Honors - Introduction to Discrete Math

Raymond Bian

November 28, 2023

Contents

We used sets to talk about *relations*. Depending what relations we were looking at, we could determine whether they were *reflextive, symmetric, antisymmetric, or transitive.*

Definition 1. An **equivalence relation** is one that is reflexive, symmetric, and transitive.

Definition 2. An **ordering relation** is one that is reflexive, antisymmetric, and transitive.

1 Functions

Below are some definitions that we use for functions.

Definition 3. A **function** is a relation such that $\forall a \exists! b(f(a) = b)$.

Definition 4. For a particular function $f\colon A \to B$, we call A the **domain** and B the **codomain**.

Definition 5. The **range** of f is $\{b \in B \mid \exists a \in A(f(a) = b)\}$

Definition 6. We say f is **one-to-one** if $\forall x, y \in A(x \neq y \Rightarrow f(x) \neq f(y))$. Another word for this is **injective**. We can use the contrapositive to prove a function f is injective.

Definition 7. We say f is **onto** if $\forall b \in B(\exists a \in A(f(a) = b))$.

Definition 8. A **bijection** is a function f that is one-to-one and onto.

Definition 9. Given a bijection f, we define the **inverse function** f^{-1}

$$f^{-1}: B \to A$$
$$f^{-1}(b) = a \Leftrightarrow f(a) = b$$

Property. f^{-1} is a bijection.

Example. Consider:

$$f: \mathbb{R} \to \mathbb{R}^+$$
$$x \to x^2.$$

This function by itself is not one-to-one. But note that we can make restrictions in our domain and codomain to make this function a bijection. ◇

Example. Consider:

$$\sin: \mathbb{R} \to \mathbb{R}.$$

This function is not one-to-one and onto (not a bijection). Therefore, to find the inverse of the function, we restrict the domain and codomain.

$$\sin: \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1, 1].$$

◇

Definition 10. Let S be a set. We say S has **cardinality** n if S has exactly n elements (there is a bijection from S to the set $[n] = \{1, 2, 3, \ldots, n\}$). We write $|S| = n$.

Remark. Cardinality is *well defined* because you have no bijection between $[n]$ and $[m]$ for $n \neq m$.

Remark. If S is infinite, then we say $|S| = \infty$. In other words, there does not exist a biection from S to any $[n]$.

Definition 11. Let A and B be sets. We say $|A| = |B|$ if there is a bijection from A to B.

Example. Let $\sim$ be a relation on $\mathcal{P}(U)$. $A \sim B$ if there is a bijection from A to B. Are all infinite sets the same? ◇

2 Countability

What does it mean for a set to be countable?

Definition 12. A set S is **countable** if there is a one-to-one mapping ($\exists f : S \to \mathbb{N}$ that is a bijection) from S to $\mathbb{N}$.

- Every finite set is countable.
- $\mathbb{N}$ is countable (you can map $\mathbb{N}$ to itself).
- $2\mathbb{N} = \{2a \mid a \in \mathbb{N}\}$ is countable.

$$\begin{aligned} f : 2\mathbb{N} &\to \mathbb{N} \\ 2a &\to a. \end{aligned}$$

Remark. There is a one-to-one mapping between sets $2\mathbb{N}$ and $\mathbb{N}$. That means they have the same cardinality, even if this goes against our intuition.

Lecture 12: Properties of Countable Sets; Cantor's Diagonalization Argument

Continuing on from last time, we also have that $\mathbb{Z}$ is countable as well.

Theorem 1. $\mathbb{Z}$ is countable.

Proof. Construct $f : \mathbb{Z} \to \mathbb{N}$. Define:

$$f(n) = \begin{cases} 0 & n = 0 \\ 2n & n > 0 \\ -2n + 1 & n < 0 \end{cases}.$$

We wish to prove that $\forall x, y (x \neq y \Rightarrow f(x) \neq f(y))$. Proceeding by contraposition, given $f(n) = f(m)$, we have the following cases:

Case 1: $n = 0$. Then $f(n) = 0 = f(m) \Rightarrow m = 0$.

Case 2: $n > 0, m > 0$. Then $f(n) = 2n = f(m) = 2m \Rightarrow 2n = 2m \Rightarrow n = m$

Case 3: $n > 0, m < 0$. Then $f(n)$ is even and $f(m)$ is odd $\lightning$. Vacuously true.

The other cases are analogous! □

Property. Let A, B be countable sets. There are the following properties of countable sets:

- $\{a\} \cup A$ is countable.

  Proof. We wish to find $g : \{a\} \cup A \to \mathbb{N}$. Construct

  $$g(x) = \begin{cases} 0 & x = a \\ f(x) + 1 & x \in A \end{cases}.$$

  □

- $F \cup A$ is also countable for any finite set F.
- $A \cup B$ is also countable.

- If $f\colon S \to A$ is one-to-one and A is countable, then S is countable.
- $A \times B$ is countable.
- $S \subseteq A$ is countable.

  Proof. Given $f\colon A \to \mathbb{N}$ is one-to-one, its restriction to S is also one-to-one. □
- $\mathbb{Q}$ is countable.

  Proof. This is because $\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{Z}$. □

2.1 Cantor's Diagonalization Argument

What about the real numbers?

Theorem 2. $\mathbb{R}$ is not countable (Cantor).

Proof. Prove instead that $(0, 1)$ (a subset of $\mathbb{R}$) is **not** countable. We will argue by contradiction. We assume that $(0, 1)$ is countable. Hence, there exists

$$f\colon (0, 1) \to \mathbb{N}.$$

shown below.

Table 1: Our one-to-one mapping (pages of our book)

$\mathbb{N}$	$(0, 1)$
0	$0.d_{11}d_{12}d_{13}d_{14}\ldots$
1	$0.d_{21}d_{22}d_{23}d_{24}\ldots$
2	$0.d_{31}d_{32}d_{33}d_{34}\ldots$
3	$0.d_{41}d_{42}d_{43}d_{44}\ldots$
$\vdots$	

Let's define $b \in \mathbb{R}$ as follows:

$$b = 0.b_1b_2b_3b_4\ldots.$$

where

$$b_i = \begin{cases} 3 & d_{ii} \neq 3 \\ 0 & d_{ii} = 3 \end{cases}.$$

Then, we claim that $f(b)$ is not well defined! In other words, there should exist $k \in \mathbb{N}$ in our book such that $f(b) = k$. However, we have constructed b such that $b_k \neq d_{kk}$: there is no $k \in \mathbb{N}$ that exists in our book $\lightning$ (b will always have one bit that is different from all entries in our mapping)! □

Exercise 1

Prove that $|S| \neq |\mathcal{P}(S)|$.

Lecture 13: Runtime Complexity

3 Analyzing Runtimes

How many comparisons should we make to choose the best out of n restuarants?

