CSCI 150 Recitations

Saad Mneimneh

Recitation 1

- Cover concept of factorial
    - First, through examples
    - Then in general, showing notation like $n! = 1 \times 2 \times \ldots \times n$
    - Describe why $n! = n \times (n-1)!$
    - Explain simplification in fractions
        - $\frac{10!}{7!} = 10 \times 9 \times 8$
        - $\frac{(n+1)!}{n!} = n + 1$
        - $\frac{n!}{(n-k)!} = \underbrace{n \times (n-1) \times \ldots \times (n-k+1)}_{\text{explain why this is } k \text{ terms}}$
- Explain that integer intervals $[a, b]$ (where $b \geq a$) contain integers $a, a+1, a+2, \ldots, b$
    - Why does it have $b - a + 1$ terms (elements)?
    - Apply to above example: $n - (n-k+1) + 1 = k$
    - What if $b = a - 1$?
- Cover the sum

$$S = 1 + 2 + \ldots + n$$

    - Show it is equal to $n(n+1)/2$. For instance,

$$\begin{array}{ccccc} & 1 & 2 & \ldots & \text{n} \\ + & \text{n} & \text{(n-1)} & \ldots & 1 \\ \hline & \text{(n+1)} & \text{(n+1)} & \ldots & \text{(n+1)} \end{array}$$

      We have $2S = n(n+1)$ ($n+1$ appears n times)

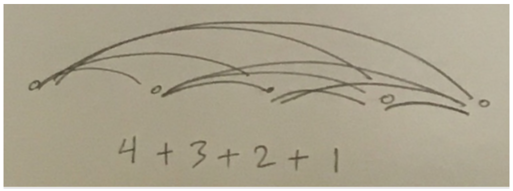
    - Explain why

$$1 + 2 + \ldots + n = n(n+1)/2$$

$$1 + 2 + \ldots + (n-1) = n(n-1)/2$$

      is "the same" formula.

    - Explain how $1+2+\ldots+(n-1) = n(n-1)/2$ counts pairs by showing the diagram below (for $n = 5$):



Recitation 2

Practice sequences, intervals, and sums.

- Sum of the first n positive odd numbers:

$$S = \sum_{i=1}^{n}(2i-1) = 1 + 3 + \ldots + (2n-1)$$

  - By splitting the sum:

$$\sum_{i=1}^{n} 2i - \sum_{i=1}^{n} 1 = 2 \underbrace{\sum_{i=1}^{n} i}_{n(n+1)/2} - n = n^2$$

  - By transformation: Dividing each term by 2 and adding 1/2 to it, we get $S/2 + n/2 = 1 + 2 + \ldots + n = n(n+1)/2$, so $S = n^2$.

- Find the 168^{th} term in

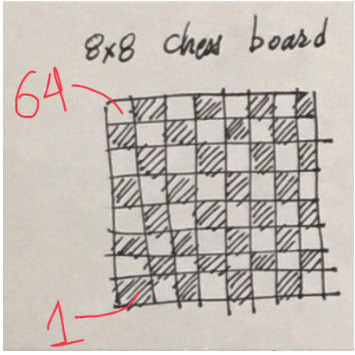
$$68, 79, 90, \ldots, 2257$$

  - Make 167 steps from 68 multiplied by the step size (the step size is 11): $68 + 167 \times 11 = 1905$.
  - Represent the i^{th} number as $68 + (i-1) \times 11$, then set $i = 168$.

- A triangle is made out of 100 starts, then 97 starts, then 94 starts, ... Write an expression for the total number of stars and evaluate it.
  - First, observe that the step size is 3, so we have $\sum_{i=0}^{?}(1+3i)$.
  - Then figure out the bound by looking at the largest number, which is 100: $1 + 3i = 100$ means $i = 33$. So we have $\sum_{i=1}^{33}(1+3i)$
  - Finally, evaluate as above by splitting the sum.

Do some counting exercises based on the snake and ladder problem.

- In how many ways can we place one snake on a chessboard if the head must be on black?



- Use the addition rule, where the categories are given by where the head is. Count how many tails are possible in each scenario. We get

$$62 + 60 + 58 + \ldots + 2 + 0$$

- Write using sum expression $\sum_{i=0}^{30}(2+2i)$
- Evaluate: $\sum_{i=0}^{30}(2+2i) = 2\sum_{i=0}^{30}(1+i) = 2\sum_{i=1}^{31} i = 2 \times \frac{31\times 32}{2} = 31 \times 32$.
- Explain why the product rule is tricky to apply: once a square is chosen, the next choice is dependent on the previous one. For instance, if we choose a black square for the head, then the number of ways we could choose another square depends on where that head is. If we simply say choose a black square (in 32 ways), then choose any square (63 ways), we do not guarantee that the higher number square is black.

