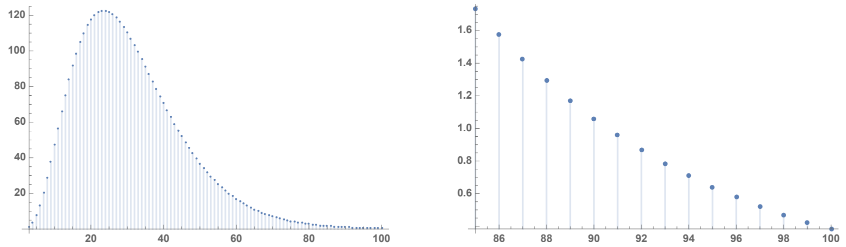


FIGURE 7. Plots of $\binom{n}{3}(7/8)^{n-3}$ with $3 \le n \le 100$ and $85 \le n \le 100$.

The event $B \cap C$ consists of flip sequences with an even number of heads in which heads outnumber tails. When $n = 4$, that means there have to be 4 heads, so $P(B \cap C) = 1/16 \neq 1/2 \cdot 5/16$, so B and C are not independent in general. □

Problem 9.2.3. There are n players in a Go tournament. In this problem we will use probability theory to show that for certain n it is possible for every collection of 3 players there exists another player who has beaten them all.

(a) Suppose that the outcome of each game is random. (Perhaps the players are lazy and flip a coin to decide the winner.) Fix a 3-subset $\{x, y, z\}$ of players and some player w not in $\{x, y, z\}$. What is the probability that w wins against x, y, and z? What is the probability that w loses against at least one of x, y, z?

(b) Suppose we have another player w' different from w, x, y, and z. Are the results of w''s matches against x, y, z independent of the results of w's matches?

(c) How many players can appear in the role of w? What is the probability that each of them loses against at least one of x, y, z?

(d) Use your answer to (c) and the fact that there are $\binom{n}{3}$ 3-subsets of $\underline{n}$ to produce an upper bound on the probability that for at least one 3-subset $\{x, y, z\}$, no player beats x, y, and z simultaneously.

(e) What does it mean if your upper bound from (d) is less than 1? Use a computer to determine if there are n for which this happens.

Solution. (a) There is a $1/8$ probability of w winning against x, y, and z (think of this as three heads in a row). The event of w losing at least once against x, y, z is complementary and has probability $7/8$.

(b) Yes, player w's outcomes are independent of w''s.

(c) There are $n - 3$ players who are not x, y, or z. The probability that all of them lose against at least one of x, y, z is $(7/8)^{n-3}$.

(d) This event is the union over all 3-subsets $\{x, y, z\}$ of the event in (c). Thus its probability is at most $\binom{n}{3}(7/8)^{n-3}$ since $P(A \cup B) \le P(A) + P(B)$ in general.

(e) If $\binom{n}{3}(7/8)^{n-3} < 1$, then in a positive fraction of tournaments, there exists a 3-subset of players defeated defeated by a single player.

As it turns out, this expression is less than 1 for all $n \ge 91$, so we are certain that such a tournament exists whenever there are 91 or more players. You can see a plot of $\binom{n}{3}(7/8)^{n-3}$ in Figure 7.

□

9.3. **Friday.** Discussion of *Todos Cuentan*.

10. WEEK 10

10.1. **Monday.**

Problem 10.1.1 (The Monty Hall problem). A game show provides contestants with the opportunity to win a car. There are three doors labeled A, B, and C. Behind two of the doors are goats, and behind one of the doors is a car. For reasons not completely clear to your instructor, you hope to select the car instead of a goat. The game proceeds in the following fashion: First, you select a door. Next, the host reveals a goat behind one of the remaining doors. (Since there are two goats, there is at least one goat to reveal.) You are then given the chance to switch your guess. If your final guess is the door with the car behind it, you win the car. **Question:** Is it advantageous to switch your guess?

Here are some assumptions on the problem which should remove any ambiguity:

» The probability that the car is placed behind any one of the three doors is $1/3$.
» The host knows where the car is.
» If the contestant picks a door with a goat behind it at the beginning, the host opens the remaining door with a goat before giving the option to switch. If the contestant picks the door with the car behind it, the host opens any of the other doors with probability $1/2$.

In class, we discussed a decision tree method for answering the question, but it is also possible to think in terms of conditional proability. Suppose that you initially pick door A and then let A, B, and C denote the events "the car is behind door A," "door B," and "door C," respectively. Let M_A, M_B, and M_C denote the events "the host opens door A," "door B," and "door C," respectively.

(a) What are $P(M_C|A)$, $P(M_C|B)$, and $P(M_C|C)$?
(b) What is $P(M_C)$? (Use the Law of Total Probability.)
(c) Suppose that the host opens door C revealing a goat. You should switch your guess to B if $P(B|M_C) > P(A|M_C)$. Compute these conditional probabilities (via Bayes' Law) and draw a conclusion.

Solution. By hypothesis, $P(A) = P(B) = P(C) = 1/3$. If we have initially picked A and the car is behind A, then the host will open B or C with equal probability. Thus $P(M_B|A) = 1/2, P(M_C|A) = 1/2, P(M_A|A) = 0$. If we have initially picked A and the car is behind B or C, then the host has only one door he can open, namely C or B, respectively. Thus $P(M_C|B) = 1$ and $P(M_B|C) = 1$.

Now suppose that the host opens door C. We want to compute $P(A|M_C)$ and $P(B|M_C)$. If the first is larger, we should stay; if the second is larger, we should switch; and if they are equal then it doesn't matter whether we stay or switch. By Bayes' Theorem and the Law of Total Probability,

$$\begin{aligned} P(A|M_C) &= \frac{P(M_C|A)P(A)}{P(M_C)} = \frac{1/2 \cdot 1/3}{P(M_C|A)P(A) + P(M_C|B)P(B) + P(M_C|C)P(C)} \\ &= \frac{1/6}{1/2 \cdot 1/3 + 1 \cdot 1/3 + 0 \cdot 1/3} = \frac{1/6}{1/2} \\ &= \frac{1}{3} \end{aligned}$$

and

$$\begin{aligned} P(B|M_C) &= \frac{P(M_C|B)P(B)}{P(M_C)} = \frac{1 \cdot 1/3}{1/2} \\ &= \frac{2}{3}. \end{aligned}$$

The latter quantity is twice as large as the first, so we should switch! □

Problem 10.1.2. A student taking a true-false test always marks the correct answer when she knows it and decides true or false on the basis of flipping a fair coin when she does not know it. If the probability that she will know an answer is $3/5$, what is the probability that she knew the answer to a correctly marked question?