3.1 Big O Notation

Big O Notation does not care about constants.

Definition 13. Given $f, g\colon \mathbb{R} \to \mathbb{R}$, we say f is big-O of g (write $f = O(g)$) if

$$\exists C > 0, k \in \mathbb{R}(|f(x)| \leq C \cdot |g(x)| \quad \forall x \geq k)$$

where C and k are arbitrary constants (witnesses).

Example. Given $f, g\colon \mathbb{N} \to \mathbb{R}$, is $f = O(g)$:

- $f(n) = 2n + 1$, $g(n) = n - 10$? Yes.
- $f(n) = 2n + 1$, $g(n) = n + \sqrt{n}$? Yes.

  Proof. We have:

  $$\begin{aligned} 2n &\leq 2n && \forall n \in \mathbb{N} \\ 1 &\leq 2\sqrt{n} && \forall n \in \mathbb{N}, n > 0. \end{aligned}$$

  Adding both sides, we have

  $$f(n) \leq 2g(n) \quad \forall n \geq 1.$$

  Therefore, $f = O(g)$ for $C = 2, k = 1$. □

- $f(n) = n\log(n)$, $g(n) = n + \sqrt{n}$? No.

  Proof. We proceed by contradiction. Assume $f = O(g)$. Then, there exists $C > 0$ and $k \in \mathbb{N}$ such that

  $$n\log(n) \leq C(n + \sqrt{n}) \quad \forall n \geq k.$$

  Simplifying, we have:

  $$\begin{aligned} \log(n) &\leq C\left(\frac{n + \sqrt{n}}{n}\right) \\ &= C\left(\frac{n}{n} + \frac{\sqrt{n}}{n}\right) \\ &= C\left(1 + \frac{1}{\sqrt{n}}\right) \\ &\leq 2C \qquad \forall n \geq 1. \end{aligned}$$

  This inequality yields a contradiction, as $\log(n)$ grows to infinity as $n \to \infty$ and therefore cannot be bounded by a constant $\lightning$. □

◇

Notation. Let $\mathcal{F} = \{f : \mathbb{N} \to \mathbb{R}\}$. We say $f \sim g$ if $f = O(g)$ and $g = O(f)$.

Note. This relation between functions $f \sim g$ is reflextive, symmetric, and transitive.

Note that proving the big-O of a function with witnesses is very time-consuming. There are several properties of big-O that we can use to simplify proofs.

Property. Let $f_i, g_i : \mathbb{N} \to \mathbb{R}$

- If $f = O(G)$, then $f + \alpha = O(g)$ for $\alpha \in \mathbb{R}$.

  Note. As long as $g \not\to 0$ as $x \to \infty$.
- If $f_1 = O(g)$, $f_2 = O(g)$, then $f_1 + f_2 = O(g)$
- If $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, then $p(x) = O(x^n)$.
- If $f_1 = O(g_1), f_2 = O(g_2)$, then $f_1 f_2 = O(g_1 g_2)$.
- $1 \leq \log(n) \leq n^\alpha \leq n^\beta \leq n^\beta \log(n) \leq 2^n$ for $\beta > \alpha > 0$

Example. Going back to the restaurants, we have two forming strategies:

1. Compare one restuarant at a time.
2. Pair the restaurants. Keep the best of each pair. Repeat.

Let $T(n)$ = the number of meals needed to find the best restaurant out of a list of length n. Then, for the first strategy, we have:

$$T(n) = T(n-1) + 2.$$

For the second strategy, we have:

$$T(n) = T\left(\frac{n}{2}\right) + n.$$

We can solve the first strategy's recurrence relation with substitution:

$$\begin{aligned} T(n) &= T(n-1) + 2 \\ &= T(n-2) + 2 + 2 \\ &= T(n-3) + 2 + 2 + 2 \\ &(\ldots) \\ &= T(n-(n-1)) + 2(n-1) \\ &= 2(n-1). && (T(1) = 0) \end{aligned}$$

And for the second:

$$\begin{aligned} T(n) &= T\left(\frac{n}{2}\right) + n \\ &= T\left(\frac{n}{4}\right) + \frac{n}{2} + n \\ &= T\left(\frac{n}{8}\right) + \frac{n}{4} + \frac{n}{2} + n \\ &(\ldots) \\ &= n\left(1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{k-1}}\right) \end{aligned}$$

.

◇

Lecture 14: Solving Recurrence Relations

4 Induction

Example. Take from last lecture the following recurrence relation:

$$T(n) = T(n-1) + 2, \quad T(1) = 0.$$

We can "guess" the solution by looking at the relation. We guess $T(n) = 2 \cdot n$. Then, we have:

$$T(n) = 2(n-1) + 2 = 2n - 2 + 2 = 2n, \quad \text{but } T(1) \neq 2.$$

So instead, we guess $T(n) = 2 \cdot (n-1)$, which satisfies our base case. ◇

We use induction to check if a statement $P(n)$ is true for all $n \in \mathbb{N}$. We check that

1. $P(0)$ is true. This is called the base case of induction.
2. Assume $P(k)$ is true for some $k \in \mathbb{N}$. This is called the inductive hypothesis.
3. Prove that $P(k) \Rightarrow P(k+1)$. This is called the step of induction.

Example. We will prove that for all $n \geq 1, n \in \mathbb{N}$,

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Let $P(n) \coloneqq 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. Formally, we wish to prove $\forall n P(n)$, $n \geq 1, n \in \mathbb{N}$. We will proceed with induction on n.

Base case: $n = 1$. Then, we have

$$P(1) \coloneqq 1 = \frac{1(1+1)}{2} = 1.$$

Step: We assume that $P(k)$ is true, where $k \geq 1, k \in \mathbb{N}$. We wish to show that $P(k+1)$ is true. From our inductive hypothesis, we have

$$1 + 2 + \ldots + k = \frac{k(k+1)}{2}.$$

Adding $k+1$ to both sides, we have

$$1+2+\ldots+k+(k+1)=\frac{k(k+1)}{2}+k+1=\frac{(k+1)(k+2)}{2}.$$

The last equality confirms that $P(k+1)$ is true.

It follows by induction that $P(n)$ is true for any $n \geq 1, n \in \mathbb{N}$. ◇

Example. Let $H_n = 1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}$. We wish to prove that $H_{2^n} \geq 1+\frac{n}{2}$ for $n \in \mathbb{N}$.