Recitation 3

Go over arithmetic and geometric series:

- Arithmetic:

$$\sum_{i=a}^{b}(xi+y) = \sum_{i=a}^{b} xi + \sum_{i=a}^{b} y = x\sum_{i=a}^{b} i + (b-a+1)y$$

$$= x(b-a+1)\frac{a+b}{2} + (b-a+1)y = (b-a+1)\left(\frac{a+b}{2}x + y\right)$$

- Geometric:

$$\sum_{i=0}^{n} ba^i = b+ba+ba^2+\ldots+ba^n = b(1+a+a^2+\ldots+a^n) = b\frac{a^{n+1}-1}{a-1} \quad (a \neq 1)$$

Review addition and product rules:

- Addition: Given k disjoint sets $S_1, S_2, \ldots, S_k$, $|S_1 \cup S_2 \cup \ldots \cup S_k| = |S_1| + |S_2| + \ldots + |S_k|$
- Product: If a task can be done in k phases and each phase i can be carried out in α_i ways (regardless of previous phases), then the entire task can be carried out in $\prod_{i=1}^{k} \alpha_i$ ways.

Practice product rule:

- The number of permutations on n objects
  - 1. choose an object ... n ways
  - 2. choose another objects ... $n - 1$ ways
  - ...
  - n. choose another objects ... 1 way

  By the product rule, we have $n(n-1)(n-2)\ldots 1 = n!$ ways. There is no overcounting because every outcome is a different permutation.

- Given m boys and n girls, in how many ways can we choose a couple?
  - 1. choose a boy ... m ways
  - 2. choose a girl ... n ways

  By the product rule, this is mn ways. There is no overcounting because every outcome is generated exactly once. For instance, assume (Bob, Alice) is one such outcome. The only way to generate it is by choosing Bob first, and choosing Alice next. There is no way we could choose Alice then Bob because the procedure above does not allow it.

- Given the same set of boys and girls, in how many ways can we choose 3 people, not all the same gender. Think of two possible categories: (1 boy, 2 girls) or (1 girl, 2 boys). For instance, let's focus on the first category:
  - 1. choose a boy ... m ways
  - 2. choose a girl ... n ways
  - 3. choose another girl ... $(n - 1)$ ways

  By the product rule, we have $mn(n-1)$. However, there is overcounting. For instance, consider the outcome (Bob, Alice, Cindy). There is another outcome, namely (Bob, Cindy, Alice), which to us would be the same. Therefore, there is overcounting by 2. So the answer must be $mn(n-1)/2$. (Can you think of another procedure that would immediately produce the $n(n-1)/2$ without overcounting?) By analogy, the second category will give us $nm(m-1)/2$. The final answer is, therefore, $mn(n-1)/2 + nm(m-1)/2 = mn(m+n-2)/2$ by the addition rule (make sure you see clearly that the two categories of outcomes are disjoint).

- Encourage the students to verify algebraically:

$$\binom{m}{2} + \binom{n}{2} + mn = \binom{m+n}{2}$$

- Encourage the students to work on the exercise mentioned at the end of Lecture 4 about placing one ladder and one snake. The idea is to use the product rule, and to recognize that one must start with the snake, since otherwise, choosing squares for the snake will become dependent on the choices made for the ladder and, as a result, the product rule cannot be applied.

  - 1. choose a black square for snake ... $n/2$ ways
  - 2. choose a white square for snake ... $n/2$ ways
  - 3. choose another square for ladder ... $n-2$ ways
  - 4. choose another square for ladder ... $n-3$ ways

  Observe that the last two phases can be permuted and would still produce the same ladder. Therefore, the above procedure overcounts by 2, and the answer is $n^2(n-2)(n-3)/8$.