Solution. Let K denote the event of knowing the answer to a particular problem and let M denote the event of correctly marking that problem. We want to determine $P(K|M)$, and do so with Bayes' Law. First note that the problem tells us that $P(K) = 3/5$, $P(M|K) = 1$, and $P(M|K^c) = 1/2$. (Here K^c is the complement of K, the event in which the student does not know the answer.) By the Law of Total Probability,

$$P(M) = P(M|K)P(K) + P(M|K^c)P(K^c) = 1 \cdot 3/5 + 1/2 \cdot 2/5 = \frac{4}{5}.$$

Thus

$$P(K|M) = \frac{P(M|K)P(K)}{P(M)} = \frac{1 \cdot 3/5}{4/5} = \frac{3}{4}.$$

In other words, there is a 75% chance of the student knowing the answer to a correctly marked question. □

10.2. **Wednesday.**

Problem 10.2.1. The digits 1, 2, 3, 4 are randomly arranged into two two-digit numbers $\overline{AB}$ and $\overline{CD}$. In this problem you will ultimately determine the expected value of $\overline{AB} \cdot \overline{CD}$.

(a) If two of the digits 1, 2, 3, 4 are randomly selected (without replacement), what is their expected product?
(b) Write $\overline{AB}$ as a linear combination of the digits A and B. Similarly express $\overline{CD}$ in terms of C and D.
(c) Finally, use linearity of expectation and your answer to (a) to determine $E(\overline{AB} \cdot \overline{CD})$.

Solution. (a) The potential values of the product are $2, 3, 4, 6, 8, 12$. For each such product, there is a unique 2-element subset $\{a, b\} \subseteq \{1, 2, 3, 4\}$ such that ab is the product in question. There are $\binom{4}{2} = 6$ such pairs, and thus each value has a $1/6$ probability of being chosen. We conclude that the expected value is $(2 + 3 + 4 + 6 + 8 + 12) \cdot 1/6 = 35/6 = 5.8333\ldots$.
(b) We have $\overline{AB} = 10A + B$ and $\overline{CD} = 10C + D$.
(c) It follows that $\overline{AB} \cdot \overline{CD} = (10A + B)(10C + D) = 100AC + 10AD + 10BC + BD$. By linearity of expectation,

$$E(\overline{AB} \cdot \overline{CD}) = (100 + 10 + 10 + 1) \cdot \frac{35}{6} = \frac{4235}{6} = 705.8333\ldots.$$

□

Problem 10.2.2 (The coupon collector problem). Safeway is running a promotion in which they have produced n coupons and you randomly receive a coupon each time you check out. You passionately hope to one day collect all n coupons. What is the expected number of times T you'll have to check out at the store in order to collect all n? There's a very clever way to solve this problem with linearity of expectation!

(a) Label the coupons C_1, C_2, …, C_n. If $n = 4$, a successful collection of all 4 coupons might look like $C_2\ C_2\ C_4\ C_2\ C_1\ C_3$. Break the sequence into segments where a segment ends when you receive a new coupon. In the example sequence, the segments are C_2, $C_2\ C_4$, $C_2\ C_1$, C_3. Because it will make our lives easier and Kyle is a benevolent problem-writer, consider these the 0-th, 1-st, …, 3-rd segments (as opposed to 1-st through 4-th). Let X_k be the length of the k-th segment, and note that k ranges from 0 through $n - 1$. In the example, $X_0 = 1$, $X_1 = 2$, $X_2 = 2$, and $X_3 = 1$. Express T, the total number of checkouts needed to collect all coupons, as a linear combination of the X_k.

(b) Compute p_k, the probability that you will collect a new coupon given that you have already collected k of them. After studying the geometric distribution in Lecture 5, we will learn that $E(X_k) = 1/p_k$. Compute this value.
(c) Use your answers to (a) and (b) to determine $E(T)$.
(d) Can you say anything about the asymptotic behavior of $E(T)$?

Solution. (a) We have $T = X_0 + X_1 + \cdots + X_{n-1}$.
(b) We are seeking to collect one of the $n-k$ uncollected coupons out of the n total coupons, so $p_k = \frac{n-k}{n}$ and $E(X_k) = \frac{1}{p_k} = \frac{n}{n-k}$.
(c) By linearity of expectation,

$$\begin{aligned} E(T) &= \sum_{k=0}^{n-1} E(X_k) \\ &= \sum_{k=0}^{n-1} \frac{n}{n-k} \\ &= n \sum_{k=0}^{n-1} \frac{1}{n-k} \\ &= n \sum_{i=1}^{n} \frac{1}{i}. \end{aligned}$$

(d) It is beyond the scope of this course to prove so, but $E(T) = n \log n + \gamma n + O(1/n)$ where $\gamma \approx 0.577$ is the *Euler-Mascheroni constant*.

□

10.3. **Friday.**

Problem 10.3.1. With your group, roll a pair of dice twelve times. Record the first roll on which you roll doubles and also the total number of doubles that you roll and report these numbers to the instructor. What is the expected number of doubles in twelve rolls? How long should it take to roll doubles? How do these numbers compare with the class's statistics?