Base case: $n=0$. Then, we have

$$H_{2^0} = H_1 = 1 \geq 1+\frac{0}{2} = 1$$

Step: Let $P(n) \coloneqq H_{2^n} \geq 1+\frac{n}{2}$. We assume $P(k)$ is true for some $k \in \mathbb{N}$. We will prove that $P(k) \Rightarrow P(k+1)$. From our inductive hypothesis, we have

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{2^k} \geq 1+\frac{k}{2}.$$

We add to both sides $\frac{1}{2^k+1}+\frac{1}{2^k+2}+\ldots+\frac{1}{2^{k+1}}$ such that

$$H_{2^k+1} \geq 1+\frac{k}{2}+\frac{1}{2^k+1}+\frac{1}{2^k+2}+\ldots+\frac{1}{2^{k+1}}.$$

It is enough to show that $\frac{1}{2^k+1}+\frac{1}{2^k+2}+\ldots+\frac{1}{2^{k+1}} \geq \frac{1}{2}$. Then, we have

$$\frac{1}{2^k+1}+\frac{1}{2^k+2}+\ldots+\frac{1}{2^{k+1}} \geq \frac{1}{2^{k+1}}+\frac{1}{2^{k+1}}+\ldots+\frac{1}{2^{k+1}} = 2^k \cdot \frac{1}{2\cdot 2^k} = \frac{1}{2}.$$

Combining these inequalities, we have

$$H_{2^{k+1}} \geq 1+\frac{k}{2}+\frac{1}{2^k+1}+\ldots+\frac{1}{2^{k+1}} \geq 1+\frac{k}{2}+\frac{1}{2} = 1+\frac{k+1}{2}$$

Therefore, $P(k+1)$ is true.

◇

Lecture 15: Induction Continued

Example. Given $\alpha \in \mathbb{R}$, $\alpha > 0$, $\alpha \neq 1$. Show that

$$1+\alpha+\alpha^2+\ldots+\alpha^n = \frac{1-\alpha^{n+1}}{1-\alpha}.$$

◇

Proof. We will proceed with induction on n.

Base case: $n=0$. Then, we have

$$1=\alpha^0=\frac{1-\alpha^{0+1}}{1-\alpha}=\frac{1-\alpha}{1-\alpha}=1.$$

Step: Assume that

$$1 + \alpha + \alpha^2 + \ldots + \alpha^k = \frac{1 - \alpha^{k+1}}{1 - \alpha} \qquad \text{for some } k \geq 0.$$

From the assumption (inductive hypothesis), we have

$$\begin{aligned} 1 + \alpha + \alpha^2 + \ldots + a^{k+1} &= (1 + \alpha + \alpha^2 + \ldots + \alpha^k) + \alpha^{k+1} \\ &= \frac{1 - \alpha^{k+1}}{1 - \alpha} + \alpha^{k+1} \\ &= \frac{1 - \alpha^{k+1} + (1 - \alpha)\alpha^{k+1}}{1 - \alpha} \\ &= \frac{1 - \alpha^{k+1} + \alpha^{k+1} - \alpha^{k+2}}{1 - \alpha} \\ &= \frac{1 - \alpha^{(k+1)+1}}{1 - \alpha}. \end{aligned}$$

which was what we wanted.

□

Example. Show that for every $n \in \mathbb{N}$, $n \geq 1$, 21 divides $4^{n+1} + 5^{2n-1}$. ◇

Proof. We will proceed with induction on n. Let $P(n)$ be the statement that $21 \mid 4^{n+1} + 5^{2n-1}$. We wish to prove that $P(n)$ is true for every $n \in \mathbb{N}$, $n \geq 1$.

Base case: $n = 1$. Then, we have

$$4^1 + 5^{2 \cdot 1 - 1} = 4^2 + 5 = 9 = 21.$$

Step: We assume $P(k)$ is true for $k \geq 1$. We wish to show that $P(k+1)$ is true as well. In other words, we wish to show that 21 divides

$$4^{(k+1)+1} + 5^{2(k+1)-1}.$$

We have:

$$\begin{aligned} 4^{(k+1)+1} + 5^{2(k+1)-1} &= 4 \cdot 4^{k+1} + 5^2 \cdot 5^{2k-1} \\ &= 4 \cdot 4^{k+1} + 25 \cdot 5^{2k-1} \\ &= 4 \cdot 4^{k+1} + (21 + 4) \cdot 5^{2k-1} \\ &= 4 \cdot 4^{k+1} + 21 \cdot 5^{2k-1} + 4 \cdot 5^{2k-1} \\ &= 4 \cdot \left(4^{k+1} + 5^{2k-1}\right) + 21 \cdot 5^{2k-1}. \end{aligned}$$

Then, from our assumption, we have

$$\begin{aligned} 4^{(k+1)+1} + 5^{2(k+1)-1} &= 4 \cdot 21 \cdot q + 21 \cdot 5^{2k-1} \\ &= 21 \cdot (4q + 5^{2k-1}). \end{aligned}$$

By definition, this means that 21 divides $4^{(k+1)+1} + 5^{2(k+1)-1}$, or $P(k+1)$ is true, which was what we wanted.

□

Example. Given a complete set of triominoes, we want to tile an $n \times n$ board.

Observe. The board cannot be tiled if n is not divisible by 3, because n^2 must be divisible by 3 for the board to be tiled.

We want to show that we can tile any $n \times n$ board with top left corner removed if n is a power of 2. ◇

Proof. We will proceed with induction on n.

Base case: $n = 1$. It is clear that we can fit a triomino in the 3 squares of the board.

Step: $n > 1$. We assume it is possible to tile some $2^k \times 2^k$ board with top left corner removed. We wish to show that it is possible to tile the $2^{k+1} \times 2^{k+1}$ board with top left corner removed as well. Here $k \in \mathbb{N}$, $k \geq 1$. By partitioning the board into 4 smaller squares, we can apply our assumption to tile the entire board (see figure below).

□

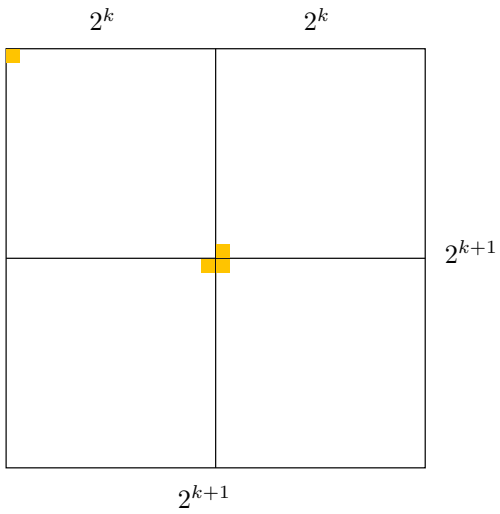

Figure 1: Triomino Tiling

Example. We have a group of N people. One person is a celebrity if everybody knows that person **and** that person knows no one. ◇

Exercise 1

Is $4^n - 1$ a multiple of 3?

Lecture 16: Strong Induction

Continuing the example from last time, we want to see for any group if there exists a celebrity. To do so, we can ask any person A whether or not they know person B. How many questions will we have to ask?