Recitation 4

- Practice the 4 ways of making selections

Select k form n	ordered	unordered
no repetition	$\frac{n!}{(n-k)!}$	$\binom{n}{k}$
with repetition	n^k	$\binom{n+k-1}{k}$

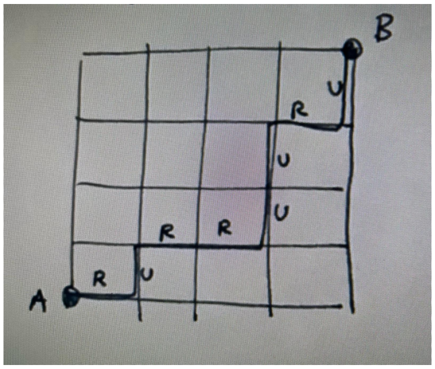
  with some typical examples of your choice. Here are some suggestions:

  - Go over the example of kids and gifts at end of Chapter 2.
  - Compare the two scenarios of making k-letter words using an n-letter alphabet, when the letters in the word must appear in alphabetical order or not. Emphasize the modeling and math over the exact literal wording; for instance, when alphabetical order is requires, we must use $\binom{n}{k}$, and when alphabetical order is not required, we must use $n!/(n-k)!$.
  - The same example above when repetitions are allowed, leading to $\binom{n+k-1}{k}$ or n^k when alphabetical order is required or not required, respectively.
  - Go over problems about binary patterns; for instance, why is the number of n-bit words 2^n, and those which have exactly k 1s $\binom{n}{k}$?

- In how many ways can we choose 3 people out of 10 to form a committee if one of them must be the chair of the committee? First, do this using the product rule by starting from scratch and adjusting for overcounting. Second, do it by abstractly modeling as a choice of 3 out of 10 without order, followed by a choice of the chair among the chosen ones. The first approach leads to $10 \cdot \frac{9 \cdot 8}{2}$, and the second leads to $\binom{10}{3} \cdot 3$.

- Practice concepts of one-to-one, onto, and bijection. Here are some examples (assume $\mathbb{N} = \{1, 2, 3, \ldots\}$):
  - $f : \mathbb{Z} \to \mathbb{Z}$, where $f(n) = 2n$
  - $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, where $f(n, m)$ is the larger of m and n
  - $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x/\pi$
  - $f : \mathbb{N} \to \mathbb{Z}$, where $f(n) = 1 - \frac{n}{2}$ if n is even, and $f(n) = \frac{n+1}{2}$ if n is odd.

- Count the number of up/right paths from A to B by establishing a bijection with binary words that have a specific number of 1s and 0s. The answer for the example below should be $\binom{8}{4}$. This is because there are that many binary words with 4 1s and 4 0s.



- Do an example of selecting k out of n with repetition and no order and remind the students that the number of ways we can do that is exactly the number of integer solutions to

$$x_1 + x_2 + \ldots + x_n = k, x_i \geq 0$$

  Use your own n and k in the example. Change the example by requiring $x_1 \geq 1$ instead. What does it really mean? (it means that in the k selection from $S = \{a_1, a_2, \ldots, a_n\}$, you must select a_1 at least once.)

Recitation 5

- If there are any items in Recitation 4 that are were not covered, cover them (or an equivalent idea) here.

- This is a word problem related to the integer solutions problem. Assume we have 20 people sitting in a row on a table, and we want to select 3 of them, but no two of the selected people can be adjacent. This can be modeled like this: The choice of the 3 people will divide the rest of the people on the table into 4 groups from left to right, with x_1, x_2, x_3, and x_4 people in each respectively, where $x_1 + x_2 + x_3 + x_4 = 17$. Given the constraints on adjacency, we know that $x_1 \geq 0$, $x_2 \geq 1$, $x_3 \geq 1$, and $x_4 \geq 0$. Using $x_2 = 1 + x'_2$ and $x_3 = 1 + x'_3$, we set up the equation:

  $$x_1 + x'_2 + x'_3 + x_4 = 15$$

  where $x_1, x'_2, x'_3, x_4 \geq 0$. The number of integer solutions is $\binom{4-1+15}{4-1} = \binom{18}{3}$.

  Remark: one might ask why did the original problem transform into the problem of choosing 3 from 18? One way to answer this is simply due to the bijection that transformed the original setting into the integer solutions problem. But another way of seeing this is as follows: Imagine all the people who are not selected. We have 17 of them. Look at the spaces between them (indicated by · below):

  .o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.o.

  There are exactly 18 spaces. The 3 selected people belong to these spaces. But given the adjacency constraint, each space can hold at most one person. Therefore, we must select 3 spaces out of the 18 to place the selected people.