Solution. We can model the sample space as $\underline{6} \times \underline{6}$, in which case the event of doubles is the diagonal $\Delta = \{(a,a) \mid a \in \underline{6}\}$. Then under the uniform distribution, $P(\Delta) = 6/36 = 1/6$. Let X be the number of doubles out of 12 rolls. Let I_j denote teh indicator variable for the j-th roll being a double. Then $E(I_j) = P(I_j = 1) = P(\Delta) = 1/6$. Since $X = I_1 + \cdots + I_{12}$, $E(X) = 12 \cdot 1/6 = 2$. We expect two doubles to be rolled. □

Problem 10.3.2. An airline has sold 205 tickets for a flight that can hold 200 passengers. Each ticketed person, independently, has a 5% chance of not showing up for the flight. What is the probability that more than 200 people will show up for the flight?

Solution. Let X be the number of people who show up for the flight. We are looking for $P(X > 200) = P(X = 201) + P(X = 202) + \cdots + P(X = 205)$. Since this is a binomial random variable, $P(X = k) = \binom{205}{k}(0.95)^k(0.05)^{205-k}$. Thus

$$P(X > 200) = \sum_{k=201}^{205} \binom{205}{k} (0.95)^k (0.05)^{205-k} \approx 0.02236.$$

We conclude that the flight will be oversold about 2.2% of the time. □

Problem 10.3.3. If the same airline consistently oversells the flight from Problem 2 at the same rate, how many flights until we expect more ticketed passengers to show up than there are seats.

Solution. This is a geometric random variable with $p = P(X > 200) \approx 0.02236$. As such, the expected number of flights until an oversold one is $1/p \approx 44.7$. $\square$

11. Week 11

11.1. **Monday.** For integers a, b, we say that a *divides* b when an integer m exists such that $b = am$; in this case we also say that b *is a multiple of* a and that a *is a divisor of* b.

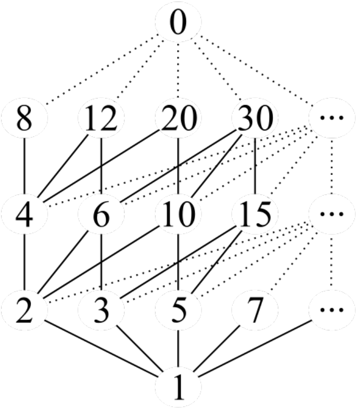
Question 11.1.1. When does $1 \mid b$? $-1 \mid b$? $a \mid 0$? $a \mid a$?

Solution. Since $b = 1 \cdot b$ for all $b \in \mathbb{Z}$, we have always have $1 \mid b$. Similarly, $b = (-1) \cdot (-b)$, so $-1 \mid b$ for all $b \in \mathbb{Z}$. Since $0 = a \cdot 0$, we always have $a \mid 0$, and sicne $a = a \cdot 1$, we always have $a \mid a$. □

Problem 11.1.2. Suppose that $a \mid b$ and $b \mid c$. Prove that $a \mid c$.

Solution. By hypothesis, there are integers m, m' such that $b = am$ and $c = bm'$. Thus $c = (am)m' = a(mm')$. Since mm' is an integer, this tells us that $a \mid c$. □

This produces a *partial order* on $\mathbb{N}$, visualized in the following diagram.



Question 11.1.3. Where should you put 9 in the diagram?

Solution. Since $9 = 3 \cdot 3$, it goes above 3 with lines coming in from 1 and 3, and lines going up to all multiples of 9. □

Problem 11.1.4. Prove that if $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$.

Solution. By hypothesis, $b = am$ and $c = an$ for some integers m, n. Thus $b + c = am + an = a(m + n)$, and since $m + n \in \mathbb{Z}$ we have that $a \mid b + c$. Similarly, $b - c = am - an = a(m - n)$, and since $m - n \in \mathbb{Z}$, $a \mid b - c$. □

A natural number $p > 1$ is *prime* if its only positive divisors are 1 and p. The fundamental theorem of arithmetic says that every positive integer is a product of primes, and that this factorization is unique up to reordering of the factors. For instance, $6 = 2 \cdot 3$, $1728 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 = 2^6 \cdot 3^3$ and $825 = 3 \cdot 5 \cdot 5 \cdot 11 = 3 \cdot 5^2 \cdot 11$. This probably seems like old hat, but not every number system has unique factorization! For instance, $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ supports addition and multiplication, but

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Number theorists are quite interested in objects like $\mathbb{Z}[\sqrt{-5}]$, but we will limit our study to $\mathbb{Z}$ where the fundamental theorem of arithmetic holds.

Question 11.1.5. Where should the prime numbers go in the divisibility diagram?

Solution. Above 1 and below everything else. □

Problem 11.1.6. Prove that a positive integer n is prime if and only if n is not divisible by any prime p with $1 < p \leq \sqrt{n}$.

Proof. First suppose that n is prime. Then it is not divisible by any positive integer except 1 and n, and thus is not divisible by the prime numbers in question.

Now suppose that n is not prime, which case it has prime factorization $n = p_1 p_2 \cdots p_k$ with $p_1 \leq \cdots \leq p_k$ all prime. Suppose for contradiction that $\sqrt{n} < p_1$. Then $n = \sqrt{n} \cdot \sqrt{n} < p_1 p_2 \leq n$, *i.e.*, $n < n$, a contradiction. □

Problem 11.1.7. Suppose that a positive integer n has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ with the p_i distinct primes. How many distinct positive integers are divisors of n?

Solution. The divisors of n take the form $p_1^{b_1} \cdots p_k^{b_k}$ with $0 \leq b_i \leq a_i$. Since there are $a_i + 1$ potential values of b_i, we know that n has $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ divisors. □

Problem 11.1.8. The book's proof does a fine job of guaranteeing that prime factorizations of integers are unique, but it elides the proof that prime factorization *exist*. Give an inductive proof that every positive integer has a prime factorization.

Solution. We want to show that every integer $n \geq 2$ has a prime factorization. Since 2 is prime, the base case holds. Fix an integer $n \geq 2$ and suppose that all integers $2 \leq m \leq n$ have prime factorization. If $n + 1$ is prime, then it has a prime factorization (itself), so suppose $n + 1$ is composite. Then there are integers $2 \leq a, b \leq n$ such that $n + 1 = ab$. By the strong inductive hypothesis, both a and b have prime factorizations, and the product of those factorizations is in turn a prime factorization of $ab = n + 1$. □

11.2. **Wednesday.** The key takeaways from §6.4 are that there are infinitely many prime numbers, and that the prime counting function $\pi(n) = |\{p \in \mathbb{N} \text{ prime} \mid p \leq n\}|$ grows like $n/\log n$. (Here we are using $\log$ for the natural logarithm function.) The first of these results is generally attributed to Euclid, c. 300B.C.E. Let's look at another proof due to Filip Saidak from 2005. In order to get it off the ground, prove the following result.