Let $T(n)$ be the minimum number of questions we must ask to determine if there is a celebrity. Note that if A knows B, A cannot be the celebrity. Also note that if A doesn't know B, then B cannot be the celebrity. Then, our recurrence relation is defined by

$$T(n) = 1 + T(n-1).$$

We wish to show that we can find whether if there is a celebrity (or not) in at most $3(n-1)$ questions.

Note. The base case is $T(2) = 2$. This is because if A knows B, you still need to check whether or not B knows A.

Proof. We will proceed with induction.

Base case: $n = 2$. We will ask both people, which is sufficient to determine if there is a celebrity. We have $2 \leq 3 = 3(2-1)$, as desired.

Step case: Assume that for any group of k people, we can determine if there is a celebrity by asking at most $3(k-1)$ questions. We wish to show that we can determine the existence of a celebrity in a group of $k+1$ people in at most $3(k+1-1) = 3k$ questions. Pick two people A and B, and ask if A knows B. Then, there are two cases:

Case 1: A does not know B. Then, we know that B cannot be a celebrity. By the inductive hypothesis applied to the original group without B, we can find whether or not there exists a (candidate) celebrity C in $3(k-1)$ steps. To confirm that C is indeed a celebrity in the group with B, we must check that B knows C, and C does not know B. This yields

$$1 + 3(k-1) + 2 = 3(k+1-1) = 3k.$$

total questions, as desired.

Case 2: A knows B. Left as an exercise to the reader!

As we have verified both the base and step case of induction, it follows that we can determine the existence of a celebrity in a group of n people in at most $3(n-1)$ moves. □

4.1 Strong Induction

Instead of assuming that the previous case is true, we assume that all previous cases are true. In other words, we check that $P(0)$ is true, and we check that $P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k) \Rightarrow P(k+1)$ is true for all $k \in \mathbb{N}$. If both are true, we can then similarly conclude that $P(k)$ is true for all $k \in \mathbb{N}$.

Example. Show that for all natural numbers $n \geq 2$ have a decomposition into prime factors. ⋄

Proof. We will proceed with strong induction on n.

Base case: $n = 2$ is prime, as desired.

Step case: Assume every natural number of up k can be decomposed into prime factors. We wish to show that $k+1$ can be decomposed into prime factors as well.

Case 1: $k+1$ is prime. Then the decomposition is trivial.

Case 2: Otherwise, $k+1$ is composite. Then, there exists $a, b \in \mathbb{N}$ such that $k+1 = ab$, $2 \leq a, b \leq k$. By the inductive hypothesis, a and b can be decomposed into prime factors. Then, $k+1$ can be decomposed into prime factors as well, as desired.

In both cases, $k+1$ can be decomposed into prime factors.

As we have verified both the base and step case of induction, it follows that for all $n \in \mathbb{N}$, $n \geq 2$, n can be decomposed into prime factors. □

Note. For strong induction, we must carefully choose our base case(s), as shown below.

Example. (Making change/coin change) There are 4 pesos bills and 5 pesos bills in an unknown country. What is the minimum value ζ such that one can make change for all $n \geq \zeta$? ◇

Proof. We wish to show that $\zeta = 12$. We will proceed with strong induction on n.

Base case: $n = 12 = 4+4+4$, $n = 13 = 4+4+5$, $n = 14 = 4+5+5$, $n = 15 = 5+5+5$.

Step case: Assume one can make change for all values $[12, k]$ for some natural number k. We wish to show that we can make change for $k+1$. To make change for $k+1$, we can use the change for $k-3$ and add one 4 peso bill.

□

4.2 Induction and Recursion

Example. Let $\{a_n\}_{n \in \mathbb{N}}$ be a sequence of numbers such that $a_0 = 1, a_1 = 3, a_2 = 9, a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for all $n \geq 3$. Prove that $a_n \leq 3^n$. ◇

Proof. We will proceed with strong induction on n.

Base case: For $n = 0$, we have $a_0 = 1 = 3^0$, as desired. For $n = 1$, we have $a_1 = 3 = 3^1$, as desired. And for $n = 2, a_2 = 9 = 3^2$, as desired.

Step case: Assume $a_k \leq 3^k$ for all values up to $k \in \mathbb{N}$. We wish to show that $a_{k+1} \leq 3^{k+1}$. We know that

$$\begin{aligned} a_{k+1} &= a_k + a_{k-1} + a_{k-2} \\ &\leq 3^k + 3^{k-1} + 3^{k-2} && \text{(Follows from inductive hypothesis)} \\ &< 3^k + 3^k + 3^k \\ &= 3^{k+1}. \end{aligned}$$

as desired.

We have verified the base and step of induction. It follows that $a_n \leq 3^n$ for all $n \in \mathbb{N}$. □

Lecture 17: Last of Induction

Example. The Fibonacci Sequence is defined as follows:

$$f_0 = f_1 = 1$$
$$f_n = f_{n-1} + f_{n-2} \qquad \forall n \geq 2.$$

We can do two things to compute the value of f_n. If $n = 0, 1$, then it will output 1. Otherwise, we return $f_{n-1} + f_{n-2}$. Note that we can also accomplish the following (more efficiently) with memoization.

Then, let $T(n)$ be the number of operations to get f_n. Note that $T(n) \geq c + T(n-1) + T(n-2)$, which implies that the number of steps to calculate the n-th Fibonacci number is greater than the n-th Fibonacci number!

Show that $f_n \geq \alpha^{n-2}$, where $\alpha = \frac{1+\sqrt{5}}{2}$. ◇

Proof. Let us proceed by induction. Note that for $n = 0$, we have $f_0 = 1 > \alpha^{0-1}$ and for $n = 1$, $f = 1 > \alpha^{1-2}$. Then, it suffices to verify the step case. Assume $f_k \geq \alpha^{k-2}$ for some $k \in \mathbb{N} \geq 0$. Then, we have:

$$\begin{aligned}
f_{k+1} &= f_k + f_{k-1} && \text{(Given)} \\
&\geq \alpha^{k-2} + \alpha^{(k-1)-2} && \text{(By I.H.)} \\
&= \alpha^{k-2} + \alpha^{k-3} \\
&= \alpha^{k-3}(\alpha + 1) \\
&= \alpha^{k-3}(\alpha^2) && (\alpha^2 = \alpha + 1) \\
&= \alpha^{k-1} \\
&= \alpha^{(k+1)-2}.
\end{aligned}$$

as desired. Therefore, $f_n \geq \alpha^{n-2}$ for all $n \in \mathbb{N}$. □

Example. Consider the following matrix $M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Note that $M \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x \end{pmatrix}$.