- Make sure students understand the Pascal triangle and why:

  $$\binom{n}{k} = \binom{n}{n-k}$$

  $$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, 0 < k < n$$

  - Prove them algebraically by replacing binomial coefficients with what they are and manipulating the expressions.
  - Prove them by combinatorial arguments, i.e. by showing that they count the same thing in two ways. For instance, to choose k things out of n, we can choose $n-k$ things out of n and throw them away, leaving k things. In addition, if we assume $S = \{1, 2, \ldots, n\}$, then to choose k out of n, we can do it by making 1 among the choices and

choosing the remaining $k-1$ out of $n-1$, or we do it by making 1 not among the choices and choosing all k out of $n-1$. These two scenarios are disjoint and, therefore, their sum must make all ways of choosing k out of n.

- Make sure students understand the binomial theorem.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

For instance, what is the coefficient of $x^{13}y^{2011}$ in $(x+y)^{2024}$? In addition, make sure they understand the special cases of the binomial theorem in $(1+1)^n$ and $(1-1)^n$. Each of these two has an equivalent fact:

$$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

but the sum represents the number of subsets, so we re-establish what we knew

$$(1-1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \sum_{k \text{ is even}} \binom{n}{k} - \sum_{k \text{ is odd}} \binom{n}{k} = 0^n$$

the number of subsets with even size is is equal to the number of subsets with odd size

Recitation 6

- Practice anagrams and the formula $\frac{n!}{n_1!n_2!\ldots n_m!}$
- Use the Pascal triangle to show the following identity:

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

One can show the identity by starting with the Pascal triangle property:

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

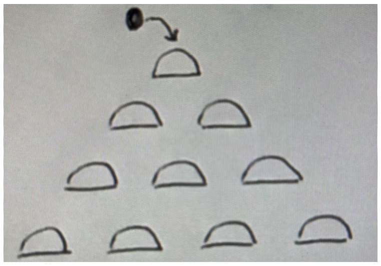
Then use

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

and keep on replacing the last term using the Pascal triangle property, until we end up with $\binom{k}{k}$ which can be replaced by $\binom{k-1}{k-1}$.

As a combinatorial argument, consider the set $S = \{1, 2, \ldots, n\}$. The binomial coefficient $\binom{n}{k}$ is the number of subsets of size k. The binomial coefficient $\binom{n-i}{k-1}$ is the number of subsets of size k containing i as the smallest element. By summing over $i = 1 \ldots n-k+1$ using the addition rule, we obtain the result.

- Counting with bijection: (another example) A ball is dropped as shown below. Upon hitting a bump, it will go either left or right. We have $2n$ rows of bumps, where $n \in \mathbb{N}$. The figure shows $n = 2$.



  - How many paths bring the ball to the middle of the last row? Think of a bijection with a set of binary patterns. The key is to consider binary patterns with n 1s and n 0s. Establish a bijection between paths that bring the ball to the center of the last row and those. Finally, conclude that the number of those paths must be $\binom{2n}{n}$.

- Make sure students understand why the following three are logically equivalent:
$$P \Rightarrow Q, \neg P \vee Q, \neg Q \Rightarrow \neg P$$

- Make sure students understand if and only if (iff) and that $\Leftrightarrow$ says it:
$$P \Leftrightarrow Q$$
$$P \text{ if and only if } Q$$
$$P \text{ iff } Q$$

P	Q	$P \Leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

- Make sure the students understand that the following is the negation of $P \Rightarrow Q$
$$P \wedge \neg Q$$
For instance, use DeMorgan's law:
$$\neg(P \Rightarrow Q) \Leftrightarrow \underbrace{\neg(\neg P \vee Q) \Leftrightarrow (P \wedge \neg Q)}_{\text{DeMorgan's}}$$

- What is the contrapositive of: r^2 is irrational $\Rightarrow$ r is irrational.

- How many Boolean functions on n variables are there? 2^{2^n} (why?)
- Put a Boolean function on three variables x, y, and z on the board and have the students figure out the logical expression using $\neg, \vee, \wedge$
- Draw analogy of associative, commutative, and distributive properties of sets operators $\cap$, $\cup$, and logical operator $\wedge$ and $\vee$

  Associative:

$$(A \cap B) \cap C = A \cap (B \cap C)$$
$$(A \wedge B) \wedge C = A \wedge (B \wedge C)$$

$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A \vee B) \vee C = A \vee (B \vee C)$$

Commutative:

$$A \cap B = B \cap A$$
$$A \wedge B = B \wedge A$$

$$A \cup B = B \cup A$$
$$A \vee B = B \vee A$$

Distributive:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$

Recitation 7

This recitation will mainly focus on proofs. You can come up with your own examples to illustrate proofs by contradiction, contrapositive, iff, etc... The first two below are existential proofs (which we have not covered explicitly in lectures).