Problem 11.2.1. Let n be a positive integer. Prove that n and $n+1$ share no common divisors greater than 1.

Solution. If a divides n and $n + 1$, then a divides $(n + 1) - n = 1$. The only positive divisor of 1 is 1. □

Proof that there are infinitely many prime numbers. Let $n > 1$ be a positive integer. As we have just proven, n and $n + 1$ share no common divisors greater than 1. Hence the number $N_2 = n(n + 1)$ must have at least two distinct prime factors. Similarly, N_2 and $N_2 + 1$ share no common divisors greater than 1, and thus $N_3 = N_2(N_2+1)$ must have at least 3 distinct prime factors. We recursively define $N_k = N_{k-1}(N_{k-1}+1)$ for $k > 2$ and observe inductively that N_k has at least k distinct prime factors. □

Note that N_k has at least k distinct prime factors, each of which is necessarily smaller than N_k. It follows that $\pi(N_k) \geq k$.

Question 11.2.2. Compute N_k for $2 \leq k \leq 5$. Is this a very effective bound on the prime counting function?

Solution. Start with $n = 2$ so that $N_2 = 2 \cdot 3 = 6$, $N_3 = 6 \cdot 7 = 42$, $N_4 = 42 \cdot 43 = 1806$, and $N_5 = 1806 \cdot 1807 = 3,263,442$. The smallest number with 5 distinct prime divisors is $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$, so this is not very efficient! □

The vaunted Prime Number Theorem (PNT) says that

$$\pi(n) \sim \frac{n}{\log n},$$

which means that

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\log n} = \lim_{n\to\infty} \frac{\pi(n)\log n}{n} = 1.$$

The proof is very difficult and beyond the scope of this course, but we will still happily use the result.

Problem 11.2.3. Show that $\lim_{n\to\infty} \pi(n)/n = 0$ and use this to show that for any $a \in \mathbb{R}$,

$$\pi(n) \sim \frac{n}{\log(n) - a}.$$

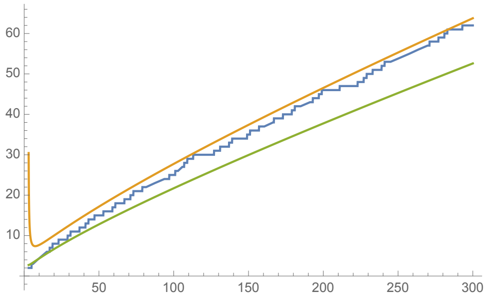
Solution. By the prime number theorem, $\pi(n)\log n/n \to 1$ as $n \to \infty$. Since $\log n \to \infty$, we must have $\pi(n)/n \to 0$ (otherwise PNT would not hold).

Now fix $a \in \mathbb{R}$ and observe that

$$\frac{\pi(n)(\log n - a)}{n} = \frac{\pi(n)\log n}{n} - \frac{a\pi(n)}{n}.$$

By PNT, the first term goes to 1, and we have just proven that the second term goes to 0. Thus $\pi(n) \sim n/(\log n - a)$. □

It turns out that $a = 1$ gives the best approximation to $\pi(n)$. In the below plot, the curve on top is the graph of $n/(\log(n) - 1$, the middle curve is the graph of $\pi(n)$, and the bottom curve is the graph of $n/\log n$.



11.3. **Friday.**

Problem 11.3.1. As an intrepid wagon wheel painter living in the Olde West, you strive to bring the highest quality, most engaging, non-monochromatic spoke paintings to your customers. You offer wagon wheels with p spokes, where p is a prime integer, painted in up to a colors, where $1 \leq a \leq p - 1$.

(a) As part of your preparation for painting, you have nailed a wagon wheel to the wall so that it can't rotate. In how many ways can you paint its spokes, assuming that each spoke gets a single color but at least two of the spokes are different colors?

(b) When you take the wheel off of the wall and fix it to an axle, you remember that it will rotate, and that your demanding customers will not accept rotated spoke paintings as genuinely different. As you turn this particular wheel around, you notice something remarkable: all of the rotations by multiples of $2\pi/p$ result in distinct colorings in the wheel-nailed-to-wall sense of unique, despite the fact that there are multiple spokes of the same color (since $a < p$). Is this a special property of your particular spoke painting, or is it true of all possible non-monochromatic paintings with a colors?

(c) Use your work in (b) to determine the total number wagon wheel paintings which your customers will accept as genuinely different. What can you deduce from the fact that this number is an integer?

Solution. (a) If we allow all colorings with each spoke one of a colors, then there are a^p colorings. Of these, a colorings are monochromatic, so there are $a^p - a$ non-monochromatic colorings.

(b) The phenomenon is generic when the number of spokes is prime. Indeed, if we can rotate by $2\pi k/p$ (for $1 \leq k < p$ an integer) and get the same coloring, then the pattern repeats every k spokes, and thus k divides p. Since p is prime, $k = 1$, but that means the pattern is monochromatic.

(c) The nailed-to-the-wall count of $a^p - a$ overcounts by a factor of p (the number of ways to rotate one pattern into others). Thus $\frac{a^p-a}{p}$ is an integer; in particular, p divides $a^p - a$. This is *Fermat's little theorem*.

□

Problem 11.3.2. How many 6-spoke wheels can you paint non-monochromatically with up to a colors for $a = 2, 3, 4, 5$?

12. Week 12

12.1. **Monday.** The *greatest common divisor* $d = \gcd(a,b)$ of integers a, b is the largest positive integer such that $d \mid a$ and $d \mid b$. We say that a and b are *relatively prime* when they share no divisors larger than 1, and this is equivalent to $\gcd(a,b) = 1$.