Show that for $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$:

$$M^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}.$$

◇

Proof. We have for $n = 1$, $M^1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, and for $n = 2$, $M^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$. Assume that for some k,

$$M^k = \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix}.$$

Then, we have

$$\begin{aligned} M^{k+1} = M^k \cdot M &= \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} f_{k+1} + f_k & f_{k+1} \\ f_k + f_{k-1} & f_k \end{pmatrix} \\ &= \begin{pmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{pmatrix}. \end{aligned}$$

as desired. □

Remark. Check $f_{n-1} \cdot f_{n+1} = f_n^2 + (-1)^n$

This is because

$$\begin{aligned} f_{n-1} \cdot f_{n+1} - f_n^2 &= \det \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \\ &= \det \left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \right) \\ &= \det \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \\ &= (-1)^n. \end{aligned}$$

Example. Count the number of bit-sequences of length n such that there are no two consecutive 1s. ◇

Let a_n be the number of bit-sequences. Note that if we place a 0, we can fill the rest with a_{n-1} sequences. Note that if we place a 1, then the next bit must be a 0, such that we can place the rest with a_{n-2}. In other words, the number of bit-sequences is given by

$$a_n = a_{n-1} + a_{n-2}.$$

Note that we have 2 bit-sequences of length 1 and 3 bit-sequences of length 2. We quickly realize that a_n is the $n+2$-nd Fibonacci number.

Example. Let s_n be the number of bit-sequences such that there are no two 1s at distance 2. ◇

We have $s_3 = 6$. Note that if we place a 0, we can fill the rest with s_{n-1} sequences. Note that if we place a 1, then we can place two 0s such that we can fill the rest with s_{n-3} sequences. Or, we can place two 1s and then two 0s such that we can fill the rest with s_{n-4} sequences. In other words, our recurrence relation is

$$s_n = s_{n-1} + s_{n-3} + s_{n-4}.$$

Note. If we define the empty string to be a bit-sequence, then $s_0 = 1$. This is ok as long as we don't use the empty string in our operation.

Lecture 18: Modular Arithmetic

5 Modular Arithmetic

Consider the relation $\equiv_m$ defined by the following:

$$a \equiv_m b \Leftrightarrow (a - b) \text{ is a multiple of } m.$$

Note. This is an equivalence relation because it is reflexive, symmetric, and transitive.

We can establish this relation because we know the following theorem (that defines a remainder):

Theorem 3. Let $b, m \in \mathbb{Z}, m > 0$. There exists a unique pair of integers q, r such that $b = qm + r$ and $0 \leq r < m$.

Example. $13 = 2(5) + 3$, such that $q = 2, r = 3$, so $13 \equiv_5 3$. ◇

Definition 14. $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ is the set of remainders when m is divided by a number.

Example. Let $m = 4$. $\mathbb{Z}_4 = \begin{Bmatrix} \overline{0} & = & \{0, \pm 4, \pm 8, \pm 12, \ldots\} \\ \overline{1} & = & \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\ \overline{2} & = & \{\pm 2, \pm 6, \pm 10, \ldots\} \\ \overline{3} & = & \{\ldots, -5, -1, 3, 7, 11, \ldots\} \end{Bmatrix}$ ◇

Notation. We write $b \pmod m$ to denote the remainder of b when divided by m.

Notation. We write $a \equiv b \pmod m$ to denote that $a \equiv_m b$.

5.1 Operations in $\mathbb{Z}_m$

How do we perform operations?

Definition 15. We define **addition** to be $\overline{a} + \overline{b} \coloneqq \overline{a + b}$.

Example. $\overline{10} + \overline{8} = \overline{10 + 8} = \overline{18} = \overline{2}$ when $m = 4$. ◇

Definition 16. We define **multiplication** to be $\overline{a} \cdot \overline{b} = \overline{ab}$.

Example. $\overline{2} + \overline{13} = \overline{5} \pmod{10}$ when $m = 10$. ◇

Note. Integers are not closed under division, so we must be careful.

As we can see, the zero property and identity property in modular multiplication does not hold. Just like in linear algebra, we must define the inverse of a number in order to perform division.

Definition 17. Let $m > 1$. We say $a \in \mathbb{Z}$ is a **divisor of of zero** if $\exists b \in \mathbb{Z}$, $b \not\equiv 0 \pmod{m}$ such that $a \cdot b \equiv 0 \pmod{m}$. In other words, $\exists \overline{b} \in \mathbb{Z}_m, \overline{b} \neq \overline{0} \wedge \overline{a} \neq \overline{0} \wedge \overline{a}\overline{b} = \overline{0}$

Definition 18. Let $a \in \mathbb{Z}$. We say a is **invertible** if $\exists b \in \mathbb{Z}$ such that $a \cdot b \equiv 1 \pmod{m}$.

Note. These two properties are mutually exclusive.

Definition 19. Let $a, b \in \mathbb{Z}$. We define their greatest common divisor (gcd) of a and b as

$$\gcd(a, b) = \max\{d \in \mathbb{Z} : d|a \wedge d|b\}.$$

Proposition 1. Let $a > b > 0$ be integers. Then, it holds that

$$\gcd(a, b) = \gcd(a - b, b).$$

Proof. Let $d = \gcd(a, b)$, $\hat{d} = \gcd(a, a - b)$. Note that if $x|y$ and $x|z$, then $x|\alpha y + \beta z$ for $x, y, z, \alpha, \beta \in \mathbb{Z}$. Then, we know that

$$d|a \wedge d|b \text{ by definition of } \gcd(a, b).$$

Set $\alpha = 1, \beta = -1$ to get $d|a - b$ fron our note. Then, d is a common divisor of both a and $a - b$. However, $\hat{d} \geq d$ because $\hat{d} = \gcd(a, a - b)$ ($\hat{d}$ is the *greatest* common divisor). We also know that

$$\hat{d}|a \wedge \hat{d}|a - b \text{ by definition of } \gcd(a, a - b).$$

Set $\alpha = 1, \beta = -1$. then, we have

$$\hat{d}|\alpha a + \beta(a - b) = a + (b - a) = b.$$

Now, we know that $\hat{d}$ is a common divisor of both a and b. Then, $d \geq \hat{d}$ because $d = \gcd(a, b)$. Because $\geq$ is antisymmetric, we conclude that $d = \hat{d}$. □

Algorithm 1: Euclidean Algorithm

Input: $a \geq b \geq 0$
Output: $\gcd(a, b)$

```
if b = 0 then
    return a;
end
return gcd(b, a mod b);
```

Lemma. Let $d = \gcd(a, m) > 1$. Then a is a divisor of zero $\pmod{m}$.