- Introduce the idea of existential proofs. For instance, prove that there exists an even prime number. Here, it's enough to exhibit an example. Actually, the only example is the prime number 2.
- Sometimes, we can show the existence, without finding an actual example: non-constructive existential proof. For example, prove that if $a < -1$, then $e^{ax} + e^x = 2$ has a positive solution. First, consider the function

  $$f(x) = e^{ax} + e^x - 2$$

  The first derivative of $f(x)$ is $ae^{ax} + e^x$, which is equal to $a + 1 < 0$ when $x = 0$. Furthermore, the second derivative of $f(x)$ is $a^2e^{ax} + e^x$, which is always positive (function is concave). Therefore, starting at $f(0) = 0$, $f(x)$ decreases, but increases back to infinity. Therefore, $f(x)$ must cross 0 for some $x > 0$.
- Proofs by parity: consider an 5×5 chessboard. Consider removing one square. Depending on the color, white or black, of the removed square, which chessboard is coverable by dominos?
- Proof by contradiction: Prove that $x^3+x+1 = 0$ does not have any rational solutions. Proceed by assuming that is does; for instance, $x = a/b$ where a and b are integers. Write $\frac{a^3}{b^3} + \frac{a}{b} + 1 = 0$, and rewrite it as $a^3 + ab^2 + b^3 = 0$. Find a contradiction by going through all cases of even and odd for a and b.
- Prove using the contrapositive: $x + y$ is odd $\Rightarrow x \neq y$.
- Illustrate why if $P \Rightarrow True$ is true, then P is not necessarily True. You can show this using the truth table of $\Rightarrow$, since you will find two rows that make the implication true for different values of P.
- Prove iff. For instance, every element of S is even iff every subset of S has even sum. Here P is "every element of S is even", and Q is "every subset of S has even sum". We want to prove $P \Leftrightarrow Q$ is true.
  - $P \Rightarrow Q$: If every element is even, then since the sum of even elements is even, every subset will have an even sum.
  - $Q \Rightarrow P$: If every subset has an even sum, then the property applied to the singletons means every element is even.

Recitation 8

- One indication of understanding Cantor's proof is to understand the answer to this question: Why does Cantor's diagonalization proof break if we replace $\mathbb{R}$ by $\mathbb{Q}$? The answer is that the number constructed to create a contradiction may not be in $\mathbb{Q}$.

- Go over some sets of your choice. Examples include: the set of all watches made on Earth, The set of positive real numbers that are smaller than some fixed ϵ, the set $\mathbb{R} - \mathbb{Q}$, the set $\mathbb{Z}^3$, the set of all finite words that can be made from the alphabet $\{a, \ldots, z\}$, ...

- How many n bit binary patterns either start with 1 or end with 0? Let S_1 be the set of all binary patterns that start with 1. Similarly, let S_0 be the set of all binary patterns that end with 0. We want $|S_1 \cup S_0$. Using inclusion exclusion:

  $$|S_1 \cup S_0| = |S_1| + |S_0| = |S_\cap S_0| = 2^{n-1} + 2^{n-1} - 2^{n-2}$$
  $$= 2 \cdot 2^{n-1} - 2^{n-2} = 2^n - 2^{n-2} = 2^{n-2}(4-1) = 3 \cdot 2^{n-2}$$

  Note: do you see why there is a 3? (*Hint*: There are 3 ways of setting the first and last bits).

- In how many ways can we color n objects using Red, Green, and Blue, if we insists that every color must be used? Inclusion-Exclusion can help find the number of ways we can color the objects if some color is missing. Let S_R be the set of colorings that do not include Red. Define S_G and S_B in the same way. Then:

  $$|S_R \cup S_G \cup S_B| = |S_R| + |S_G| + |S_B| - |S_R \cap S_G| - |S_R \cap S_B| - |S_G \cap S_B| + |S_R \cap S_G \cap SB|$$

  Now

  - $|S_R| = |S_G| = |S_B| = 2^n$
  - $|S_R \cap S_G| = |S_R \cap S_B| = |S_G \cap S_B| = 1$
  - $|S_R \cap S_G \cap S_B| = 0$ We obtain:

    $$2^n + 2^n + 2^n - 1 - 1 - 1 + 0 = 3 \cdot 2^n - 3$$

    Therefore, the answer to the original questions would be $3^n - (3 \cdot 2^n - 3) = 3^3 - 3 \cdot 2^n + 3$.