Problem 12.1.1. Draw a divisor diagram for 84 and 105. Where does the $\gcd$ appear in partially ordered set of divisors?

Solution. The $\gcd$ is the "greatest lower bound" (or *infimum*) of the common divisors of 84 and 105. □

If we know the prime factorizations of a and b, this number is easy to determine. Let $\{p_1, p_2, \ldots, p_k\}$ be the set of distinct prime divisors of a and b. Then we may write

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \\ b &= p_1^{b_1} p_2^{b_2} \cdots p_k^{a_k} \end{aligned}$$

for nonnegative integers a_i, b_i and

$$\gcd(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_k^{\min\{a_k,b_k\}}.$$

It is frequently the case, though, that we do not have access to the prime factorizations of integers. In this case, the *Euclidean algorithm* allows us to determine the greatest common divisor. Let's execute the algorithm with $a = 81$, $b = 57$:

$$\begin{aligned} 81 &= 1 \cdot 57 + 24 \\ 57 &= 2 \cdot 24 + 9 \\ 24 &= 2 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

We conclude that the final nonzero remainder, 3, is the $\gcd$ of 81 and 57. Indeed, $81 = 3^4$ and $57 = 3 \cdot 19$, so this agrees with our first method for determining $\gcd$'s.

The Euclidean algorithm can be described formally as follows:

1. Assume $a > b$ are integers (if $a < b$, swap them).
2. Perform long division to express to express $a = qb + r$ where $0 \le r \le b - 1$.
3. Replace a with b and b with r.
4. If $r \neq 0$, return to step 2; else
5. if $r = 0$, conclude that the final nonzero remainder is $\gcd(a,b)$.

A generic run of the algorithm then looks like

$$\begin{aligned} a &= q_0 b + r_1 \\ b &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

where $1 \le r_k \le r_{k-1}$ and we conclude that $r_n = \gcd(a,b)$ (since $r_{n+1} = 0$).

Problem 12.1.2. Suppose an integer x divides integers y and z. Show that for any $k, \ell \in \mathbb{Z}$, $x \mid ky + \ell z$.

Solution. We know that there are integers m, n such that $y = mx$, $z = nx$. Thus $ky + \ell z = kmx + \ell nx = (km + \ell n)x$, exhibiting that x divides $ky + \ell z$ since $km + \ell n \in \mathbb{Z}$. □

Problem 12.1.3. Why does the Euclidean algorithm work? Start at the end of the algorithm and check that $r_n \mid r_{n-1}$, then inductively check that $r_n \mid r_k$ for $-1 \leq k \leq n$ where we write $r_0 = b$ and $r_{-1} = a$ for notational convenience. Conclude that r_n divides a and b. Use a similar argument starting at the beginning of the algorithm to show that $\gcd(a, b)$ divides r_k for $-1 \leq k \leq n$. Why does this prove that the algorithm produces the $\gcd$.

Solution. The equation $r_{n-1} = q_n r_n$ clearly exhibits that $r_n \mid r_{n-1}$. Fix $0 \leq k \leq n$ and assume for (downward, strong) induction that $r_n \mid r_\ell$ for $k \leq \ell \leq n$. The equation $r_{k-1} = q_k r_k + r_{k+1}$ expresses r_{k-1} as an integral linear combination of r_k and r_{k+1}, both of which are divisible by r_n, hence r_n divides r_{k-1} as well. We conclude that $r_n \mid r_k$ for all $-1 \leq k \leq n$, including $r_{-1} = a$ and $r_0 = b$.

Beginning with $a = q_0 b + r_1$, we have $r_1 = a - q_0 b$ and hence any common divisor of a and b divides r_1. In general, $r_k = r_{k-2} - q_{k-1} r_{k-1}$, permitting a strong inductive proof that $\gcd(a, b)$ divides r_k for $-1 \leq k \leq n$.

We now know that r_n is a common divisor of a and b and that $\gcd(a, b) \mid r_n$. This makes r_n a divisor of a and b which is at least as large as $\gcd(a, b)$, whence $r_n = \gcd(a, b)$. □

Problem 12.1.4. The Euclidean algorithm gives us a way to dissect a rectangle with integer sides into squares. Run the Euclidean algorithm to find $\gcd(23, 13)$. Interpret the first step ($23 = 1 \cdot 13 + 10$) as telling you that $q_0 =$ 1-many 10×10 squares fit inside a 23×13 rectangle. Figure out what instructions the rest of the algorithm is giving you and draw a corresponding picture. At the end, your 23×13 rectangle should be partitioned into squares! What is special about this procedure if you start with consecutive Fibonacci numbers $a = F_{n+1}$, $b = F_n$?

Solution. The Euclidean algorithm runs as follows:

$$\begin{aligned} 23 &= 1 \cdot 13 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

This corresponds to breaking a 23×13 rectangle into one 13×13 square, one 10×10 square, three 3×3 squares, and three 1×1 squares.

If you start with F_{n+1} and F_n, the Euclidean algorithm has $q_k = 1$ for all k and you get the Fibonacci approximation to the golden rectangle. □

Problem 12.1.5. Run the Euclidean algorithm when $a = 45$, $b = 16$. How is it related to the expression

$$\frac{45}{16} = 2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3}}}?$$

Come up with a general procedure by which the Euclidean algorithm produces *continued fraction* expressions for rational numbers of the form

$$\frac{a}{b} = x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{x_4 + \cdots}}}$$

where the x_i are integers.

Solution. The Euclidean algorithm runs as follows:

$$\begin{aligned}45 &= 2\cdot 16+13\\ 16 &= 1\cdot 13+3\\ 13 &= 4\cdot 3+1\\ 3 &= 3\cdot 1+0.\end{aligned}$$

We have $x_k = q_{k-1}$. □

12.2. **Wednesday.** The book says that integers a and b are congruent modulo another integer m (denoted $a \equiv b \pmod{m}$) if a and b have the same remainder upon division by m. In your homework, you will prove that this is equivalent to $m \mid a-b$, and you should assume this result for the rest of today's class.