Proof. Let $b = \frac{m}{d}$. Then, $a \cdot b = a \cdot \frac{m}{d} = \frac{a}{d} \cdot m \equiv 0 \pmod{m}$. The last equality follows from the fact that $d|a$. □

Example. Let $a = 2$, $m = 10$. Then, $b = \frac{10}{2} = 5$, and $2 \cdot 5 \equiv 0 \pmod{10}$. ◇

Theorem 4. Let $a \geq b$, $a, b \in \mathbb{N}$. Then,

$$\gcd(a, b) = \min\{d > 0 : \exists \alpha, \beta \ d = \alpha a + \beta b\}.$$

We will prove this next lecture!

Lemma. Let $1 = \gcd(a, m)$. Then, $\exists! b \in \mathbb{Z}_m$ such that $\overline{a} \cdot \overline{b} = \overline{1}$. In other words, a is invertible $(\text{mod } m)$.

Proof. From the theorem, we have $\exists \alpha, \beta : 1 = \alpha a + \beta m$. If we take this expression $(\text{mod } m)$, we have $\overline{1} = \overline{\alpha} \cdot \overline{a} + \overline{\beta} \cdot \cancelto{0}{\overline{m}}$. So, α is the inverse of $a \pmod{m}$ □

Note. From these two lemmas, we can classify every integer a as invertible, or a divisor of 0.

Lecture 19: Modular Arithmetic Continued

How do we solve $\overline{ax} = \overline{b}$ in $\mathbb{Z}_m$?

It suffices to solve the cases where $\overline{b} = \overline{0}$ and $\overline{b} = \overline{1}$. We first check $\gcd(a, m) = d$.

Example. Find $\gcd(30, 12)$. ◇

By the Euclidean algorithm, we have

$$\begin{aligned} &\gcd(30, 18) && (30 = 18 \cdot 1 + 12) \\ &= \gcd(18, 12) && (18 = 12 \cdot 1 + 6) \\ &= \gcd(12, 6) && (12 = 6 \cdot 2 + 0) \\ &= \gcd(6, 0) = 6. \end{aligned}$$

Then, let us go back to the spot where we have a remainder of 6. Then, we get a linear combination

$$6 = 18 \cdot 1 + 12 \cdot (-1).$$

We also get from one step above that:

$$6 = 18 \cdot 1 + (30 \cdot 1 + 18 \cdot -2) \cdot (-1) = 30 \cdot (-1) + 18 \cdot 3.$$

In other words, we have now found a method for finding the coefficients of the linear combination that represents the gcd in terms of the two numbers we started with.

Definition 20. Let $d = \gcd(a, b)$. Then, there exists numbers $s, t \in \mathbb{Z}$ such that $d = as + bt$. These are known as **Bezout coefficients**.

We can use the Extended Euclidean Algorithm to find one such coefficient.

Remark. If $d = 1$, then s is the inverse of $a \pmod{b}$.

Algorithm 2: Extended Euclidean Algorithm

Input: $(a, b), a \geq b$
Output: (d, s, t) such that $d = \gcd(a, b)$, $d = as + bt$

$r_0 = a$;
$r_1 = b$;
$s_0 = 1$;
$s_1 = 0$;
$t_0 = 0$;
$t_1 = 1$;
while $r_k \neq 0$ **do**
  $r_{k+1} = r_{k-1} \pmod{r_k}$;
  $s_{k+1} = s_{k-1} - (r_{k-1} \text{ div } r_k) \cdot s_k$;
  $t_{k+1} = t_{k-1} - (r_{k-1} \text{ div } r_k) \cdot t_k$;
end
return $(r_{k-1}, s_{k-1}, t_{k-1})$;

We can also solve systems of linear equations in $\mathbb{Z}_m$. Let's say we wish to find a number such that we can satisfy

$$\begin{pmatrix} x & \equiv a_1 & (\text{mod } m_1) \\ x & \equiv a_2 & (\text{mod } m_2) \\ & & \dots \\ x & \equiv a_k & (\text{mod } m_k) \end{pmatrix}.$$

Theorem 5. (Chinese Remainder Theorem) Let $m_1, m_2, \dots m_k \in \mathbb{N}$ be numbers such that $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$. Then, the system has a unique solution in $\mathbb{Z}_M$ where $M = m_1 m_2 \dots m_k$.

Proof. First, we will prove the solution's existence. Set $M_i = \frac{M}{m_i}$. Because all m's don't share a factor, $\gcd(m_i, M_i) = 1$. Let y_i be the inverse of $M_i \pmod{m_i}$. Consider:

$$x = M_1 \cdot y_1 \cdot a_1 + M_2 \cdot y_2 \cdot a_2 + \ldots + M_k \cdot y_k \cdot a_k.$$

Then, we check:

$$\begin{aligned} x &\equiv M_1 \cdot y_1 \cdot a_1 + \cancelto{0}{M_2 \cdot y_2 \cdot a_2} + \ldots + \cancelto{0}{M_k \cdot y_k \cdot a_k} \pmod{m_1} \\ &\equiv \cancelto{1}{M_1 \cdot y_1} \cdot a_1 \equiv a_1 \pmod{m_1}. \end{aligned}$$

We can reprove this for each $2 \leq i \leq k$. □

Example. Solve

$$\begin{matrix} x & \equiv 3 & (\text{mod } 5) \\ x & \equiv 2 & (\text{mod } 7) \end{matrix}.$$

◇

We first check that $\gcd(5,7) = 1$, which it is. Then, we continue as follows:

$$\begin{aligned} M &= 5 \cdot 7 = 35 \\ M_1 &= \frac{35}{5} = 7 \\ M_2 &= \frac{35}{7} = 5 \\ y_1 &= 3 && \text{(Inverse of 7 mod 5)} \\ y_2 &= 3 && \text{(Inverse of 5 mod 7)} \\ &. \end{aligned}$$

Therefore, the solution is as follows:

$$\begin{aligned} x &= M_1 \cdot y_1 \cdot a_1 + M_2 \cdot y_2 \cdot a_2 \\ &= 7 \cdot 3 \cdot 3 + 5 \cdot 3 \cdot 2 = 93 \\ &\equiv 23 \pmod{35}. \end{aligned}$$

Note. This solution ($x \equiv 93 \pmod{35}$) is the only solution, which we will prove in our homework.

Lecture 20: What the Modular Arithmetic

Fix $m \in \mathbb{N}$, $m > 1$.

Let $a \in \mathbb{N}$. Then,

$$\{a^n\}_{n \geq 0} \text{ in } \mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Note that we can easily calculate a^k with

$$a^k \pmod m = \left(a^{k-1} \pmod m\right)(a \pmod m) \pmod m.$$

as well as finding repetition. What do we mean by this?

Example. Let $m = 6$, and $a = 11$. Then, a^n has periodicity 2 when taken mod m. ◇

Example. What is $4^{2023} \pmod 7$? Note that $2023 \equiv 1 \pmod 3$ (from the periodicity), so $4^{2023} \equiv 4^1 \equiv 4 \pmod 7$. ◇

Theorem 6. Let $a \in \mathbb{N}$. a is divisible by 3 if and only if the sum of its digits is divisible by 3.