- Given the set $\{1, 2, \ldots, 100\}$, show that if we select 6 numbers, two of them, say x and y, must satisfy $|x - y| \leq 19$. The idea is to use Pigeonhole. Divide the numbers into 5 "boxes" as follows:

  $$1 \ldots 20, 21 \ldots 40, 41 \ldots 60, 61 \ldots 80, 81 \ldots 100$$

  Since we select 6 numbers, two must come from the same box, which means two must have a difference of at most 19.

- A person cannot have more than 500,000 strands of hair on his/her head. In a city of 10 million people, show that at least 20 people must have the same number of hair strands. Another obvious use of Pigeonhole: There are 500,001 possible values for the number of strands $\{0, 1, \ldots, 500,000\}$. We place 10 pillion people in 500,001 boxes. By Pigeonhole, at least one box must contain at least $\lceil 10000000/500001 \rceil = 20$ people.
- Given 6 points on the perimeter of a rectangle, show that you can cut the rectangle into two pieces of the same area such that at least 4 points are in one piece. Here we have to be smart about it since the Piegonhole will give $\lceil 6/2 \rceil = 3$, which is not enough. Idea: pick a point on the perimeter and cut the rectangle by a line that goes through that point and the center. By symmetry, both pieces have the same area. Now, for the remaining 5 points, one piece must contain at least $\lceil 5/2 \rceil = 3$ of them. With the initial point being in "both" pieces, we have our 4 points.

Recitation 9

For this recitation, focus on proofs by Induction. You could also cover topics in inclusion-exclusion and pigeonhole based on students questions. For all proofs focus on the following:

- What the base case/s is/are. What n_0 is (the largest base case).
- Express the inductive hypothesis $P(k)$ (or $\wedge_{i \le k} P(i)$ for strong induction), and $P(k+1)$
- Emphasize the inductive step $\forall k \ge n_0, P(k) \Rightarrow P(k{+}1)$, or $\forall k \ge n_0, \wedge_{i \le k} P(i) \Rightarrow P(k+1)$ (for strong induction)

Here are some ideas for proofs by induction.

- Prove that $\sum_{i=1}^{n}(2i-1) = n^2$ for all $n \in \mathbb{N}$
  - $n_0 = 0$
  - $P(k) : \sum_{i=1}^{k}(2i-1) = k^2$
  - $P(k+1) : \sum_{i=1}^{k+1}(2i-1) = (k+1)^2$
- Prove that $\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1}$ for all $n \ge 0$ if $a \ne 1$
  - $n_0 = 0$
  - $P(k) : \sum_{i=0}^{k} a^i = \frac{a^{k+1}-1}{a-1}$
  - $P(k+1) : \sum_{i=0}^{k+1} a^i = \frac{a^{k+2}-1}{a-1}$

- Prove that $n(n+1)(2n+1)$ is divisible by 6 for all $n \geq 0$.
    - $n+0=0$
    - $P(k) : k(k+1)(2k+1) = 6m$
    - $P(k+1) : (k+1)(k+2)(2k+3) = 6m'$
    - Inductive step: (this might be a little involved) The trick is to expend $(k+1)(k+2)(2k+3)$ while exposing $k(k+1)(2k+1)$. The easiest way is to show that the difference is a multiple of 6, as follows: $(k+1)(k+2)(2k+3) - (k(k+1)(2k+1) = (k+1)[((k+2)(2k+3) - k(2k+1)] = (k+1)(2k^2+3k+4k+6-2k^2-k) = (k+1)(6k+6) = 6(k+1)^2$. Therefore, $(k+1)(k+2)(2k+3) = 6m + 6(k+1)^2 = 6m'$.

- (strong induction) Prove that every integer in $\mathbb{N}$ can be expressed as a sum of distinct powers of 2.
    - $n_0 = 1$
    - $\wedge_{i \leq k} P(i)$: every integer up to k is a sum of distinct powers of 2
    - $P(k+1) : k+1$ is a sum of distinct powers of 2
    - Inductive step: if $k+1$ is odd, then $k+1 = 2m+1 = 2m+2^0$ where $m \leq k$. By the inductive hypothesis, m is a sum of distinct powers of 2. Therefore, $2m$ is also a sum of distinct powers of 2, none of which is $2^0 = 1$. So $k+1$ is a sum of distinct powers of 2. If $k+1$ is even, then $k+1 = 2m$ where $m \leq k$. By the same argument above, $k+1$ is a sum of distinct powers of 2. Now, to make sure that the base case is sufficient, observe that the proof works only if $m \leq k$. In the first case $m = k/2$, and in the second case $m = (k+1)/2$. So we need $(k+1)/2 \leq k$, which means the proof works for $k \geq 1$. That's n_0.