Question 12.2.1. When is $a \equiv b \pmod{2}$? $a \equiv b \pmod{1}$? $a \equiv b \pmod{0}$?

Solution. We have $a \equiv b \pmod{2}$ when a and b are both odd or both even. Since $1 \mid a-b$ for all a, b, we always have $a \equiv b \pmod{1}$. We only have $0 \mid a-b$ when $a-b=0$, i.e., congruence modulo 0 is just equality of integers. □

Problem 12.2.2. Prove that $\equiv \pmod{m}$ is an equivalence relation on $\mathbb{Z}$. What are the associated equivalence classes? How many equivalence classes are there?

Solution. Fix m and write $\equiv$ for congruence modulo m. This relation is reflexive ($a \equiv a$) since $m \mid 0 = a-a$. It is symmetric since when $m \mid a-b$ we also have $m \mid b-a = (-1)(a-b)$. For transitivity, suppose $a \equiv b$ and $b \equiv c$, in which case there are integers k, ℓ such that $a-b=km$ and $b-c=\ell m$. Then $a-c=(a-b)+(b-c)=(k+\ell)m$, so $a \equiv c$, as desired.

Write $\overline{a}$ for the equivalence class of a modulo m. Then

$$\overline{a} = \{a+km \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}$$

and there are exactly m equivalence classes,

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}.$$

□

When considering the equivalence relation $\equiv \pmod{m}$ on $\mathbb{Z}$, we write $\overline{a}$ for the equivalence class of a. (We elide m from the notation; it should be clear from context.) We call $\overline{a}$ the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(\equiv \pmod{m})$ for the set of congruence classes modulo m.

Problem 12.2.3. Define addition and multiplication of equivalence classes in $\mathbb{Z}/m\mathbb{Z}$. Show that for every $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ there exists $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ such that $\overline{a}+\overline{b}=\overline{0}$.

Solution. We define $\overline{a}+\overline{b}=\overline{a+b}$ and $\overline{a}\cdot\overline{b}=\overline{ab}$. These are well-defined operations since

$$\overline{(a+km)+(b+\ell m)} = \overline{(a+b)+(k+\ell)m} = \overline{a+b}$$

and

$$\overline{(a+km)(b+\ell m)} = \overline{ab+(a\ell+bk+k\ell m)m} = \overline{ab}.$$

Since $\overline{a}+\overline{m-a}=\overline{m}=\overline{0}$, $\mathbb{Z}/m\mathbb{Z}$ has additive inverses. □

Let's now shift gear and discuss the *dynamics* of addition in $\mathbb{Z}/m\mathbb{Z}$. Fix $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$. Make a directed graph[5] $G(\overline{a}, m)$ with vertex set $\mathbb{Z}/m\mathbb{Z}$ such that $(\overline{b}, \overline{c})$ is an edge if and only if $\overline{c}=\overline{b}+\overline{a}$.

[5] The edges in a directed graph have a source and target, indicated by an arrow. Thus the edges in a directed graph are encoded by ordered pairs of vertices, with first entry the source, and second entry the target.

Problem 12.2.4. Draw $G(\overline{a}, m)$ for a germane collection of $\overline{a}$ and m.

Problem 12.2.5. Make a conjecture regarding the shape of $G(\overline{a}, m)$. Prove it.

Solution. The graph $G(\overline{a}, m)$ consists of disjoint directed cycles, all of the same size. Each cycle has length ℓ where ℓ is the smallest positive integer such that $\ell a \equiv 0 \pmod{m}$. We can re-express this number as $\ell = \operatorname{lcm}(a, m)/a$. □

12.3. **Friday.** In §6.8 you learned that there are commutative, associative operations $+, \cdot$ on $\mathbb{Z}/n\mathbb{Z}$ and that $+$ admits an inverse $-$ such that $\overline{a} - \overline{a} = \overline{0}$. When n is prime, everything in $\mathbb{Z}/n\mathbb{Z}^\times = \mathbb{Z}/n\mathbb{Z} \smallsetminus \{\overline{0}\}$ admits a multiplicative inverse as well, *i.e.*, for each $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^\times$, there exists $\overline{a}^{-1} \in \mathbb{Z}/n\mathbb{Z}^\times$ such that $\overline{a} \cdot \overline{a}^{-1} = \overline{1}$. We sometimes write $\overline{1}/\overline{a}$ for $\overline{a}^{-1}$ and $\overline{a}/\overline{b}$ for $\overline{a}\overline{b}^{-1}$.

Problem 12.3.1. Our previous version of Fermat's little theorem said that if p was prime and $1 \leq a \leq p-1$, then $p \mid a^p - a$. Of course, $p \mid 0 = 0^p - 0$, so this holds for $0 \leq a \leq p-1$ as well.

(a) Check that this is equivalent to $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.
(b) Suppose $a \not\equiv 0 \pmod{p}$. Prove that $a^{p-1} \equiv 1 \pmod{p}$.
(c) For $p > 2$, what are the possible values of $a^{(p-1)/2}$ mod p? (Note that $p-1$ is even when $p > 2$, so $(p-1)/2$ makes sense.)
(d) For $a \in \mathbb{Z}$ such that $a \not\equiv 0 \pmod{p}$, define $o_p(a)$ (the *order of a modulo p*) to be the smallest positive integer such that $a^{o_p(a)} \equiv 1 \pmod{p}$. Since $a^{p-1} \equiv 1 \pmod{p}$, we know that $1 \leq o_p(a) \leq p-1$. Prove that $o_p(a) \mid p-1$.
(e*) Prove that there exists $a \in \mathbb{Z}$ such that $o_p(a) = p-1$.
(f) Assume (e*) (which is a challenge problem you can try outside of class) and take $a \in \mathbb{Z}$ such that $o_p(a) = p-1$. Show that each a^n, $1 \leq n \leq p-1$, is in a distinct congruence class modulo p and thus the values of a^n cycle through all the nonzero congruence classes mod p with period $p-1$.[6]