Proof. All of $\{10^n\}_{n \geq 0}$ in $\mathbb{Z}_3$ are in the class of $\overline{1}$! Therefore, $10^k \equiv 1 \pmod 3$. Then, a can be written as

$$a = (a_k a_{k-1} a_{k-2} \ldots a_1 a_0)_{10} \qquad a_i \in \{0, 1, 2, \ldots 9\}.$$

Then, we know that

$$\begin{aligned} a &= 10^k a_k + \ldots + 10^2 a_2 + 10 a_1 + a_0 \\ &\equiv \overbrace{\overline{10^k}}^{1} \cdot \overline{a_k} + \ldots + \overbrace{\overline{10^2}}^{1} \cdot \overline{a_2} + \overbrace{\overline{10}}^{1} \cdot \overline{a_1} + a_0 \pmod 3 \\ &= a_k + \ldots + a_1 + a_0 \pmod 3. \end{aligned}$$

□

Theorem 7. Let $a \in \mathbb{N}$. a is divisible by 4 if and only if the last two digits of a are divisible by 4.

Proof. We know that $\{10^n\}_{n\geq 0}$ in $\mathbb{Z}_4$ are $\overline{1}$ for $n = 0$, $\overline{2}$ for $n = 1$, and $\overline{0}$ for $n \geq 2$. Therefore, we only look at $n = 0$ and $n = 1$ (tens and ones place). □

Lemma. If $1 \leq i < j \leq p-1$. Then, $ai \not\equiv aj \pmod{p}$.

Proof. $ai - aj = a(i-j) \not\equiv 0 \pmod{p}$. □

Theorem 8. (Fermat) Let p be prime. Let $a \in \mathbb{N}$ such that $\gcd(a, p) = 1$. Then, $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Fix p, prime number. Then we know for a^n in $\mathbb{Z}_p$, $a \in \mathbb{N}$, $\gcd(a, p) = 1$. Therefore, all of

$$1, a, a^2, a^3, \ldots, a^n.$$

are invertible. Then all of

$$\overline{1}, \overline{2}, \overline{3}, \overline{p-1}.$$

and

$$\overline{1a}, \overline{2a}, \overline{3a}, \overline{(p-1)a}.$$

are invertible. Note that the previous two sets are the same sets. Then, we have

$$\begin{aligned} \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \ldots \cdot \overline{(p-1)} &\equiv \overline{1a} \cdot \overline{2a} \cdot \overline{3a} \cdot \overline{(p-1)a} \pmod{p} \\ (p-1)! &\equiv (p-1)! \cdot a^{p-1} \pmod{p} \\ 1 &\equiv a^{p-1} \pmod{p}. \end{aligned}$$

□

Example. What is $4^{2023} \pmod{7}$? ◇

Note that 7 is prime, and therefore $4^6 \equiv 1 \pmod{7}$. Then, $4^{2023} \equiv 4^{2023 \pmod 6} \equiv 4 \pmod{7}$.

Example. What is $4^{2023} \pmod{131}$? ◇

Note that $2023 \pmod{130} = 73$. Then, by Fermat's theorem, $4^{2023} \equiv 4^{73} \pmod{131}$.

Going even deeper, What about counting the number of invertible elements?

$$|\{1 \leq x \leq m \colon \gcd(x, m) = 1\}| = \varphi(m).$$

is the number of invertible elements in $\mathbb{Z}_m$. Then, $\varphi(p) = p - 1$. Note that $\varphi(p^2) = p(p-1)$.

Theorem 9. $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ as long as $\gcd(a, b) = 1$.

Theorem 10. (Euler) Let $m \in \mathbb{N}$. Let $p_1, p_2, \ldots, p_k$ be the distinct prime factors of m. Then,

$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$

Theorem 11. (Euler) Let $m \in \mathbb{N}$, $m > 1$. Let $a \in \mathbb{N}$ such that $\gcd(a, m) = 1$. Then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

5.2 Cryptography

From Euler's theorem, we have $a^{\varphi(m)+1} \equiv a \pmod{m}$.

We label our alphabet such that $A \to 00$, $B \to 01$, $Z \to 25$, etc. Then, you can write every message as a sequence of digits. Let this message be m. We release to the world public key (N, e).

The encryption key is $m^e \pmod{N}$. Then, the decryption key is then $m^{t\cdot\varphi(N)+1} \equiv m \pmod{N}$. the decryption strategy is that if we find $d \in \mathbb{N}$ such that $ed \equiv 1 \pmod{\varphi(n)}$, then we have

$$(m^e)^d = m^{e\cdot d} = m^{t\cdot\varphi(n)+1} \equiv m \pmod{n}.$$

such that we can then decrypt the message.

Note. For the public key, we need $\gcd(\varphi(N), e) = 1$.

Remark. We usually set $N = p \cdot q$, both prime. Then, $\varphi(N) = (p-1)(q-1)$. This is better than N prime because our enemies need to factorize N to find our p and q. By the time they read our message, it is already too late.

Note. If a message is longer than N, we need to break it into pieces because when don't want some number congruent to the message, but the message itself.

Lecture 21: Counting

6 Counting

We can use the product rule for counting (when counting happens sequentially).

Example. Let a license plate be defined by 3 letters followed by 3 digits. How many possible license plates are there? ◇

We can choose 26 for the first letter, 26 for the second, and 26 for the third. Then, we can choose 10 for the first digit, 10 for the next, and 10 for the last. Therefore, our answer is

$$26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = (260)^3.$$

Example. Let $|A| = n$, $|B| = m$. How many functions are there such that $f : A \to B$? ◇

Every element in A can be mapped to an element in B, such that there are m choices for all n elements. Then, the total number of functions is m^n.

Example. Let $|A| = n$, $|B| = m$. How many functions $f : A \to B$ are there such that f is onto? $\diamond$

Note that a_1 must be mapped to an element in B. There are m choices to do so. Then, a_2 must be mapped to an element in B, not equal to $f(a_1)$. There are $m-1$ choices to do so. Then, a_3 must be mapped to an element in B, not equal to $f(a_1)$ and $f(a_2)$. There are $m-2$ choices to do so. It follows that the total number of functions is

$$\begin{cases} m(m-1)(m-2)\cdots(m-n+1) = (m)_n & m \geq n \\ 0 & m < n \end{cases}.$$

Notation. $(m)_n = \frac{m!}{(m-n)!} = m(m-1)(m-2)\dots(m-n+1)$

We can use the sum rule to add together cases in counting:

Example. Count the number of passwords consisting of letters and digits, with length 8-10. $\diamond$

We can count passwords of length 8, 9, and 10 separately.

$$36^8 + 36^9 + 36^{10}.$$

We can also use the subtraction rule! We can count the number of things that do not satisfy our condition, then subtract that number from the total number of things.