- (strong induction) Let $a_0 = 1$, $a_1 = 1$, and $a_n = a_{n-1} + 2a_{n-2}$ for $n \geq 2$. Prove that $a_n = \frac{2^n - (-1)^n}{3}$ for all $n \geq 0$.
    - $n_0 = 1$, the bases cases are for $n = 0$ and $n = 1$
    - $\wedge_{i \leq k} P(i) : a_i = [2^i - (-1)^i]/3$ for all $i \leq k$
    - $P(k+1) : a_{k+1} = [2^{k+1} - (-1)^{k+1}]/3$
    - Inductive step: (use recurrence, of course what else!) $a_{k+1} = a_k + a_{k-1} = [2^k - (-1)^k]/3 + 2[2^{k-1} - (-1)^{k-1}]/3 = [2^k - (-1)^k + 2^k - 2(-1)^{k-1}] = [2 \cdot 2^k + (-1)^{k+1} - 2(-1)^{k+1}]/3 = [2^{k+1} - (-1)^{k+1}]/3$. The proof works if $k+1 \geq 2$ so we can apply the recurrence, which means $k \geq 1$, and that's n_0.

Recitation 10

- Solving linear homogeneous recurrences using the characteristic equation method.
  - $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 3$, $a_1 = 1$, $a_2 = 4$. The characteristic equation is $x^2 = 5x - 6$, which has solutions $p = 2$ and $q = 3$. Therefore, a_n has the form $a_n = c_1 2^n + c_2 3^n$. Solve for c_1 and c_2 using a_1 and a_2. We get $a_n = -\frac{1}{2}2^n + \frac{2}{3}3^n$.
  - $a_n = 8a_{n-1} - 16a_{an-2}$ for $n \geq 2$, $a_0 = 1$, $a_1 = 12$. The characteristic equations is $x^2 = 8x - 16$, which has solutions $p = q = 4$. Therefore, a_n as the form $a_n = c_1 4^n + c_2 n 4^n$. Solve for c_1 and c_2 using a_0 and a_1. We get $a_n = 4^n + 2n4^n$.

- Turning recurrences into linear homogeneous.
  - $a_n = 3a_{n-1} + 2^n$. Consider the recurrence for $n-1$: $a_{n-1} = 3a_{n-2} + 2^{n-1}$.

$$a_n = 3a_{n-1} + 2^n$$

$$a_{n-1} = 3a_{n-2} + 2^{n-1}$$

$$a_n - 2a_{n-1} = 3a_{n-1} + 2^n - 6a_{n-2} - 2^n$$

$$a_n = 5a_{n-1} - 6a_{n-2}$$

- Higher order recurrences.
  - $a_n = 4a_{n-1} - 3a_{n-2} + 2^n$ for $n \geq 3$, $a_1 = 1$, $a_2 = 11$. Using the above method, we can turn this recurrence into a homogeneous linear one, to obtain

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}, \text{ for } n \geq 4$$

In addition, knowing a_1 and a_2, we can find $a_3 = 49$. The characteristic equation is

$$x^3 - 6x^2 + 11x - 6 = 0$$

One can guess that $p = 1$ is a solution. Therefore, we can factor $(x-1)$. We get

$$(x-1)(x^2 + ax + 6) = 0$$

It is then easy to find that $a = -5$ by matching powers. So we have:

$$(x-1)(x^2 - 5x + 6) = 0$$

which has solutions $p = 1$, $q = 2$, and $r = 3$. Therefore, a_n has the form $a_n = c_1 + c_2 2^n + c_3 3^n$. We solve for c_1, c_2, and c_3 using a_1, a_2, and a_3. We get

$$a_n = 0 \cdot 1^n - 4 \cdot 2^n + 3 \cdot 3^n$$

Recitation 11

- Talk about divisibility, make sure students are comfortable with notation. For two integers a and b, all the following are equivalent:

  - $a|b$ (notation)
  - a divides b
  - a is a divisor of b
  - b is a multiple of a
  - $\exists m \in \mathbb{Z}, b = ma$ (definition)

  Furthermore, even if a does not divide b, notated by $a \nmid b$, we can still relate a and b as follows:

  $$b = aq + r$$

  where $0 \leq r < a$ with $a|b$ iff $r = 0$. The constraint that $0 \leq r < a$ makes this representation involving a and b unique. We call a the quotient of the division of b by a, and r its remainder.