Solution. (a) The congruence $a^p \equiv a \pmod{p}$ means that p divides $a^p - a$, as desired.
(b) If $a \not\equiv 0 \pmod{p}$, then a has a multiplicative inverse modulo p. Multiplying both sides of the congruence by this inverse results in $a^{p-1} \equiv 1 \pmod{p}$.
(c) Working in $\mathbb{Z}/p\mathbb{Z}$ (and dropping the bars from our notation), let $b = a^{(p-1)/2}$. Then $b^2 = a^{p-1} = 1$, whence $0 = b^2 - 1 = (b+1)(b-1)$. Thus $b = \pm 1$.
(d) First let $o = o_p(a)$ and use the division algorithm to write $p - 1 = qo + r$ where $0 \leq r < o$. Then $qo = p-1-r$ and thus $1 = 1^q = (a^o)^q = a^{qo} = a^{p-1-r}$. Multiplying by a^r we get $a^r = a^{p-1} = 1$. Since o is the minimal positive integer such that $a^o = 1$, we know that $r = 0$, whence $o \mid p-1$, as desired.
(e) We will leave this is a challenge problem — it's hard, but important!
(f) Take $1 \leq m \leq n \leq p-1$ and suppose $a^m = a^n \in \mathbb{Z}/p\mathbb{Z}$. Then $1 = a^{n-m}$ where $0 \leq n-m \leq p-2$. Since $o_p(a) = p-1$, we must have $n - m = 0$, *i.e.*, $n = m$. Since the values of a^n with $1 \leq n \leq p-1$ are distinct, there are $p-1$ of them, and they all live in $\mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\}$ (which has size $p-1$), we get that $\mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\} = \{a^n \mid 1 \leq n \leq p-1\}$.

□

Problem 12.3.2. Make a multiplication table for $\mathbb{Z}/7\mathbb{Z}^\times$. Select a congruence class and circle all its occurrences in the table. Observe that this is a solution to the non-capturing rooks problem on a 6×6 chessboard. Does it work for other congruence classes? For $\mathbb{Z}/p\mathbb{Z}^\times$ and $(p-1) \times (p-1)$ chessboards in general? Why?

Proof. This works in general because with fixed $a, c \in \mathbb{Z}/p\mathbb{Z}^\times$, there is a unique $b \in \mathbb{Z}/p\mathbb{Z}^\times$ such that $ab = c$. (Indeed, $b = c/a$.) □

[6] An algebraist would say that $\mathbb{Z}/p\mathbb{Z}^\times$ is a cyclic group of order $p-1$.

Problem 12.3.3. How many squares are there mod p? *i.e.*, how large is $\{\overline{x}^2 \mid \overline{x} \in \mathbb{Z}/p\mathbb{Z}^\times\}$? What is the probability that $x^2 \equiv a \pmod{p}$ will have a solution? Suppose $x^2 \equiv a \pmod{p}$ has a solution; how many solutions does it have? In the diagonal of the multiplication table for $\mathbb{Z}/p\mathbb{Z}^\times$, why does $\overline{1}$ always and only appear in the top left and bottom right corner?

Proof. The squaring function is 2-to-1 onto its image, so its image must have size $(p-1)/2$. Thus $1/2$ of the equations $x^2 \equiv a \pmod{p}$ have solutions (for varying $1 \leq a \leq p-1$).

The final observation is just that $1^2 = 1$ and $(p-1)^2 = (-1)^2 = 1$. □

Problem 12.3.4. Your vitamin regimen requires you to take *Doctor Snoggleswarf's Health Elixir* ® every five days. You take the first dose in the bottle on a Sunday and the final dose on a Thursday. You're not sure how many doses you took, but you know that there are at least 50 doses in a bottle. What is the minimum number of doses you took?

Solution. Number the days 0 through 6, starting with Sunday, and note that Thursday corresponds to 4. You take the n-th dose on the day corresponding to the congruence class of $5(n-1)$ modulo 7. Thus we are looking for the minimum $n \geq 50$ such that $5(n-1) \equiv 4 \pmod{7}$. Adding 5 to both sides, this becomes $5n \equiv 2 \pmod{7}$. The multiplicative inverse of 5 mod 7 is 3 (since $3 \cdot 5 = 15 \equiv 1 \pmod{7}$), and thus $n \equiv 6 \pmod{7}$. Recalling that $50 \equiv 1 \pmod{7}$, we see that n must be 55. □

13. Week 13

13.1. **Monday.** Suppose $n = p_1^{a_1} \cdots p_k^{a_k}$ for positive integers a_i and distinct primes p_i. Recall that $\phi(n)$ is the number of positive integers smaller than n and relatively prime to n. We claim that

$$\phi(n) = n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k).$$

To prove this, we count the number of positive integers which are at most n and are not relatively prime to n. This is the case if and only if one of the p_i divides n. Of course, there are n/p_i positive integers $\leq n$ and divisible by p_i, so it is tempting to guess that $\phi(n) = n - (n/p_1 + n/p_2 + \cdots + n/p_k)$, but inclusion-exclusion tells us we need to be more careful with numbers which are divisible by multiple primes. The correct formula is

$$\phi(n) = n - \sum_{1 \leq i \leq k} \frac{n}{p_i} + \sum_{1 \leq i_1 < i_2 \leq k} \frac{n}{p_{i_1} p_{i_2}} - \sum_{1 \leq i_1 < i_2 < i_3 \leq k} \frac{n}{p_{i_1} p_{i_2} p_{i_3}} + \cdots \pm \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}$$

where the signs alternate and the final sign is $+$ if k is even and $-$ if k is odd. Factoring out an n and thinking deeply about the distributive law, we see that this is the same as

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

What a remarkable formula! For instance, if $n = 6160 = 2^3 \cdot 5^2 \cdot 7 \cdot 11$, then

$$\phi(6160) = 6160(1 - 1/2)(1 - 1/3)(1 - 1/5)(1 - 1/7)(1 - 1/11) = 1280.$$

Also note that there is a probabilistic interpretation of this formula. The probability that an integer between 1 and n is relatively prime to n is

$$\frac{\phi(n)}{n} = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Fascinatingly, the probability only depends on the primes dividing n, and it suggests an alternate proof of our formula.