Example. Count the number of passwords with at least one digit. $\diamond$

Note that if we naively fix the position of the digit, make it a digit, and fill the rest of the letters (with 36 options), then we will be over-counting passwords!

Instead, we count the total number of passwords with no constraints, and subtract the number of passwords with no digits, yielding solution

$$36^8 + 36^9 + 36^{10} - (26^8 + 26^9 + 26^{10}).$$

Notation. We will define factorial (!) as

$$n! \coloneqq \begin{cases} 1 & n = 0 \\ n(n-1)! & n > 0 \end{cases}.$$

There is also a division rule, where we count every element exactly N times.

Definition 21. Permutations count the number of something where order matters! It is written as

$$P(n,k) = \frac{n!}{(n-k)!} = \#\text{ of ordered } k\text{-tuples from } n \text{ elements.}$$

We derive this formula from the division rule: if we have a permutation of length n of n elements, we are counting the number of permutations of length k of n elements $n-k$ times!

Definition 22. Combinations count the number of something where order *order doesn't matter*. It is written as

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

Note that permutations also counts this, but there are $k!$ ways to order a combination. Therefore, we divide the number of permutations by $k!$ to yield this amount.

We can also use recursion for counting sets. Let $1, 2, 3, \ldots, n$ be the elements we can choose from. We can add k to the number of sets of size $n-1$ without k, of which there are $\binom{n-1}{k-1}$ of them. We can add k to the number of sets of size $n-1$ with k, of which there are $\binom{n-1}{k}$ of them. Therefore, we have Pascal's identity:

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

Lecture 22: Counting Continued

Example. How many strings of 10 bits are there such that there are exactly 4 1's? ◇

We can choose 4 places of 10 to place 1's, and the rest are 0's. So the answer is $\binom{10}{4}$.

Example. How many strings of 10 bits are there such that there are at most 4 1's? ◇

We can use the sum rule!

$$\binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3} + \binom{10}{4} = 386.$$

Example. Show that if $|S| = n$, then $|\mathcal{P}(S)| = 2^n$. ◇

A subset can be formed by choosing whether or not to include every element. Therefore, the number of subsets, the cardinality of the powerset, is $2^{|S|} = 2^n$.

Theorem 12.

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Proof. For each term $(a+b)(a+b)\ldots(a+b)$, we can choose to either multiply the a or the b. If there are k number of a's, then there are $n-k$ number of b's. Therefore, the number of terms with k number of a's is $\binom{n}{k}$. Therefore, the coefficient of $a^k b^{n-k}$ is $\binom{n}{k}$. Summing over all k gives the result. □

Exercise 1

Prove the binomial theorem with induction!

Lecture 23: Pigeonhole Principle

Going back to functions and countability,

Proposition 2. Let's say we have a function $f : A \to B$ and $|A| > |B|$. Then, f cannot be one-to-one.

6.1 Pigeonhole Principle

The following is called a priciple because it is so obvious that it is not worth proving.

Theorem 13. (Pigeonhole Principle) If $k+1$ pigeons nest on k pigeonholes, then at least one pigeonhole must have more than one pigeon.

Example. There are 56 students in this class. Prove that at least two of them will have birthdays on the same month of the year. ◇

Let the students be the pigeons, and the months of the year be the pigeonholes. We have $56 > 13 > 12$, such that by the pigeonhole principle, at least two students with share the same birthday month.

Theorem 14. (Generalized Pigeonhole Principle) If N pigeons nest on k pigeonholes, then at least one pigeonhole must have at least $\lceil \frac{N}{k} \rceil$ pigeons.

Example. In some CS2051 class, final letter grades are from the set $\{A, B, C, D, F\}$. What's the minimum number of students to guarantee:

- 10 students will get the same grade? We need N such that $\lceil \frac{N}{k} \rceil \geq 10$ for $k = 5 = |\{A, B, C, D, F\}|$. The minimum such $N = (\text{Ans} - 1) \cdot k + 1 = 46$.
- 3 students will get an A? There is no minimum number of students that will guarantee this.

This example will be on the HW! ◇

Example. Show that every natural number $n > 0$ has a multiple whose decimal expansion is made of 1's and 0's only. ◇

Note that for any n, we will have n possible remainders. These possible remainders will be the pigeonholes. Consider the infinite set of numbers $\{1, 11, 111, 1111, \ldots\}$. By the pigeonhole principle, there are two numbers in this set $a > b$, such that $a \equiv b \pmod{n}$ (they are in the same pigeonhole). If $a = 111\ldots1$ and $b = 11\ldots1$. Then, $a - b = 111\ldots10\ldots000$ is a multiple of n.

Example. You choose $n+1$ numbers from the set $\{1, 2, 3, \ldots 2n\}$. Show that there is a pair of numbers $a < b$ such that $a|b$. ◇

Consider the odd part of a number k. If $1 \leq k \leq 2n<$ then its odd part is in the set $\{1, 3, 5, 7, \ldots 2n-1\}$, which has cardinality n! By the pigeonhole principle, at least two numbers

a, b have the same odd part. Write

$$a = 2^\alpha \cdot p \qquad b = 2^\beta \cdot p.$$

Because $a < b$, $\alpha < \beta$ such that $a|b$.

Example. Five points are placed inside a equare of side 2. Show that there are two points at a distance at most $\sqrt{2}$. ◇

We can break the square into 4 squares of side 1, which means two points must go inside one box. Therefore, these two points are at most $\sqrt{2}$ away from each other.

Example. Color the plane using three colors. Show that there are two points of the same color separated by an integer distance. ◇

Consider a rectangle on the plane with side lengths 3 and 4. Then, it's diagonal is of length 5. Because there are 3 colors, 2 of 4 of the corners must be colored the same color. Then, the distance between these 2 colors is an integer distance.

Exercise 1

Show that for all $n \in \mathbb{N} > 0$, there exists a power of 2 such that the first digits are those of n.

Lecture 24

6.2 With Repetition

Example. Let n be the number of objects, and $t_1, t_2, \ldots, t_k$ denote the k types. We want to find a permutation of these objects such that $t_1 + t_2 + \ldots + t_k = n$. How should we do this? ◇

We can use the division rule, dividing out every permutation between identical objects. There are t_i ways to permute objects of type i. Therefore, our answer is

$$\frac{n!}{t_1!t_2!\ldots t_k!}.$$

Example. What if we don't want to find a permutation of these objects, but instead a combination? ◇

We visualize this combination as a permutation of stars and bars. There are total of $n + k - 1$ stars and bars, of which n are stars and $k - 1$ are bars. Therefore, our answer is then

$$\frac{(n+k-1)!}{n!(k-1)!} = \binom{n+k-1}{k-1}.$$