- A common divisor of a and b is an integer d such that $d|a \wedge d|b$. One important concept is the greatest common divisor of two integers a and b, denoted by $\gcd(a, b)$. The $\gcd(a, b)$ is defined as the largest d such that d is a common divisor of a and b. This concept is well-defined because:

  - 1 is always a common divisor, so a common divisor exists
  - a divisor d of a must satisfy $d \leq a$; therefore, $\gcd(a, b) \leq \min(a, b)$, so the largest common divisor exists

- Finding the greatest common divisor has many applications in mathematics and computer science. It can be done by brute force: simply go through the set of all divisors of a and the set of all divisors of b, and find the largest that is in the intersection of both sets. Here's an example of finding $\gcd(300, 18)$:

  $$D_{300} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300\}$$

  $$D_{18} = \{1, 2, 3, 6, 9, 18\}$$

  $$D_{300} \cap D_{18} = \{1, 2, 3, 6\}$$

  Therefore, $\gcd(300, 18) = 6$

- A more efficient way of finding $\gcd(a, b)$ is based on the following important observation: Assume $a = bq + r$, then

  $$d|a \wedge d|b \Leftrightarrow d|b \wedge d|r$$

This means $\gcd(a, b) = \gcd(b, r)$. For instance,

$$\gcd(300, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0)$$

which corresponds to the following decreasing sequence (the sequence reaches 0 quickly):

$$300, 18, 12, 6, 0$$

Can you see the answer?

Recitation 12

Practice the extended Euclidean algorithm to find the $\gcd(a, b)$, and when $\gcd(a, b) = 1$, to find the inverse of a modulo b.

- Find $\gcd(1180, 482)$
- Find the inverses of $\{1, 2, 3, 4, 5, 6\}$ modulo 7
- Find $\gcd(127, 5)$ and the inverse of 5 modulo 127. Using this information, solve $5x = 36 \pmod{127}$.
- Solve

  $$12x + 31y \equiv 2 \pmod{127}$$
  $$2x + 89y \equiv 23 \pmod{127}$$

  Let's multiply the second equation by 6.

  $$12x + 534y \equiv 138 \pmod{127}$$

  and by observing that 534 is 26 and 138 is 11 modulo 127, we can write:

  $$12x + 26y \equiv 11 \pmod{127}$$

  By subtracting, we get $5y \equiv -9 \pmod{127}$, and since -9 is 118 modulo 127, we have

  $$5y \equiv 118 \pmod{127}$$

  We need the inverse of 5 modulo 127. The Euclidean algorithm:

127	5	2	1	0
1	0	1	-2	
0	1	-25	51	

  Therefore, the inverse of 5 modulo 127 is 51. We finally conclude that y must be $51 \cdot 118 = 6018$ modul0 127. So $\underline{y = 49}$.

  Replacing in the first equation, we have $2x + 31 \cdot 49 \equiv 2 \pmod{127}$, which can be written as

  $$2x \equiv -4338 \pmod{127}$$

  So $2x \equiv 107 \pmod{127}$ (because $-4338 = -35 \cdot 127 + 107$). Using the Euclidean algorithm again, one can find that the inverse of 2 modulo 127 is -63 modulo 127, which is 64. So $x \equiv 64 \cdot 107 = 6848 \pmod{127}$, and $\underline{x = 117}$.

Recitation 13

Go over equivalence relations and partial order relations. Use Lectures 32 and 33 as a guide.

Recitation 14

Go over prime numbers and Fermat's Theorem. Use Lectures 34 and 35 as a guide.

Use Fermat's Theorem to find

$$2^{124} \mod 127$$

We know that $2^{126} \equiv 1$ (mod127), and $2^{124} = 2^{-2}2^{126} = 4 \cdot 2^{126}$. So $2^{124} \equiv 2^{-2} = 4^{-1}$ (mod 127). So that's the inverse of 4 modulo 127, which is 32 (do the extended Euclidean algorithm)

Consider an RSA key set with $p = 17$, $q = 23$, and $e = 3$. What value of d should be used for the secret key? What is the encryption of the message 41?

352	3	1	0
1	0	1	
0	1	-117	

So the answer is -117, which is the same as 235 modulo 352.

The private key d is the inverse of e modulo $(p-1)(q-1)$, so this is the inverse of 3 modulo 352. The encryption of 41 is $41^e \mod n$, where $n = pq$. So this is $68921 \mod 391 = 105$.

Recitation 15

Go over graphs. Use Lectures 36 and 37 as a guide.