Problem 13.1.1. Let $\underline{n}$ be our sample space with uniform distribution. Define the event ND_i to be the set of $r \in \underline{n}$ such that $p_i \nmid r$.

(a) What is $P(ND_i)$?

(b) Let RP be the collection of $r \in \underline{n}$ which are relatively prime to n. Check that $RP = ND_1 \cap ND_2 \cap \cdots \cap ND_k$.

(c) Argue that the events ND_i are independent and thus $P(RP) = P(ND_1) \cdots P(ND_k)$. Note that this is equivalent to the above formula for $\phi(n)$.

Solution. (a) Let's first consider the complementary event of $r \in \underline{n}$ divisible by p_i. These are precisely $p_i, 2p_i, 3p_i, \ldots, (n/p_i) \cdot p_i$, so there are n/p_i such integers. As such, $|ND_i| = n - n/p_i$ and

$$P(ND_i) = \frac{n - n/p_i}{n} = 1 - \frac{1}{p_i}.$$

(b) In order that $\gcd(r, n) = 1$, r and n must share no common divisors. This is the case if and only if $p_i \nmid r$ for all prime divisors p_i of n. This in turn is the intersection $ND_1 \cap \cdots \cap ND_k$.

(c) These events are independent if and only if their complements are independent. (Check this!) A number is divisible by $p_1, \ldots, p_k$ if and only if it is divisible by $p_1 \cdots p_k$. The probability of the latter event is

$$\frac{n/(p_1 \cdots p_k)}{n} = \frac{1}{p_1 \cdots p_k}.$$

This is equal to

$$\frac{1}{p_1} \cdots \frac{1}{p_k},$$

the product of the individual events. This proves independence.[7]

□

13.2. **Wednesday.**

Question 13.2.1. Solve the system of congruences

$$2x \equiv 5 \pmod 7$$
$$3x \equiv 4 \pmod 8.$$

Solution. First multiply the first congruence by the mod 7 inverse of 2, which is 4, to get $x \equiv 6 \pmod 7$. Then multiply the second congruence by the mod 8 inverse of 3, which is 3, to get $x \equiv 4 \pmod 8$.

Since 7 and 8 are relatively prime, Sunzi's theorem applies, there is exactly one solution $0 \leq x_0 < 7 \cdot 8 = 56$ and all other solutions are of the form $x_0 + 56n$ for some $n \in \mathbb{Z}$. The solutions to $x \equiv 4 \pmod 8$ between 0 and 55 are

$$4, 12, 20, 28, 36, 44, 52.$$

The only one of these satisfying $x \equiv 6 \pmod 7$ is $x_0 = 20$. Thus all solutions are of the form $20 + 56n$, $n \in \mathbb{Z}$. □

Problem 13.2.2. What is the remainder when you divide 135^3 by 1728? (*Hint*: $1728 = 64 \cdot 27$.)

Solution. The remainder under consideration is the unique r such that $0 \leq r < 1728$ and $r \equiv 135^3 \pmod{1728}$. Such an r also satisfies the congruences

$$r \equiv 135^3 \pmod{64}$$
$$r \equiv 135^3 \pmod{27}.$$

Since $135 \equiv 7 \pmod{64}$, we know that $135^2 \equiv 7^2 \equiv -15 \pmod{64}$ and $135^3 \equiv -15 \cdot 7 \equiv -105 \equiv 23 \pmod{64}$. Similarly, since $135 \equiv 0 \pmod{27}$, we have $135^3 \equiv 0 \pmod{27}$. Thus we may rewrite the system of congruences as

$$r \equiv 23 \pmod{64}$$
$$r \equiv 0 \pmod{27}.$$

By the second congruence, we know that r is of the form $27k$ for some integer k. Since $\gcd(27, 64) = 1$, we know that 27 has a multiplicative inverse mod 64. Running the extended Euclidean algorithm, we find that 19 is its inverse, whence $k \equiv 19 \cdot 23 \equiv 437 \equiv 53 \pmod{64}$. Thus $r = 27 \cdot 53 = 1431$. □

Recall that the Fermat-Euler Theorem is a generalization of Fermat's Little Theorem which states that

$$a^{\phi(n)} \equiv 1 \pmod n$$

when $\gcd(a, n) = 1$. We will prove a special case of this theorem in which n is the product of k distinct primes, $n = p_1 p_2 \cdots p_k$. In this case, $\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$. Let $q_i = \phi(n)/(p_i - 1)$ for $i = 1, 2, \ldots, k$. Then

$$a^{\phi(n)} = (a^{p_i - 1})^{q_i} \equiv 1^{q_i} \equiv 1 \pmod{p_i}$$

for all i. We see then that $x = a^{\phi(n)}$ is a simultaneous solution of the congruences

$$x \equiv 1 \pmod{p_1},\ x \equiv 1 \pmod{p_2},\ \ldots,\ x \equiv 1 \pmod{p_k}.$$

[7] For full independence, we would need to check this for any subset of prime divisors, but the argument is the same.

But $x = 1$ is another solution! By Sunzi's theorem, it follows that $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Problem 13.2.3. How can the above argument be extended to the case in which $n = p_1^{a_1} \cdots p_k^{a_k}$ where the p_i are distinct primes and $a_i \geq 1$?

Solution. The extension is possible and hinges on considering congruence classes modulo $p_i^{a_i}$. For variety's sake, here is a totally different method:

Enumerate the integers between 0 and n which are relatively prime to n: $x_1, x_2, \ldots, x_{\phi(n)}$. If $ax_i \equiv ax_j \pmod{n}$, then, multiplying by a^{-1} mod n gives $x_i \equiv x_j \pmod{n}$. This means that multiplication by a permutes the x_i's. As such,

$$\prod_{i=1}^{\phi(n)} x_i \equiv \prod_{i=1}^{\phi(n)} ax_i \equiv a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i \pmod{n}.$$

Multiplying by $(\prod x_i)^{-1}$ mod n gives $1 \equiv a^{\phi(n)} \pmod{n}$, as desired. □

13.3. **Friday.** Review session.